FACULDADE AUTÔNOMA DE DIREITO - FADISP/UNIALFA
ESCOLA DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO *STRICTO SENSU* EM DIREITO
MESTRADO EM FUNÇÃO SOCIAL DO DIREITO

DANILO TARTARINI SANCHES

RESPONSABILIDADE CIVIL DAS PLATAFORMAS DIGITAIS E PROTEÇÃO DE CRIANÇAS E ADOLESCENTES: PRESSUPOSTOS E LIMITES DA IMPUTAÇÃO OBJETIVA SOB O ECA DIGITAL

São Paulo
2026

DANILO TARTARINI SANCHES

RESPONSABILIDADE CIVIL DAS PLATAFORMAS DIGITAIS E PROTEÇÃO DE CRIANÇAS E ADOLESCENTES: PRESSUPOSTOS E LIMITES DA IMPUTAÇÃO OBJETIVA SOB O ECA DIGITAL

Dissertação apresentada ao Programa de Pós-Graduação *Stricto Sensu* em Direito da Faculdade Autônoma de Direito - FADISP/UNIALFA, como requisito parcial para obtenção do título de Mestre em Direito.
Área de concentração: Função Social do Direito.
Orientadora: Profa. Dra. Priscila Alves Patah.

São Paulo
2026

Dados Internacionais de Catalogação na Publicação (CIP)

S211r

Sanches, Danilo Tartarini.

Responsabilidade civil das plataformas digitais e proteção de crianças e adolescentes: pressupostos e limites da imputação objetiva sob o ECA digital. / Danilo Tartarini Sanches – São Paulo, 2026.

172 fls; 30cm.

Dissertação (Mestrado) – Faculdade Autônoma de Direito – FADISP – Programa de Pós-Graduação Stricto Sensu – Função Social do Direito – São Paulo, 2026.

Orientador (a): Profa. Dra. Priscila Alves Patah.

1. Responsabilidade civil objetiva. 2. ECA Digital. 3. Plataformas digitais. I. Patah, Priscila Alves. II. Faculdade Autônoma de Direito. III. Título.

CD

Bibliotecário responsável: Adenilto Lopes do Prado Junior – CRB-8/11438

FOLHA DE APROVAÇÃO

DANILO TARTARINI SANCHES

RESPONSABILIDADE CIVIL DAS PLATAFORMAS DIGITAIS E PROTEÇÃO DE CRIANÇAS E ADOLESCENTES: PRESSUPOSTOS E LIMITES DA IMPUTAÇÃO OBJETIVA SOB O ECA DIGITAL

Dissertação apresentada ao Programa de Pós-Graduação *Stricto Sensu* em Direito da Faculdade Autônoma de Direito - FADISP/UNIALFA, como requisito parcial para obtenção do título de Mestre em Direito. Área de concentração: Função Social do Direito.

Aprovada em: ____ de _____ de 2026.

Banca examinadora:

Profa. Dra. Priscila Alves Patah
Orientadora - FADISP/UNIALFA

_____

Prof. Dr.
Avaliador interno

_____

Prof. Dr.
Avaliador externo

_____

RESUMO

Esta dissertação analisa os pressupostos e os limites da responsabilidade civil objetiva na proteção de crianças e adolescentes em ambientes digitais sob o Estatuto Digital da Criança e do Adolescente, instituído pela Lei nº 15.211/2025. O problema de pesquisa consiste em saber em que medida os deveres proativos atribuídos às plataformas digitais podem justificar a imputação objetiva por violação de deveres proativos, especialmente quando a arquitetura do serviço cria ou amplia riscos previsíveis a pessoas em desenvolvimento. A pesquisa adota abordagem qualitativa, bibliográfica, documental e dogmática, com exame de legislação brasileira, doutrina civilista, proteção integral, direito do consumidor, proteção de dados, jurisprudência do STF e parâmetros comparados. Sustenta-se que o ECA Digital não transforma plataformas em garantidoras universais de todo dano online, mas densifica deveres de prevenção, segurança, transparência e resposta quando o serviço é acessado por crianças e adolescentes. Conclui-se que a responsabilização objetiva deve depender da demonstração de dever violado, risco criado ou ampliado, dano juridicamente relevante e nexo causal, admitindo excludentes compatíveis com a proteção integral.

Palavras-chave: responsabilidade civil objetiva; ECA Digital; plataformas digitais; proteção integral; crianças e adolescentes.

ABSTRACT

This dissertation examines the requirements and limits of strict civil liability concerning the protection of children and adolescents in digital environments under the Brazilian Digital Statute of the Child and Adolescent, enacted by Law No. 15,211/2025. The research question is whether proactive duties imposed on digital platforms may justify strict liability grounded on the breach of proactive duties, especially when the design and operation of the service create or increase foreseeable risks to developing persons. The study adopts a qualitative, bibliographical, documentary and dogmatic approach, based on Brazilian legislation, civil liability doctrine, integral protection, consumer law, data protection, Federal Supreme Court precedents and comparative parameters. It argues that the Digital Statute does not turn platforms into universal guarantors for every online harm, but it gives legal density to duties of prevention, safety, transparency and response when the service is accessed by children and adolescents. The conclusion is that strict liability should depend on a violated duty, created or increased risk, legally relevant harm and causal link, while allowing defenses compatible with integral protection.

Keywords: strict civil liability; Digital Statute of the Child and Adolescent; digital platforms; integral protection; children and adolescents.

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANPD	Agência Nacional de Proteção de Dados
CDC	Código de Defesa do Consumidor
CGI.br	Comitê Gestor da Internet no Brasil
CONANDA	Conselho Nacional dos Direitos da Criança e do Adolescente
CPC	Código de Processo Civil
DOU	Diário Oficial da União
DSA	*Digital Services Act*
ECA	Estatuto da Criança e do Adolescente
FGV	Fundação Getúlio Vargas
ICO	*Information Commissioner's Office*
LGPD	Lei Geral de Proteção de Dados Pessoais
MJSP	Ministério da Justiça e Segurança Pública
NBR	Norma Brasileira
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OECD	*Organization for Economic Co-operation and Development*
ONU	Organização das Nações Unidas
RE	Recurso Extraordinário
REsp	Recurso Especial
SECOM	Secretaria de Comunicação Social da Presidência da República
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TIC	Tecnologias da Informação e Comunicação
UNICEF	Fundo das Nações Unidas para a Infância

SUMÁRIO

1 INTRODUÇÃO 9
1.1 Contextualização do tema e relevância social da proteção digital infantojuvenil 12
1.2 Delimitação do objeto, problema de pesquisa e hipóteses 15
1.3 Objetivos, justificativa e metodologia 18
1.4 Estrutura da dissertação 20
2 PLATAFORMAS DIGITAIS E O REGIME PROATIVO DO ECA DIGITAL 22
2.1 Provedores de aplicações, redes sociais e serviços digitais 23
2.2 Modelo de negócio, curadoria algorítmica e monetização da atenção 25
2.3 Dever geral de cuidado diante de crianças e adolescentes 32
2.4 Âmbito de aplicação da Lei nº 15.211/2025 e acesso provável por menores 38
2.5 *Safety by design*, aferição de idade e privacidade por padrão 43
2.6 Obrigações proativas, deveres de resposta e proteção de dados 48
3 FUNDAMENTOS CIVIL-CONSTITUCIONAIS DA RESPONSABILIDADE DAS PLATAFORMAS 55
3.1 Art. 227 da Constituição Federal e proteção integral 55
3.2 Estatuto da Criança e do Adolescente e sujeito em desenvolvimento 61
3.3 Responsabilidade subjetiva, responsabilidade objetiva e atividade de risco 65
3.4 Função social da responsabilidade civil e deveres preventivos 71
3.5 Hipervulnerabilidade digital, relação de consumo e diálogo das fontes 77
3.6 Presunção de causalidade e ônus da prova em danos digitais complexos 83
4 REGIME GERAL DO MARCO CIVIL DA INTERNET, TEMAS 987 E 533 DO STF E A ESPECIALIDADE PROTETIVA DO ECA DIGITAL 90
4.1 Art. 19 do Marco Civil da Internet e ordem judicial específica 90
4.2 Tema 987 da repercussão geral 97
4.3 Tema 533 da repercussão geral 101
4.4 Limites do afastamento da responsabilidade objetiva no regime geral 105
4.5 ECA Digital como *lex specialis* de proteção infantojuvenil 111
5 CRITÉRIOS DOGMÁTICOS PARA A RESPONSABILIZAÇÃO OBJETIVA DAS PLATAFORMAS 119
5.1 Pressupostos de incidência no microssistema do ECA Digital 120
5.2 Descumprimento de dever proativo e presunção de causalidade 125

5.3 Excludentes admissíveis e limites da imputação 131
5.4 Tutela inibitória, tutela coletiva e distribuição dinâmica do ônus da prova 138
5.5 Danos individuais, coletivos e danos ao desenvolvimento biopsicossocial ... 144
5.6 Parâmetros comparados como apoio interpretativo 150
6 CONCLUSÃO 156
REFERÊNCIAS 164

1 INTRODUÇÃO

A experiência digital de crianças e adolescentes deixou de ocupar uma posição periférica na vida social. Redes sociais, plataformas de vídeos, jogos conectados, serviços de mensageria, publicidade comportamental e sistemas de recomendação participam da formação de vínculos, do consumo, da educação, da expressão cultural e da própria construção identitária de pessoas em desenvolvimento. Como esses ambientes são estruturados por agentes econômicos que definem regras de circulação, coleta de dados, moderação, impulsionamento e tratamento de denúncias, a responsabilidade civil já não pode ser examinada apenas depois do dano: ela passa a envolver, também, prevenção, governança e segurança do serviço (BRASIL, 1988; BRASIL, 1990a; COMITÊ GESTOR DA INTERNET NO BRASIL, 2026).

Não se questiona a licitude da atividade das plataformas digitais, tampouco se presume que todo dano ocorrido *online* deva ser transferido ao fornecedor. A questão é mais delimitada: em quais circunstâncias a arquitetura do ambiente digital cria, amplia ou conserva riscos previsíveis para crianças e adolescentes, tornando juridicamente relevante uma omissão empresarial ou uma resposta insuficiente? Para responder, é necessário distinguir a postagem isolada de terceiro da falha de moderação, do desenho persuasivo da interface, da recomendação automatizada, da publicidade dirigida e do tratamento de dados pessoais, pois cada situação mobiliza deveres e critérios de imputação próprios (BRASIL, 2014a; BRASIL, 2018; FRAZÃO, 2021).

A Lei nº 15.211/2025, denominada ECA Digital, conferiu maior densidade normativa a esse debate ao estabelecer deveres proativos de proteção no ambiente digital. Desde março de 2026, a lei está em vigor e conta com regulamentação geral promovida pelo Decreto nº 12.880/2026. O novo microssistema não substitui o Marco Civil da Internet, a LGPD, o Código Civil, o Código de Defesa do Consumidor ou o Estatuto da Criança e do Adolescente; sua função é coordenar e especializar a incidência desses diplomas quando o serviço é dirigido a menores ou provavelmente acessado por eles. A orientação adotada, portanto, recusa tanto a revogação implícita dos regimes gerais quanto sua utilização para esvaziar a proteção especial (BRASIL, 2002; BRASIL, 2014a; BRASIL, 2025a; BRASIL, 2026a).

A investigação não sustenta uma responsabilidade integral das plataformas. Tal modelo converteria o fornecedor em garantidor universal de qualquer evento

danoso ocorrido no serviço, solução incompatível com a complexidade da *internet*, com a liberdade comunicativa e com a preservação de espaços legítimos de inovação. O que se propõe é a responsabilidade objetiva por violação de deveres proativos: objetiva porque dispensa a demonstração de culpa e se vincula ao risco da atividade e à posição de controle do fornecedor; fundada em deveres porque o suporte fático da imputação não é o mero exercício da atividade, mas a identificação de um dever concretamente violado, de risco criado ou ampliado, de dano juridicamente relevante e de nexo causal demonstrado ou inferido por critérios controláveis (TEPEDINO; TERRA; GUEDES, 2024; FARIAS; ROSENVALD; BRAGA NETTO, 2023).

Cabe advertir, desde logo, que não se propõe aqui um *tertium genus* entre a responsabilidade subjetiva e a objetiva, nem a criação de categoria autônoma de responsabilidade civil. O regime invocado é o da responsabilidade objetiva já consagrada no art. 927, parágrafo único, do Código Civil e no art. 14 do Código de Defesa do Consumidor, cuja incidência dispensa a demonstração de culpa. A referência à violação de deveres proativos não altera a espécie de imputação: ela descreve o suporte fático que a desencadeia. Diferentemente das hipóteses em que basta o exercício de atividade normalmente perigosa ou a existência de defeito de concepção do produto, a imputação aqui examinada exige a identificação de um dever legalmente exigível de organização, prevenção, transparência ou resposta, cujo descumprimento se conecte causalmente ao dano. Trata-se, ademais, de responsabilidade fundada na teoria do risco criado, e não do risco integral, razão pela qual as excludentes da responsabilidade civil tradicionais permanecem (HIRONAKA, 2005; SCHREIBER, 2015).

A vulnerabilidade infantojuvenil, embora juridicamente central, não pode funcionar como atalho argumentativo. A prioridade absoluta não elimina a necessidade de prova, proporcionalidade e individualização da conduta relevante. Pelo contrário: como a matéria envolve proteção de dados, consumo, liberdade de expressão, direitos da personalidade e desenvolvimento biopsicossocial, a tutela digital de menores exige fundamentação mais rigorosa. O argumento protetivo somente adquire utilidade dogmática quando esclarece qual dever era exigível, em que momento ocorreu a falha e de que maneira ela se relacionou com o dano (BRASIL, 1988; AZEVEDO; TORRES, 2023).

A prova constitui uma dificuldade própria desse tipo de litígio. A criança, o adolescente ou sua família normalmente percebem a manifestação externa da lesão

pela exposição de imagem, assédio, recomendação nociva, contato abusivo, publicidade exploratória ou circulação indevida de dados, mas não têm acesso aos registros internos que permitem reconstruir a cadeia técnica. Métricas de alcance, parâmetros de recomendação, histórico de denúncias, critérios de bloqueio e documentação de resposta permanecem, em regra, sob controle da plataforma. A assimetria não autoriza condenação automática, mas justifica a distribuição dinâmica do ônus probatório e o emprego de presunções relativas quando a informação decisiva estiver concentrada no fornecedor (BRASIL, 2015a; MULHOLLAND, 2009).

A comparação com regimes jurídicos estrangeiros não cumpre, nesta dissertação, função meramente ilustrativa ou de reforço retórico. Ela é metodologicamente necessária por três razões articuladas. A primeira é interpretativa: o próprio ECA Digital incorporou categorias de origem comparada – proteção desde a concepção (*safety by design*), avaliação de risco, privacidade por padrão e, sobretudo, o critério de serviço "provavelmente acessado" por menores, cuja formulação remonta ao *Age Appropriate Design Code* britânico. Conceitos transplantados não podem ser interpretados como se tivessem nascido no vazio; compreender o sentido que adquiriram e as dificuldades que enfrentaram em sua origem é condição para aplicá-los com precisão no direito brasileiro (ICO, 2022; UNIÃO EUROPEIA, 2022; UNITED KINGDOM, 2023). A segunda razão é de concretização: os deveres proativos instituídos pela Lei nº 15.211/2025 são, em larga medida, conceitos jurídicos indeterminados, e a experiência estrangeira demonstra como obrigações abertas de prevenção, transparência e resposta podem ser traduzidas em rotinas técnicas verificáveis, oferecendo repertório para densificar o padrão de diligência exigível. A terceira razão é dogmática e conecta-se diretamente à dissertação: como as plataformas reguladas operam em escala transnacional e já implementam tais medidas para cumprir a legislação europeia e britânica, a comparação evidencia a viabilidade técnica dessas providências e a previsibilidade dos riscos correspondentes – elementos que, no plano da imputação objetiva, reforçam a exigibilidade do dever e afastam a alegação de impossibilidade fática de prevenção.

A comparação também situa o ordenamento brasileiro no plano das obrigações internacionais assumidas pelo país. O Comentário Geral nº 25 do Comitê dos Direitos da Criança interpreta a Convenção sobre os Direitos da Criança, internalizada pelo Decreto nº 99.710/1990, e concretiza, no ambiente digital, o mandamento de proteção integral do art. 227 da Constituição; nessa medida, o parâmetro comparado não é

inteiramente externo ao sistema, mas auxilia a leitura de fontes que já vinculam o Brasil (BRASIL, 1988; BRASIL, 1990c; UNITED NATIONS, 2021). Além disso, o contraste entre regimes cumpre função crítica: ao confrontar a bipartição brasileira entre crianças e adolescentes com modelos estrangeiros construídos sobre um único marco etário, a análise revela a especificidade da solução nacional e previne a transposição acrítica de categorias concebidas para contextos normativos distintos.

Fixado esse alcance, os referenciais estrangeiros são mobilizados com função comparativa, e não como fundamento autônomo de responsabilização. O *Age Appropriate Design Code*, o *Digital Services Act*, o *Online Safety Act* e o Comentário Geral nº 25 demonstram que proteção desde a concepção, avaliação de risco, transparência e canais de resposta podem ser traduzidos em rotinas juridicamente verificáveis; a validade da dissertação, contudo, permanece ancorada no art. 227 da Constituição, no ECA, no Código Civil, no CDC, na LGPD, no Marco Civil da Internet e na Lei nº 15.211/2025 (UNITED NATIONS, 2021; ICO, 2022; UNIÃO EUROPEIA, 2022; UNITED KINGDOM, 2023).

Diante desse recorte, a pergunta central é a seguinte: em que medida os deveres proativos estabelecidos ou reforçados pelo ECA Digital permitem sustentar a responsabilidade civil objetiva das plataformas por danos sofridos por crianças e adolescentes, sem convertê-las em garantidoras universais dos riscos *online*? A hipótese afirma que a imputação é admissível quando coexistem acesso provável por menores, dever concreto de prevenção ou resposta, descumprimento verificável, risco criado ou ampliado pela arquitetura do serviço e nexo suficiente entre a falha e o dano. Esses elementos orientam a estrutura analítica desenvolvida nos capítulos seguintes.

1.1 Contextualização do tema e relevância social da proteção digital infantojuvenil

A presença de crianças e adolescentes na internet brasileira demonstra que a discussão deixou de ser eventual. O acesso digital acompanha lazer, sociabilidade, estudo, consumo, produção de conteúdo e participação cultural. Essa inserção amplia oportunidades, mas também expõe menores a formas específicas de contato abusivo, exploração comercial, coleta de dados, recomendação nociva, circulação de imagens e pressão por engajamento. A relevância jurídica decorre justamente dessa ambivalência: o mesmo ambiente que permite participação e aprendizagem também pode organizar riscos em escala, com velocidade e permanência que tornam

insuficiente uma resposta apenas reparatória (COMITÊ GESTOR DA INTERNET NO BRASIL, 2025; UNICEF, 2025).

A proteção integral impõe que essa realidade seja lida a partir da condição peculiar de desenvolvimento. Crianças e adolescentes não se relacionam com publicidade, recomendação algorítmica, exposição de imagem ou coleta de dados do mesmo modo que usuários adultos. A menor capacidade de antecipar consequências futuras, de compreender estratégias de persuasão e de avaliar a permanência dos registros digitais justifica um padrão reforçado de cuidado. Esse padrão não retira a autonomia progressiva do adolescente, mas exige que ela seja compatibilizada com segurança, informação adequada e prevenção proporcional (BRASIL, 1988; BRASIL, 1990a; UNITED NATIONS, 2021).

A relevância social também se manifesta na natureza dos danos digitais. A remoção posterior de um conteúdo pode ser necessária, mas nem sempre é suficiente. Uma imagem compartilhada, uma sequência de recomendações autolesivas, um perfilamento indevido ou uma publicidade dirigida a menor pode produzir efeitos sobre privacidade, reputação, saúde mental e desenvolvimento emocional antes mesmo da formação de uma demanda judicial. Por isso, a responsabilidade civil precisa dialogar com prevenção, documentação da resposta e preservação de provas, sem perder sua função reparatória quando o dano já se consumou (SAFERNET BRASIL, 2025; FRAZÃO, 2021).

A arquitetura das plataformas digitais torna o problema mais complexo. Serviços digitais não apenas recebem conteúdos; eles definem visibilidade, permanência, prioridade, circulação, monetização e padrões de interação. Essa constatação não significa que toda plataforma seja autora de conteúdo de terceiro, mas impede que a neutralidade técnica seja afirmada de modo absoluto. O relevante para a responsabilidade civil é verificar se a plataforma, por escolhas próprias de desenho, recomendação, moderação, privacidade ou resposta, criou ou ampliou risco previsível a menores (SOUZA; LEMOS, 2016; GILLESPIE, 2018; FRAZÃO, 2022).

O modelo econômico baseado em engajamento também precisa ser considerado. A permanência do usuário, a reação emocional, o compartilhamento e a coleta de dados podem se converter em valor econômico. Esse dado, isoladamente, não fundamenta dever de indenizar; contudo, ajuda a compreender previsibilidade, capacidade de prevenção e grau de controle. Quando a plataforma sabe que determinado público vulnerável frequenta o serviço, conhece padrões de uso e dispõe

de ferramentas para reduzir exposição indevida, a omissão pode ganhar relevância jurídica (ZUBOFF, 2019; COHEN, 2019; DONEDA, 2020).

A proteção digital infantojuvenil não deve ser confundida com censura prévia generalizada ou vigilância absoluta. A prevenção exigível deve ser proporcional, transparente e adequada ao risco. Canais de denúncia, padrões de privacidade por padrão, avaliação de risco, explicação mínima sobre recomendação, moderação tempestiva e preservação de registros podem ser medidas relevantes em determinados contextos. O ponto jurídico não está em eliminar todo risco da vida *online*, mas em impedir que riscos previsíveis e administráveis sejam transferidos integralmente à criança, ao adolescente ou à família (BRASIL, 2025a; ICO, 2022).

A discussão também se relaciona com o consumo. Serviços digitais aparentemente gratuitos podem envolver relação de consumo quando a plataforma explora dados, atenção ou publicidade como contrapartida econômica. Nessa hipótese, a criança ou o adolescente é simultaneamente usuário, titular de dados, destinatário de publicidade e sujeito protegido por prioridade absoluta. A leitura do CDC em diálogo com o ECA, a LGPD e o ECA Digital permite identificar deveres de segurança e informação sem desconsiderar as particularidades do ambiente digital (BRASIL, 1990b; BENJAMIN; MARQUES; BESSA, 2022; MIRAGEM, 2019).

A assimetria probatória reforça a relevância do tema. Em danos digitais complexos, a vítima raramente tem acesso aos critérios de recomendação, aos *logs* de denúncia, à documentação de resposta ou à lógica de moderação. A plataforma, por sua vez, controla informações que podem esclarecer se o dano decorreu apenas de conduta de terceiro ou se foi ampliado por falha própria do serviço. Essa diferença justifica que a análise da responsabilidade considere não apenas o evento lesivo, mas também a distribuição de informação técnica entre as partes (BRASIL, 2015a; MULHOLLAND, 2009).

Nesses termos, a relevância social da proteção digital infantojuvenil não decorre de um temor abstrato da tecnologia. Ela nasce da combinação entre presença massiva de menores na *internet*, exploração econômica da atenção, opacidade técnica, coleta de dados e dificuldade de reparação integral posterior. A função da dissertação é transformar essa constatação em critérios jurídicos verificáveis, evitando tanto a omissão do sistema de responsabilidade civil quanto a imputação sem limites dogmáticos.

Relatórios institucionais também mostram que a proteção não pode ser formulada apenas a partir de categorias abstratas. O panorama internacional sobre infância conectada identifica benefícios educacionais e participativos, mas registra desigualdades de acesso, exposição a contatos indesejados e dificuldades de compreensão sobre coleta de dados. No Brasil, registros de denúncias e orientações públicas sobre uso de telas revelam que mediação familiar, desenho do serviço e resposta institucional precisam atuar de forma complementar. Esses documentos não substituem a análise jurídica, mas oferecem base empírica para avaliar previsibilidade do risco e adequação das medidas de prevenção (UNICEF, 2019; BRASIL, 2025e; BRASIL, 2025f).

1.2 Delimitação do objeto, problema de pesquisa e hipóteses

A dissertação delimita seu objeto à responsabilidade civil de plataformas digitais por danos sofridos por crianças e adolescentes em ambientes digitais, com ênfase nos deveres proativos associados ao ECA Digital. Não se pretende examinar todos os conflitos jurídicos da internet, nem todas as formas de regulação administrativa, penal ou concorrencial. A pesquisa concentra-se nas hipóteses em que a organização do serviço digital, seus mecanismos de recomendação, moderação, publicidade, proteção de dados ou resposta institucional podem criar, ampliar ou conservar riscos relevantes a pessoas em desenvolvimento (BRASIL, 2025a).

O recorte subjetivo da pesquisa merece justificativa própria. A concentração em crianças e adolescentes, e não em outros grupos hipervulneráveis, decorre, em primeiro lugar, do próprio objeto normativo analisado: a Lei nº 15.211/2025 é um estatuto dirigido especificamente à proteção da infância e da adolescência no ambiente digital, de modo que investigar a responsabilidade civil por ela densificada implica, necessariamente, centrar a análise nesse público. Em segundo lugar, a proteção de crianças e adolescentes apoia-se em um regime constitucional singular – a prioridade absoluta e a proteção integral do art. 227 da Constituição –, qualitativamente distinto dos fundamentos que amparam idosos e pessoas com deficiência, os quais contam com microssistemas normativos próprios, como o Estatuto da Pessoa Idosa (BRASIL, 2003) e o Estatuto da Pessoa com Deficiência (BRASIL, 2015b). Em terceiro lugar, a vulnerabilidade infantojuvenil possui natureza desenvolvimental: decorre da condição de pessoa em formação, da evolução progressiva das capacidades e da menor aptidão para antecipar consequências e

reconhecer estratégias de persuasão, o que a diferencia tanto da vulnerabilidade situacional do consumidor quanto daquela associada ao envelhecimento ou à deficiência (BRASIL, 1988; BRASIL, 1990a; BRASIL, 2025a).

Esse recorte não afirma que os demais grupos hipervulneráveis estejam menos expostos a riscos digitais, nem que sua tutela seja menos importante. A opção responde a uma exigência metodológica de profundidade: cada grupo mobiliza fundamentos, deveres e parâmetros próprios, cuja análise conjunta comprometeria o rigor dogmático pretendido. Ademais, a matriz de imputação desenvolvida nesta dissertação – assentada em dever concreto, risco criado ou ampliado, dano juridicamente relevante e nexo causal – não é logicamente restrita à infância; seus critérios podem, com as devidas adaptações, oferecer subsídio à reflexão sobre a responsabilidade civil por danos digitais a outros sujeitos hipervulneráveis, tema que se remete a investigações posteriores.

Essa delimitação afasta a ideia de que a mera existência de conteúdo lesivo de terceiro basta para responsabilizar a plataforma. O ponto de partida é distinguir conteúdo produzido por usuário, conduta própria do serviço e falha de resposta. Quando a plataforma apenas hospeda conteúdo e age conforme o regime legal aplicável, a discussão permanece mais próxima do Marco Civil da Internet. Quando, porém, o dano se relaciona com impulsionamento, desenho inseguro, tratamento indevido de dados, demora injustificada ou ausência de mecanismos proporcionais de proteção, a análise passa a envolver deveres próprios do fornecedor (BRASIL, 2014a; FRAZÃO, 2022).

O problema de pesquisa consiste em saber se, e em que medida, os deveres proativos do ECA Digital podem fundamentar a responsabilidade objetiva das plataformas digitais por danos infantojuvenis. A referência à violação de deveres proativos é empregada para evitar dois extremos: de um lado, a imunização da plataforma por simples invocação de neutralidade técnica; de outro, a responsabilização automática por qualquer dano ocorrido online. A imputação deve depender de dever concretamente exigível, risco previsível, falha verificável, dano e nexo causal suficiente (TEPEDINO; TERRA; GUEDES, 2024; SCHREIBER, 2015).

A hipótese principal sustenta que a Lei nº 15.211/2025 reforça a possibilidade de responsabilização objetiva quando o serviço é direcionado a crianças e adolescentes ou provavelmente acessado por eles, e quando a plataforma descumpre deveres de prevenção, segurança, transparência ou resposta que estavam dentro de

sua esfera de controle. O fundamento não está apenas no dano, mas no vínculo entre o risco organizado pela atividade, o dever violado e a condição especial da vítima. A responsabilidade objetiva, nessa leitura, não elimina o nexo; ela desloca a análise da culpa subjetiva para a gestão do risco (BRASIL, 2002; BRASIL, 2025a).

A primeira hipótese secundária é que a especialidade protetiva do ECA Digital deve ser lida em diálogo com o Marco Civil da Internet. O art. 19 do Marco Civil continua relevante para discussões sobre responsabilização por conteúdo de terceiro, especialmente pela exigência de ordem judicial específica em determinadas hipóteses. Contudo, esse regime não esgota todas as situações de dano digital, sobretudo quando o problema não é apenas a existência de conteúdo, mas a organização técnica de sua circulação, a falha de canais de denúncia, o tratamento de dados de menores ou o descumprimento de dever proativo de segurança (BRASIL, 2014a; BRASIL, 2025b; BRASIL, 2025c).

A segunda hipótese secundária é que a hipervulnerabilidade digital de crianças e adolescentes exige atenção especial à prova. A dificuldade de demonstrar a cadeia técnica do dano não pode resultar em inviabilidade prática da tutela. Em situações nas quais a plataforma controla os registros decisivos, a distribuição dinâmica do ônus da prova e a presunção relativa de causalidade podem funcionar como instrumentos de equilíbrio, desde que vinculados a indícios concretos de falha e não a presunções abstratas de responsabilidade (AZEVEDO; TORRES, 2023; MULHOLLAND, 2009; BRASIL, 2015a).

As duas hipóteses secundárias operam em planos distintos e complementares. A primeira situa-se no plano normativo e responde a qual regime incide sobre o dano digital infantojuvenil; a segunda situa-se no plano processual e verifica se esse regime é praticável diante da assimetria informacional que caracteriza o ambiente digital.

Com essa delimitação, a dissertação preserva o recorte jurídico do trabalho. O objetivo não é produzir estudo geral sobre *internet*, nem defender controle absoluto de plataformas, mas formular critérios para decidir quando a atividade digital, ao alcançar menores, cria ou amplia risco que pode ser imputado objetivamente ao fornecedor. A delimitação do objeto, portanto, organiza a investigação e evita dispersão em temas paralelos.

1.3 Objetivos, justificativa e metodologia

O objetivo geral da dissertação é analisar se os deveres proativos previstos ou reforçados pelo ECA Digital podem fundamentar a responsabilidade civil objetiva de plataformas digitais por danos sofridos por crianças e adolescentes. A análise busca identificar os pressupostos dessa imputação, seus limites dogmáticos e sua compatibilidade com o Marco Civil da Internet, a LGPD, o Código Civil, o CDC e a proteção integral.

Os objetivos específicos são: examinar o alcance do ECA Digital quanto a serviços direcionados ou provavelmente acessados por menores; distinguir responsabilidade por conteúdo de terceiro e responsabilidade por falha própria da plataforma; verificar como a proteção integral, a hipervulnerabilidade digital e a relação de consumo interferem na imputação civil; analisar a tensão entre Marco Civil, STF e especialidade protetiva; e propor critérios para dever, falha, risco, dano, nexo causal, presunções relativas, excludentes e tutela coletiva.

A justificativa acadêmica decorre da necessidade de aproximar campos que muitas vezes são tratados separadamente: responsabilidade civil, proteção da infância, direito digital, proteção de dados e consumo. O tema exige articulação dogmática porque a simples soma de normas não resolve o problema da imputação. É preciso compreender a função de cada fonte, o papel de cada dever e o modo como a arquitetura digital transforma riscos previsíveis em situações juridicamente relevantes (GUSTIN; DIAS; NICÁCIO, 2020).

A justificativa social está relacionada à intensidade da presença de menores em ambientes digitais e aos efeitos persistentes de danos ligados a imagem, reputação, privacidade, saúde mental e desenvolvimento. A reparação posterior pode ser insuficiente quando o dano se espalha rapidamente ou quando a vítima não consegue reconstruir a cadeia técnica de exposição. Por isso, a prevenção, a transparência e a documentação da resposta assumem importância prática (COMITÊ GESTOR DA INTERNET NO BRASIL, 2026; SAFERNET BRASIL, 2025).

Essas duas dimensões da justificativa – acadêmica e social – inscrevem-se diretamente na área de concentração Função Social do Direito e, em especial, na linha de pesquisa Função Social dos Institutos de Direito Privado, projeto Função Social da Responsabilidade Civil. A investigação parte da centralidade dos direitos fundamentais e da dignidade da pessoa humana para examinar um problema

tipicamente situado no âmbito das relações privadas: o vínculo entre plataformas digitais e crianças e adolescentes. Ao sustentar que o art. 227 da Constituição e a proteção integral vinculam também agentes econômicos privados, a pesquisa concretiza a aplicação direta das normas constitucionais às relações intersubjetivas e recusa a rígida dicotomia entre direito público e direito privado, tratando a Constituição como parâmetro legítimo de regulação de condutas empresariais que afetam pessoas em desenvolvimento (BRASIL, 1988; TEPEDINO; TERRA; GUEDES, 2024).

O recorte também se articula ao eixo do desenvolvimento humano, uma vez que o bem jurídico tutelado é o próprio desenvolvimento biopsicossocial de crianças e adolescentes, ameaçado por arquiteturas de serviço e por um modelo econômico estruturado sobre a monetização da atenção. Ao propor critérios que orientem a solução de conflitos privados – inclusive diante de insuficiência normativa infraconstitucional – à luz da função social da responsabilidade civil, da justiça social e da proteção de sujeitos hipervulneráveis, a dissertação busca contribuir para uma ordem jurídica comprometida com a efetivação de direitos fundamentais no ambiente digital e com a consolidação do Estado Democrático de Direito.

A pesquisa adota abordagem qualitativa, bibliográfica, documental e dogmática. A revisão bibliográfica reúne obras de responsabilidade civil, direito do consumidor, proteção de dados, direito digital e direito da criança e do adolescente. O *corpus* documental compreende legislação, decisões judiciais, relatórios institucionais e documentos internacionais. O raciocínio predominante é dedutivo: parte-se dos fundamentos normativos e dogmáticos para testar sua aplicação em hipóteses específicas de atuação das plataformas, sem dispensar a análise funcional de cada serviço e de cada risco (GIL, 2022; GUSTIN; DIAS; NICÁCIO, 2020).

O recorte possui limites deliberados. A dissertação não realiza pesquisa empírica própria com usuários nem auditoria técnica de algoritmos, e tampouco pretende oferecer uma taxonomia exaustiva de todos os serviços digitais. Seu propósito é construir uma matriz dogmática de decisão a partir de fontes jurídicas e institucionais verificáveis. Por essa razão, exemplos tecnológicos são empregados para testar a coerência dos critérios propostos, e não para afirmar conclusões empíricas universais sobre uma plataforma específica.

As fontes estrangeiras são mobilizadas de forma subsidiária para iluminar técnicas de desenho seguro, avaliação de risco, transparência e proteção por padrão. Não se procede à importação automática de categorias regulatórias. Sempre que um

parâmetro comparado é utilizado, sua compatibilidade é verificada à luz da Constituição, do ECA, do Código Civil, do CDC, da LGPD, do Marco Civil e do ECA Digital. Essa cautela preserva o caráter nacional da conclusão e evita que experiências institucionais distintas sejam tratadas como equivalentes.

Compreendidos nesses limites, os parâmetros comparados contribuem para a construção de deveres de diligência sem substituir a legislação nacional: regras estrangeiras sobre desenho apropriado à idade, avaliação de risco e dever de cuidado demonstram que a prevenção pode ser operacionalizada tecnicamente, ao passo que a validade da responsabilização no Brasil permanece dependente da Constituição, do ECA, do Código Civil, do CDC, da LGPD, do Marco Civil e do ECA Digital, além da jurisprudência nacional aplicável (UNITED NATIONS, 2021; ICO, 2022; UNIÃO EUROPEIA, 2022).

A apresentação formal da pesquisa segue o Manual de Normalização da FADISP/UNIALFA e as normas da Associação Brasileira de Normas Técnicas nele indicadas, especialmente quanto à estrutura, às citações e às referências. Essa observância não integra o fundamento dogmático da dissertação, mas assegura uniformidade acadêmica e transparência na identificação das fontes utilizadas (BIBLIOTECAS ALFA EDUCAÇÃO, 2025).

1.4 Estrutura da dissertação

A dissertação está organizada em introdução, quatro capítulos de desenvolvimento e conclusão. A ordem adotada segue uma progressão lógica: primeiro se delimita o ambiente digital e os deveres proativos; depois se apresentam os fundamentos civil-constitucionais da responsabilidade; em seguida se examina a tensão com o Marco Civil da Internet e a jurisprudência do STF; por fim se formulam critérios dogmáticos para a responsabilização objetiva por violação de deveres proativos.

O capítulo 2 trata das plataformas digitais e do regime proativo do ECA Digital. Nele são analisados provedores de aplicações, redes sociais, serviços digitais, modelo de negócio, curadoria algorítmica, monetização da atenção, dever geral de cuidado, acesso provável por menores, *safety by design*, aferição de idade, privacidade por padrão, deveres de resposta e proteção de dados.

O capítulo 3 apresenta os fundamentos civil-constitucionais da responsabilidade das plataformas. A análise parte do art. 227 da Constituição Federal,

do Estatuto da Criança e do Adolescente e da noção de sujeito em desenvolvimento, passando pela responsabilidade objetiva, pela atividade de risco, pela função social da responsabilidade civil, pela hipervulnerabilidade digital, pela relação de consumo, pelo diálogo das fontes, pela presunção de causalidade e pela distribuição do ônus da prova.

O capítulo 4 examina o Marco Civil da Internet, o Supremo Tribunal Federal e a especialidade protetiva do ECA Digital. A finalidade é distinguir o regime geral de responsabilização por conteúdo de terceiro, especialmente a partir do art. 19 do Marco Civil e dos Temas 987 e 533, das hipóteses em que a plataforma pode responder por dever próprio de prevenção, segurança, transparência ou resposta.

O capítulo 5 sistematiza os critérios dogmáticos para a responsabilização objetiva das plataformas. São tratados os pressupostos de incidência no microssistema do ECA Digital, o descumprimento de dever proativo, a presunção relativa de causalidade, as excludentes admissíveis, os limites da imputação, a tutela inibitória, a tutela coletiva, a distribuição dinâmica do ônus da prova e os danos ao desenvolvimento biopsicossocial.

A conclusão retoma o problema de pesquisa e verifica a hipótese central e as duas hipóteses secundárias. O objetivo final é demonstrar se a responsabilidade objetiva por violação de deveres proativos constitui resposta juridicamente adequada para danos digitais infantojuvenis quando houver dever proativo descumprido, risco criado ou ampliado pela plataforma, dano juridicamente relevante e nexo causal suficiente.

2 PLATAFORMAS DIGITAIS E O REGIME PROATIVO DO ECA DIGITAL

Antes de examinar a responsabilidade civil, é preciso compreender o objeto sobre o qual ela incide. A plataforma não será tratada como simples espaço neutro de hospedagem, mas como ambiente organizado por decisões técnicas, econômicas e normativas. Termos de uso, padrões de privacidade, sistemas de recomendação, métricas de engajamento, canais de denúncia, moderação e publicidade moldam a experiência do usuário e podem interferir na criação ou na ampliação de riscos. Essa constatação não antecipa a imputação; apenas define o campo em que ela será construída (SOUZA; LEMOS, 2016; GILLESPIE, 2018).

O regime proativo do ECA Digital altera a perspectiva temporal do problema. Já não basta perguntar se determinado conteúdo foi retirado depois da provocação do usuário ou do Judiciário. Também importa verificar se o serviço incorporou, antes do incidente, medidas proporcionais de prevenção, transparência, resposta e proteção de dados para um público infantojuvenil previsível. Essa lógica não elimina o Marco Civil da Internet; acrescenta-lhe uma camada especial de cuidado quando o serviço alcança pessoas em desenvolvimento (BRASIL, 2014a; BRASIL, 2025a).

A função deste capítulo é delimitar como o risco digital é organizado antes de discutir o art. 927 do Código Civil, a relação de consumo, a causalidade e as excludentes da responsabilidade civil. A responsabilidade objetiva aqui defendida não decorre da mera presença de tecnologia. Ela pressupõe a combinação entre atividade econômica, acesso previsível por menores, capacidade técnica de prevenção e descumprimento de um dever verificável. Sem essa descrição funcional, a análise tenderia a confundir plataforma, usuário e terceiro produtor de conteúdo (BRASIL, 2002; FRAZÃO, 2021).

Esse percurso afasta duas simplificações frequentes. A primeira atribui à plataforma a autoria de tudo o que circula em seu ambiente; a segunda nega qualquer dever próprio sempre que o conteúdo tenha sido produzido por terceiro. Entre esses extremos, interessa examinar a conduta institucional do serviço: a existência de mecanismos preventivos, a eventual ampliação algorítmica do risco, a tempestividade da resposta, a adequação do tratamento de dados e a qualidade dos registros disponíveis para reconstrução do evento.

A previsibilidade da presença de crianças e adolescentes é o fator que intensifica o padrão de cuidado. Serviços formalmente destinados a adultos podem

ser amplamente utilizados por menores, circunstância que não pode ser ignorada quando a empresa dispõe de métricas de acesso, sinais de uso, linguagem de interface e dados sobre conteúdos promovidos. O critério de acesso provável impede que a incidência da proteção dependa exclusivamente de declarações contratuais e aproxima o direito do funcionamento efetivo do serviço (BRASIL, 2025a; ICO, 2022).

O capítulo examina, assim, as plataformas como ambientes de risco organizado. A expressão não presume ilicitude: indica apenas que escolhas empresariais podem produzir, ampliar, reduzir e documentar riscos. A responsabilidade civil somente poderá ser formulada com consistência depois que essas escolhas e seus limites forem descritos com precisão.

2.1 Provedores de aplicações, redes sociais e serviços digitais

O Marco Civil da Internet consolidou a categoria dos provedores de aplicações ao distinguir acesso à rede, aplicações e conteúdo. Essa distinção foi relevante para evitar responsabilização automática de intermediários e para preservar liberdade de expressão, inovação e segurança jurídica. Contudo, a evolução das plataformas digitais tornou insuficiente uma leitura puramente formal da intermediação. Redes sociais, serviços de vídeo, jogos conectados, aplicativos de mensagens, lojas de aplicativos e ambientes de publicidade comportamental não exercem todos a mesma função nem organizam riscos do mesmo modo (BRASIL, 2014a; SOUZA; LEMOS, 2016).

A análise jurídica deve começar pela atividade concreta do serviço. Um provedor que apenas disponibiliza infraestrutura técnica não possui o mesmo grau de ingerência de uma rede social que recomenda conteúdo, mede engajamento, define padrões de visibilidade, estabelece regras de moderação e monetiza atenção. Essa diferença importa porque a responsabilidade civil depende da identificação do dever violado. Não basta afirmar que o fornecedor é plataforma; é preciso demonstrar qual funcionalidade estava sob seu controle e como ela se relacionou com o dano (TEFFÉ, 2015; MEDEIROS, 2020).

As redes sociais ocupam posição específica porque organizam interação e circulação de conteúdo em escala. O conteúdo pode ser produzido por terceiros, mas sua visibilidade, permanência e velocidade de difusão podem depender de decisões técnicas do serviço. Recomendação algorítmica, impulsionamento, notificações, ordenação de comentários, destaque de perfis e resposta a denúncias compõem uma

arquitetura de circulação. A responsabilidade civil não deve confundir essa arquitetura com autoria do conteúdo, mas também não pode ignorá-la quando ela amplia risco previsível a menores (GILLESPIE, 2018; FRAZÃO, 2022).

Serviços de vídeo curto e jogos conectados acrescentam outra camada ao debate. Nessas plataformas, permanência, recompensa, competição, compras integradas, comunicação entre usuários e publicidade podem formar ambiente especialmente sensível para adolescentes. O risco não está apenas na existência de conteúdo impróprio, mas na combinação entre *design* persuasivo, engajamento contínuo e dificuldade de supervisão familiar. Quando o fornecedor conhece o público provável e dispõe de meios técnicos de mitigação, a omissão pode assumir relevância jurídica (AZEVEDO; TORRES, 2023; FERNANDES; TEFFÉ; BRANCO, 2024).

Aplicativos de mensagens e comunidades fechadas exigem cautela diferente. Nesses ambientes, há maior peso da privacidade comunicacional e menor visibilidade pública do conteúdo. Isso não significa ausência de deveres, mas exige que medidas de prevenção sejam proporcionais e compatíveis com sigilo, segurança e autonomia dos usuários. Canais de denúncia, mecanismos de bloqueio, preservação de evidências em hipóteses legais e respostas a riscos graves podem ser relevantes, mas não autorizam vigilância indiscriminada (BRASIL, 2014a; BRASIL, 2018).

A noção de provedor de aplicação, portanto, precisa ser combinada com a noção de poder de organização. Quanto maior a capacidade do serviço de definir fluxo de informação, coletar dados, recomendar conteúdo, responder a denúncias e documentar incidentes, maior a necessidade de justificar a adequação de suas medidas de proteção quando menores são afetados. Essa leitura não transforma toda plataforma em seguradora universal, mas impede que a complexidade técnica seja usada como escudo absoluto contra deveres civis (FRAZÃO, 2021; SCHREIBER, 2015).

A responsabilidade civil das plataformas deve ser examinada em camadas. A primeira camada identifica o tipo de serviço e sua funcionalidade relevante. A segunda verifica se havia acesso provável por crianças ou adolescentes. A terceira identifica o dever de prevenção, segurança, informação ou resposta. A quarta analisa se houve descumprimento e se esse descumprimento se relaciona com o dano. Somente depois dessas etapas se pode falar em imputação objetiva.

Tal leitura permite preservar o regime do Marco Civil da Internet e, ao mesmo tempo, reconhecer deveres especiais de proteção. O art. 19 continua a desempenhar

papel importante quando a pretensão se funda exclusivamente na não remoção de conteúdo de terceiro. Contudo, quando o dano decorre de falha própria de arquitetura, tratamento de dados, recomendação, publicidade dirigida ou resposta institucional inadequada, a análise não pode se limitar à pergunta sobre ordem judicial específica. É necessário examinar a conduta organizacional da plataforma (BRASIL, 2014a; BRASIL, 2025a; FRAZÃO, 2022).

Para crianças e adolescentes, essa distinção tem efeito prático. Uma postagem ofensiva isolada pode exigir regime de remoção; uma recomendação reiterada de conteúdo autolesivo, uma publicidade comportamental incompatível com a idade ou a demora sistemática diante de denúncias envolvendo menor exigem exame de deveres próprios. Em cada caso, o julgador deve reconstruir o caminho do risco: quem tinha informação, quem podia agir, que medida era proporcional e como a falha se conectou ao dano.

Pode-se concluir que provedores de aplicações, redes sociais e serviços digitais não devem ser analisados como categoria única e homogênea. A dissertação utilizará essa distinção para evitar tanto a responsabilização genérica quanto a irresponsabilidade estrutural. O critério relevante será sempre funcional: que papel a plataforma exerceu na organização do ambiente, que dever podia ser exigido e de que modo sua conduta se relacionou com o dano sofrido por criança ou adolescente.

2.2 Modelo de negócio, curadoria algorítmica e monetização da atenção

O modelo de negócio das plataformas digitais é relevante para a responsabilidade civil porque revela como o serviço transforma permanência, atenção, dados e interação em valor econômico. Essa constatação não significa que a exploração econômica da internet seja ilícita; significa apenas que o desenho do serviço não é juridicamente indiferente quando o público alcançado inclui crianças e adolescentes. Quanto maior a dependência de engajamento contínuo, maior a necessidade de examinar se a arquitetura adotada intensifica riscos previsíveis a sujeitos em desenvolvimento (ZUBOFF, 2019; FRAZÃO, 2021).

A curadoria algorítmica altera a experiência do usuário ao selecionar, ordenar, recomendar ou repetir conteúdos de acordo com padrões inferidos do comportamento anterior. O ponto jurídico não é afirmar que o algoritmo cria todo conteúdo exibido, mas reconhecer que ele influencia a intensidade, a frequência e o contexto em que esse conteúdo chega ao destinatário. A recomendação de vídeos, perfis, desafios,

anúncios ou comunidades pode transformar uma interação isolada em exposição reiterada, o que aproxima a análise da organização do serviço e não apenas da conduta de terceiros (GILLESPIE, 2018; PASQUALE, 2015).

A monetização da atenção assume especial relevância quando a plataforma sabe, ou deveria saber, que menores utilizam o serviço de modo habitual. Sistemas concebidos para prolongar permanência, estimular reação emocional e multiplicar retorno à plataforma podem afetar crianças e adolescentes de forma diversa dos adultos. O direito civil deve, portanto, avaliar se havia previsibilidade do risco, se existiam meios razoáveis de mitigação e se o fornecedor documentou adequadamente as medidas adotadas (AZEVEDO; TORRES, 2023; LIVINGSTONE; STOILOVA; HOPWOOD, 2021).

A imputação objetiva não decorre automaticamente da existência de curadoria algorítmica. É necessário identificar a funcionalidade específica, o público provavelmente atingido, o risco previsível, o dever aplicável e o nexo com o dano. Uma falha de moderação após denúncia reiterada, por exemplo, não tem o mesmo tratamento de uma recomendação automatizada que amplia conteúdos nocivos a adolescentes ou de uma publicidade comportamental dirigida a crianças. Cada hipótese exige descrição própria do dever violado (BRASIL, 2014a; BRASIL, 2025a).

A assimetria probatória é um dos pontos centrais desse tópico. A família ou o adolescente normalmente percebe o resultado da exposição, mas não possui acesso aos critérios de ranqueamento, aos *logs* de denúncia, ao histórico de moderação, aos testes de segurança ou às métricas de alcance. Por isso, a prova do nexo não pode ser tratada como se todos os elementos estivessem igualmente disponíveis às partes. A distribuição dinâmica do ônus da prova e a presunção relativa de causalidade podem ser úteis quando vinculadas a indícios concretos de falha e à posse empresarial das informações decisivas (BRASIL, 2015a; MULHOLLAND, 2009).

O diálogo com o direito do consumidor também é relevante. Plataformas que oferecem serviços em troca de atenção, dados ou exposição publicitária podem ser analisadas como fornecedoras, especialmente quando direcionam funcionalidades a usuários vulneráveis. O CDC não elimina a necessidade de prova do dano e do nexo, mas reforça deveres de segurança, informação adequada, prevenção de riscos e boa-fé objetiva no ambiente digital (BRASIL, 1990b; BENJAMIN; MARQUES; BESSA, 2022; MIRAGEM, 2019).

O controle jurídico da monetização da atenção deve evitar dois excessos. O primeiro é tratar todo modelo baseado em engajamento como ilícito. O segundo é aceitar que a lógica econômica do serviço afaste qualquer dever de cuidado. A solução intermediária é examinar se a plataforma, conhecendo o uso provável por menores e dispondo de instrumentos de mitigação, deixou de adotar medidas proporcionais de segurança, transparência ou resposta. Nessa hipótese, a arquitetura econômica do serviço passa a integrar a avaliação do risco criado ou ampliado.

Considerados esses elementos, o modelo de negócio deve ser tratado como parte da reconstrução do risco, e não como conclusão antecipada do tópico. A análise precisa avançar da descrição econômica para a identificação da funcionalidade que interferiu no caso, da informação disponível à plataforma e das salvaguardas que poderiam ter reduzido a exposição. É essa passagem entre incentivo, controle e dano que permite formular um dever juridicamente verificável.

A curadoria algorítmica também altera a forma de analisar o nexo causal. Não se exige abertura integral do código-fonte em toda demanda, mas a plataforma deve ser capaz de explicar critérios gerais de recomendação, medidas de redução de alcance, histórico de denúncia e resposta a conteúdos potencialmente nocivos. A discussão jurídica, portanto, não recai sobre a existência abstrata de algoritmo, e sim sobre o modo como determinada funcionalidade participou da exposição do menor ao risco concretamente alegado. Essa é a diferença entre responsabilizar pelo conteúdo de terceiro e responsabilizar pela organização empresarial da circulação (GILLESPIE, 2018; FRAZÃO, 2021).

O ponto sensível está em separar monetização legítima de exploração juridicamente relevante da vulnerabilidade. Plataformas podem remunerar-se por publicidade, assinaturas, compras internas ou tratamento de dados, mas devem demonstrar que a maximização de permanência não foi estruturada de modo incompatível com a proteção de menores. Quando notificações, *autoplay*, ranqueamento, desafios virais e publicidade comportamental são combinados para intensificar engajamento de crianças e adolescentes, o risco deixa de ser apenas externo e passa a integrar a lógica do serviço. Essa leitura aproxima a economia da atenção do dever de segurança, sem transformar lucro em ilicitude automática (ZUBOFF, 2019; MIRAGEM, 2019).

A ligação com a responsabilidade objetiva aparece quando o desenho econômico deixa de ser apenas pano de fundo e passa a integrar o risco da atividade.

Se a plataforma estimula permanência prolongada, exposição repetida e interação com conteúdos sensíveis, deve demonstrar que adotou medidas proporcionais para usuários vulneráveis. A ausência de salvaguardas não transforma automaticamente a atividade em ilícita, mas pode revelar defeito organizacional quando conectada a dano concreto e previsível (TEPEDINO; TERRA; GUEDES, 2024; SCHREIBER, 2015).

O controle jurídico da monetização da atenção também exige proporcionalidade. Não se deve exigir que a plataforma elimine todo mecanismo de recomendação, pois a própria utilidade do serviço pode depender de seleção e organização de conteúdo. O que se exige é que funcionalidades de alto impacto sobre menores sejam acompanhadas de avaliação de risco, opção de redução de personalização, canais de denúncia efetivos e transparência compatível com a idade. O dever não é abolir a tecnologia, mas tornar sua utilização compatível com a prioridade absoluta (BRASIL, 1988; BRASIL, 2025a).

O exemplo da publicidade comportamental ilustra a relevância do recorte. Uma propaganda genérica visualizada por adolescente não tem o mesmo significado jurídico de uma campanha segmentada a partir de dados sensíveis, interesses inferidos ou vulnerabilidades comportamentais. Quando o anúncio explora insegurança corporal, impulsividade, dependência de jogos, consumo compulsivo ou exposição de imagem, a análise passa a envolver proteção de dados, relação de consumo e proteção integral. A responsabilidade dependerá da demonstração de que a plataforma participou da segmentação ou deixou de limitar prática previsivelmente nociva (BRASIL, 1990b; BRASIL, 2018; MIRAGEM, 2019).

Em termos probatórios, a curadoria automatizada exige documentação mínima. A vítima não precisa demonstrar todos os critérios técnicos do algoritmo, mas deve apresentar indícios de exposição reiterada, recomendação ou falha de resposta. A plataforma, por sua vez, possui melhores condições de informar se havia histórico de denúncia, filtros aplicáveis, limitação de alcance, classificação etária ou medida de mitigação. A distribuição dinâmica do ônus da prova encontra aí campo de aplicação, desde que vinculada a fatos específicos e não a presunções abstratas (BRASIL, 2015a; MULHOLLAND, 2009).

A participação da plataforma na circulação não é uniforme. Há seleção quando o sistema escolhe quais conteúdos serão exibidos; ranqueamento quando estabelece uma ordem de prioridade; amplificação quando aumenta o alcance; e segmentação quando direciona mensagens, anúncios ou recomendações a perfis específicos. Essa

taxonomia evita tratar toda curadoria como fenômeno único e permite relacionar cada intervenção a deveres, provas e consequências próprias (GILLESPIE, 2018; PASQUALE, 2015).

A experiência do usuário também é moldada por escolhas de interface. Reprodução automática, rolagem infinita, recompensas intermitentes e notificações insistentes podem reduzir a capacidade de interrupção consciente, sobretudo entre usuários mais jovens. Esses recursos não são ilícitos por definição, mas devem ser avaliados em conjunto com idade provável, frequência de uso e conteúdo promovido. A relevância jurídica surge quando o design intensifica risco previsível sem mecanismos proporcionais de controle e sem alternativas compreensíveis para o público infantojuvenil (ICO, 2022; LIVINGSTONE; STOILOVA; HOPWOOD, 2021).

Os incentivos econômicos precisam ser conectados à governança interna. Uma plataforma que remunera equipes e sistemas exclusivamente por crescimento de engajamento pode criar ambiente institucional pouco sensível a sinais de risco. A análise civil pode considerar metas, relatórios de impacto, fluxos de aprovação e autonomia das áreas de segurança, desde que tais elementos sejam vinculados ao evento discutido. O modelo econômico é relevante porque ajuda a explicar decisões organizacionais, e não porque a obtenção de lucro seja, por si só, ilícita (COHEN, 2019; ZUBOFF, 2019).

A prova dessa contribuição pode ser estruturada por camadas. A vítima apresenta histórico de exposição, registros de interação, denúncias e efeitos percebidos; a plataforma esclarece objetivos do sistema, critérios gerais de distribuição, testes de segurança e providências adotadas; e a perícia, quando necessária, verifica a coerência entre essas informações. Esse método preserva segredos empresariais legítimos sem permitir que a opacidade técnica elimine a possibilidade de controle judicial (BRASIL, 2015a; MULHOLLAND, 2009).

O teste jurídico deve, portanto, separar receita legítima, risco empresarial e defeito do serviço. A obtenção de vantagem econômica integra o contexto, mas a imputação depende de demonstração adicional: previsibilidade do público vulnerável, capacidade de intervenção, ausência de salvaguarda razoável e relação entre a funcionalidade e o dano. Essa sequência impede que a monetização seja usada como presunção absoluta e, ao mesmo tempo, evita que a gratuidade aparente do serviço o coloque fora dos deveres de segurança e informação (MIRAGEM, 2019; TEPEDINO; TERRA; GUEDES, 2024).

A monetização dirigida a menores também deve ser confrontada com a Resolução CONANDA nº 163/2014, que considera abusivo o direcionamento de publicidade e comunicação mercadológica à criança. Em plataformas digitais, a publicidade pode estar incorporada ao fluxo de recomendação, ao conteúdo de influenciadores, a recompensas de jogos ou a formatos que dificultam a percepção de sua natureza comercial. A incidência da resolução não transforma qualquer anúncio em dano indenizável, mas reforça o dever de distinguir conteúdo comercial, impedir exploração da inexperiência e documentar os critérios de segmentação usados quando o público infantil é previsível (BRASIL, 2014b; MIRAGEM, 2019).

A curadoria algorítmica também deve ser examinada a partir de seus objetivos de otimização. Sistemas orientados exclusivamente a tempo de permanência tendem a privilegiar materiais capazes de provocar reação intensa, ainda que a reação seja medo, indignação ou ansiedade. Para crianças e adolescentes, essa lógica pode produzir ciclos de exposição que não seriam escolhidos conscientemente. A relevância civil surge quando a empresa conhece o padrão, dispõe de métricas sobre seus efeitos e deixa de adotar salvaguardas proporcionais, como limites de repetição, diversidade de recomendações ou interrupções de uso (ZUBOFF, 2019; GILLESPIE, 2018).

A prova da contribuição algorítmica não exige acesso irrestrito ao segredo industrial. É possível trabalhar com documentos de governança, resultados de testes, relatórios de impacto, parâmetros gerais de classificação e histórico de recomendações recebido pelo perfil afetado. O juiz pode preservar informações sensíveis e, ainda assim, exigir explicação suficiente sobre a função do sistema. A ausência de transparência não deve produzir presunção absoluta de culpa, mas pode justificar redistribuição do ônus quando a empresa detém exclusivamente os elementos necessários à reconstrução do dano.

A segmentação comercial reforça a necessidade de distinguir recomendação editorial de publicidade. Conteúdos patrocinados, ofertas incorporadas a jogos e divulgações de influenciadores podem aparecer de modo semelhante a comunicações espontâneas. Para o público infantil, a dificuldade de reconhecer a intenção persuasiva exige identificação ostensiva e limitação de técnicas que explorem urgência, recompensa ou pertencimento. O descumprimento dessas medidas pode caracterizar defeito informacional do serviço e violação da proteção contra publicidade abusiva (BRASIL, 1990b; BRASIL, 2014b).

Outro aspecto é a formação de perfis inferidos. Mesmo sem declarar idade, o comportamento de navegação pode revelar interesses escolares, jogos, linguagem e horários típicos de menores. Se a plataforma utiliza esses sinais para personalizar publicidade, torna-se incoerente alegar desconhecimento absoluto da presença infantil quando chamada a adotar proteção. O uso econômico das inferências deve vir acompanhado de responsabilidade por sua governança, respeitando finalidade, necessidade e melhor interesse (BRASIL, 2018; MENDES, 2014).

Nesse quadro, a monetização deve ser compreendida como elemento de contexto causal. Ela ajuda a explicar por que determinados conteúdos recebem prioridade e por que medidas de proteção podem contrariar incentivos empresariais. Não basta, porém, demonstrar que a empresa lucra. A parte autora deve relacionar o mecanismo de remuneração à exposição, à amplificação ou ao atraso na resposta. Essa exigência impede condenações abstratas e concentra a análise na forma concreta pela qual o modelo de negócio contribuiu para o risco.

Um primeiro cenário evidencia a recomendação reiterada de conteúdo autolesivo a adolescente que demonstrou interesse inicial em tema relacionado à saúde mental. A funcionalidade relevante não é a mera hospedagem, mas a sequência automatizada de recomendações. O risco consiste na intensificação progressiva da exposição; o dever envolve avaliação de risco, limitação de repetição e mecanismos de interrupção; a prova pode abranger histórico de recomendações, parâmetros de classificação e alertas internos. A plataforma poderá afastar a imputação se demonstrar que adotou salvaguardas adequadas e que a cadeia lesiva decorreu de circunstância externa não previsível.

Em segundo cenário, publicidade comportamental de produto inadequado é direcionada a criança a partir de perfil inferido por dados de navegação. Aqui, a conduta própria está no tratamento de dados e na segmentação comercial. O risco decorre da exploração da menor capacidade de compreensão persuasiva; o dever envolve privacidade por padrão, restrição de perfilamento e observância da Resolução CONANDA nº 163/2014. A análise causal deverá verificar se a segmentação contribuiu efetivamente para a exposição e se a plataforma possuía meios razoáveis de identificar o público infantil.

Por fim, imagine-se o impulsionamento pago de desafio perigoso dirigido a adolescentes. A remuneração e o controle da distribuição aproximam a plataforma do risco produzido. Documentos de contratação, critérios de aprovação do anúncio,

segmentação, alcance e histórico de denúncias tornam-se centrais. A defesa não se limita a alegar autoria de terceiro: deverá demonstrar triagem, resposta tempestiva e diligência compatível com a gravidade do conteúdo. O caso ilustra a diferença entre circulação orgânica e amplificação comercial, especialmente após o julgamento conjunto, pelo STF, dos Temas 987 e 533 da repercussão geral.

2.3 Dever geral de cuidado diante de crianças e adolescentes

O dever geral de cuidado diante de crianças e adolescentes nasce da combinação entre prioridade constitucional, proteção integral e atividade econômica organizada em ambiente digital. Não se trata de exigir vigilância absoluta, censura prévia generalizada ou eliminação de todo risco, mas de impor às plataformas um padrão de diligência compatível com a previsibilidade de uso por menores e com a capacidade técnica do fornecedor (BRASIL, 1988; BRASIL, 1990a; FRAZÃO, 2021).

Esse dever deve ser concretizado por medidas verificáveis. Em serviços digitais acessados por menores, cuidado não pode significar apenas cláusula genérica em termos de uso. Ele deve aparecer em padrões de privacidade, linguagem adequada, canais de denúncia acessíveis, resposta tempestiva, avaliação de risco, preservação de registros e desenho de interface compatível com a idade provável do usuário. A relevância jurídica está na possibilidade de comparar o risco previsível com a medida efetivamente adotada (BRASIL, 2025a; UNITED NATIONS, 2021).

A proteção integral modifica a intensidade do cuidado porque crianças e adolescentes não têm a mesma capacidade de compreender coleta de dados, publicidade comportamental, recomendação automatizada e circulação permanente de imagens. A autonomia progressiva deve ser respeitada, mas não pode servir como justificativa para transferir ao menor toda a carga de risco criada por ambientes tecnicamente organizados. A plataforma continua podendo inovar, comunicar e monetizar, desde que compatibilize essas atividades com salvaguardas proporcionais (BRASIL, 1990a; ROSA; PIN, 2022).

O dever de cuidado também depende do tipo de serviço. Uma rede social aberta, um jogo com interação entre usuários, uma plataforma de vídeo curto e um aplicativo de mensagens não apresentam o mesmo grau de visibilidade pública, controle de circulação ou risco de exposição. Por isso, o cuidado exigível deve ser funcional: deve considerar a arquitetura concreta, a idade provável do público, o tipo

de interação, a intensidade da coleta de dados e a possibilidade real de intervenção sem violar outros direitos fundamentais.

A responsabilidade civil objetiva por violação de dever proativo exige que o descumprimento do dever seja descrito com precisão. Não basta afirmar que a plataforma não protegeu suficientemente o menor. É necessário identificar se houve falha em aviso, moderação, privacidade por padrão, resposta a denúncia, limitação de publicidade, recomendação algorítmica ou preservação de evidências. Essa especificação impede que a proteção integral se torne argumento genérico e permite controle judicial da imputação (TEPEDINO; TERRA; GUEDES, 2024; SCHREIBER, 2015).

A prova do dever violado pode depender de documentação interna. Políticas de segurança, relatórios de risco, histórico de resposta, métricas de denúncia e registros de moderação ajudam a demonstrar se a plataforma atuou de modo diligente. Quando esses elementos estão sob controle exclusivo do fornecedor, a distribuição dinâmica do ônus da prova pode funcionar como técnica de equilíbrio, sem dispensar a vítima de apresentar narrativa mínima e indícios plausíveis do dano (BRASIL, 2015a; MULHOLLAND, 2009).

O dever geral de cuidado tem ainda dimensão preventiva e coletiva. Muitos danos digitais não atingem apenas uma vítima isolada, pois podem decorrer de desenho sistêmico, falha recorrente de moderação, publicidade segmentada inadequada ou padrão de recomendação perigoso. Nesses casos, a tutela civil não deve se limitar à indenização posterior; pode envolver tutela inibitória, obrigações de fazer, deveres de transparência e medidas de correção do serviço (BRASIL, 1990b; BRASIL, 1985).

Assim, o dever geral de cuidado diante de crianças e adolescentes não transforma a plataforma em garantidora universal. Ele funciona como ponte entre proteção integral e responsabilidade civil, exigindo que o fornecedor demonstre coerência entre risco conhecido, capacidade técnica e medida adotada. Quando essa coerência falta e o dano se relaciona ao risco criado ou ampliado pela atividade, abre-se espaço para a imputação objetiva.

O exame deve considerar a autonomia progressiva. Crianças e adolescentes não formam grupo homogêneo; há diferenças relevantes entre primeira infância, pré-adolescência e adolescência. Por isso, o cuidado não deve ser confundido com exclusão absoluta do ambiente digital. A medida adequada pode variar entre restrição

de publicidade, reforço de privacidade, aviso contextual, limitação de contato com desconhecidos, supervisão parental proporcional ou resposta prioritária a denúncia. A função civil do cuidado é calibrar proteção e participação, preservando o desenvolvimento da pessoa menor de idade (BRASIL, 1990a; UNITED NATIONS, 2021).

O dever geral de cuidado não pode ser descrito apenas como recomendação ética. Em serviços digitais acessados por menores, ele se manifesta em providências verificáveis: linguagem compreensível, canais de denúncia simples, resposta tempestiva, bloqueio proporcional, revisão de recomendações, limitação de publicidade inadequada e registro das medidas adotadas. A utilidade dogmática desse dever está em permitir que o julgador pergunte o que a plataforma poderia razoavelmente saber, prevenir e documentar no momento anterior ao dano, e não apenas depois da judicialização (FRAZÃO, 2021; BRASIL, 2025a).

A função preventiva da responsabilidade civil aparece com clareza nesse ponto. Se o serviço possui meios razoáveis de reduzir risco conhecido antes da lesão, o direito não deve limitar-se à compensação posterior. Obrigações de fazer, ajustes de interface, melhoria de canais de denúncia e preservação de registros são formas de aproximar tutela civil e prevenção. Essa leitura é compatível com a função social da responsabilidade civil e com a prioridade constitucional de proteção infantojuvenil (ROSENVALD, 2017; BRASIL, 1988).

O cuidado ganha conteúdo especial quando o dano é cumulativo. Exposição de imagem, humilhação pública, recomendação reiterada de conteúdo autolesivo ou contato abusivo podem produzir efeitos persistentes, ainda que cada ato isolado pareça insuficiente para explicar a extensão do prejuízo. A análise deve considerar a sequência de eventos e a resposta institucional da plataforma. A demora ou a ausência de registro pode transformar um risco administrável em dano ampliado (SAFERNET BRASIL, 2025; AZEVEDO; TORRES, 2023).

Também é necessário reconhecer limites. O dever de cuidado não autoriza monitoramento absoluto de conversas privadas, quebra generalizada de sigilo ou censura automática de manifestações legítimas. A medida deve ser adequada ao risco e ao tipo de ambiente. Em redes abertas, a moderação e a redução de alcance podem ter maior peso; em mensageria privada, canais de denúncia, bloqueio e preservação de evidências em hipóteses legais podem ser mais proporcionais. A responsabilidade

civil precisa dialogar com privacidade e liberdade comunicativa (BRASIL, 2014a; BRASIL, 2018).

A plataforma não se exime do dever de cuidado apenas por inserir cláusula contratual que transfere responsabilidade ao usuário ou aos responsáveis. Termos de uso são relevantes, mas não substituem desenho seguro e resposta efetiva. Em ambiente acessado por menores, linguagem excessivamente técnica, aviso escondido ou mecanismo de denúncia difícil de localizar pode revelar inadequação do serviço. A boa-fé objetiva e o dever de informação exigem comunicação compatível com a compreensão do público atingido (BRASIL, 1990b; BENJAMIN; MARQUES; BESSA, 2022).

A intensidade do cuidado depende da idade provável do público. Crianças em idade inicial, pré-adolescentes e adolescentes possuem graus diversos de compreensão, autonomia e vulnerabilidade. O direito não deve tratar esses grupos como bloco homogêneo. Uma medida adequada para adolescente mais velho pode ser insuficiente para criança pequena, especialmente em temas como publicidade, compras internas, exposição pública de imagem e contato com desconhecidos. A proteção integral exige gradação, e não tutela indiferenciada (BRASIL, 1990a; UNITED NATIONS, 2021).

O dever geral de cuidado deve ser lido como dever jurídico concretizável, e não como apelo moral. Para ter utilidade dogmática, ele precisa ser traduzido em comportamentos verificáveis: avaliação prévia de risco, canal de denúncia compreensível, tempo de resposta proporcional, limitação de contato abusivo, linguagem adequada e documentação da medida adotada. A responsabilidade civil só se estrutura quando se identifica qual desses deveres foi omitido ou cumprido de forma insuficiente diante do risco apresentado (BRASIL, 2025a; FRAZÃO, 2021).

Outra questão prática é a personalização de conteúdo sensível. Plataformas podem usar sinais de comportamento para recomendar vídeos, comunidades ou anúncios, mas devem ter cautela quando tais sinais revelam sofrimento psíquico, isolamento, busca por temas autolesivos ou exposição sexualizada. A resposta adequada não precisa ser idêntica em todos os casos; pode envolver redução de recomendação, oferta de canais de ajuda, limitação de publicidade ou revisão humana. O ponto é que o conhecimento inferido pela própria plataforma aumenta sua responsabilidade de governança (LIVINGSTONE; STOILOVA; HOPWOOD, 2021; SAFERNET BRASIL, 2025).

O dever geral de cuidado não se confunde com obrigação de impedir todo dano. Seu conteúdo deve ser extraído da combinação entre a natureza do serviço, o público previsível, o grau de controle técnico, a gravidade do risco e o custo razoável das medidas preventivas. Em uma plataforma frequentada por menores, pode ser exigível oferecer canal de denúncia acessível, resposta compatível com a urgência, configurações protetivas e informação clara. Em serviço de pequena escala ou com reduzida ingerência sobre conteúdo, a diligência poderá assumir forma distinta. A proporcionalidade impede tanto a imunidade ampla quanto a imposição de dever impossível (FRAZÃO, 2021; BRASIL, 2025a).

A condição peculiar de desenvolvimento modifica o padrão de diligência porque certas funcionalidades produzem efeitos diferentes sobre adultos e menores. Linguagem persuasiva, recompensas intermitentes, notificações insistentes e exposição pública por padrão podem ser compreendidas de maneira limitada por crianças ou adolescentes. O fornecedor que projeta o serviço para ampla utilização deve avaliar essas diferenças antes de lançar ou alterar funcionalidades relevantes. O melhor interesse da criança, nessa perspectiva, não funciona como slogan, mas como critério para escolher entre soluções técnicas igualmente viáveis aquela que reduz riscos sem excluir participação digital legítima (UNITED NATIONS, 2021; ICO, 2022).

A concretização do dever de cuidado depende ainda de documentação. Políticas internas, avaliações de risco, registros de treinamento, fluxos de atendimento e critérios de priorização permitem verificar se a proteção existia apenas no discurso institucional ou se foi incorporada à operação. A ausência de documentação não gera, isoladamente, responsabilidade, mas pode enfraquecer a alegação de diligência quando a empresa detém controle exclusivo sobre as informações relevantes. Em contrapartida, registros consistentes de prevenção e resposta podem demonstrar que o dano decorreu de evento imprevisível ou de conduta externa que não poderia ser razoavelmente evitada (BRASIL, 2025a; FRAZÃO, 2021).

A monetização por dados também exige leitura integrada com a proteção do consumidor. Quando a plataforma oferece uma experiência gratuita, mas condicionada à coleta massiva de informações e à exposição a publicidade, o custo do serviço aparece de modo indireto. Para menores, essa forma de remuneração é menos perceptível e torna mais difícil avaliar consequências futuras. A responsabilidade civil pode reconhecer que a transparência econômica do serviço

integra o dever de cuidado, sobretudo quando escolhas de *design* incentivam permanência e compartilhamento sem compreensão suficiente (BRASIL, 1990b; DONEDA, 2020).

O dever de cuidado precisa ser concretizado segundo classes de risco. Riscos de contato envolvem aliciamento, assédio e aproximação por desconhecidos; riscos de conteúdo abrangem materiais violentos, sexuais ou autolesivos; riscos de conduta incluem humilhação, desafios perigosos e compartilhamento indevido; riscos contratuais decorrem de publicidade, compras e exploração de dados. A distinção ajuda a selecionar medidas adequadas e evita políticas genéricas que tratem problemas diferentes com a mesma resposta (LIVINGSTONE; STOILOVA; HOPWOOD, 2021; OECD, 2021).

Em riscos de contato, ferramentas de bloqueio, limitação de mensagens e alertas sobre desconhecidos podem ser prioritárias. Em riscos de conteúdo, recomendação e classificação etária assumem maior importância. Em riscos contratuais, transparência, consentimento e restrição de publicidade ganham centralidade. A diligência esperada não é catálogo fixo; resulta da relação entre funcionalidade, frequência, gravidade e capacidade técnica.

A participação de familiares não exonera a plataforma de deveres próprios. Pais e responsáveis possuem papel educativo e de mediação, mas não controlam algoritmos, publicidade ou tratamento de dados. Transferir integralmente a eles a prevenção desconsidera a assimetria técnica. Em sentido inverso, a existência de dever empresarial não elimina a importância de orientação familiar. O modelo adequado é de corresponsabilidade, com obrigações diferenciadas conforme capacidade de intervenção.

O dever de cuidado também inclui acessibilidade. Canais de denúncia complexos, informações jurídicas extensas ou respostas em linguagem incompreensível reduzem efetividade para menores. A comunicação deve considerar idade, deficiência, idioma e contexto. Medidas formais que não possam ser usadas pelo público protegido não satisfazem integralmente a obrigação, sobretudo quando a empresa apresenta o canal como principal mecanismo de segurança.

A avaliação judicial do cuidado deve evitar retrospectiva perfeita. O fato de o dano ter ocorrido não prova, sozinho, inadequação de todas as medidas. O parâmetro é o que poderia ser razoavelmente exigido antes do evento, considerando conhecimento disponível e práticas do setor. Essa análise preserva inovação e, ao

mesmo tempo, impede que riscos conhecidos sejam tratados como inevitáveis apenas porque envolvem tecnologia complexa.

2.4 Âmbito de aplicação da Lei nº 15.211/2025 e acesso provável por menores

O âmbito de aplicação da Lei nº 15.211/2025 deve ser interpretado a partir da finalidade protetiva do ECA Digital e da realidade de uso dos serviços. A proteção não pode depender apenas da declaração formal de que a plataforma é destinada a adultos, quando elementos concretos indicam acesso provável por crianças e adolescentes. Linguagem, *design*, conteúdos promovidos, comunidades, publicidade, funcionalidades e dados de audiência podem revelar que o serviço alcança público infantojuvenil de modo previsível (BRASIL, 2025a; FERNANDES, 2026).

A noção de acesso provável por menores impede que a proteção seja esvaziada por escolhas contratuais unilaterais. Se o fornecedor conhece ou deveria conhecer que seu ambiente é utilizado por adolescentes, deve avaliar riscos compatíveis com esse público. Esse conhecimento pode decorrer de dados de cadastro, métricas internas, denúncias, padrões de consumo, apelo visual, influenciadores, jogos, desafios, vídeos curtos e publicidade dirigida. O critério é a previsibilidade concreta, não a intenção declarada pela plataforma (ICO, 2022; EUROPEAN COMMISSION, 2025).

A aplicação do ECA Digital deve variar conforme a intensidade do vínculo entre serviço e público menor. Serviços diretamente dirigidos a crianças exigem salvaguardas mais evidentes. Serviços não dirigidos, mas amplamente acessados por adolescentes, exigem avaliação proporcional de riscos. Já ambientes sem sinal razoável de acesso por menores podem estar sujeitos a deveres menos intensos. Essa gradação evita tanto a omissão protetiva quanto a imposição de deveres impossíveis ou desproporcionais.

A aferição de acesso provável também tem impacto probatório. A plataforma possui melhores condições de apresentar métricas de uso, perfis etários estimados, relatórios de segurança e medidas adotadas para restringir ou adaptar funcionalidades. Se a empresa explora dados para fins de publicidade, recomendação ou personalização, não parece coerente alegar desconhecimento absoluto sobre a presença relevante de menores quando essa presença era detectável por seus próprios sistemas (DONEDA, 2020; ROSA; PIN, 2022).

O acesso provável por menores não autoriza coleta indiscriminada de dados de idade. A proteção deve ser conciliada com privacidade, minimização de dados e proporcionalidade. A exigência jurídica é que a plataforma escolha métodos adequados ao risco: em alguns casos, basta linguagem apropriada e padrões de privacidade; em outros, pode ser necessária aferição de idade mais robusta, controle de publicidade ou limitação de funcionalidades. O critério deve ser calibrado pelo risco e pelo impacto sobre direitos fundamentais (BRASIL, 2018; UNITED NATIONS, 2021).

A delimitação do âmbito de aplicação é decisiva para a responsabilidade civil. Só faz sentido exigir dever proativo específico quando houver relação entre o serviço, o acesso provável por menores e o risco que se concretizou. Se a presença de menores era imprevisível e o evento decorreu exclusivamente de terceiro sem falha da plataforma, a imputação perde força. Se, ao contrário, o serviço conhecia a presença de menores e deixou de adotar salvaguardas compatíveis, a análise objetiva ganha fundamento.

A Lei nº 15.211/2025, portanto, deve ser aplicada de modo funcional. O julgador deve observar quem era o público provável, qual risco era previsível, que medida estava tecnicamente disponível, qual dever foi descumprido e como esse descumprimento contribuiu para o dano. Essa metodologia permite concretizar a proteção infantojuvenil sem transformar o ECA Digital em cláusula geral ilimitada de responsabilização.

Também é necessário evitar aplicação indiscriminada. Acesso eventual por menor não basta, por si só, para impor a todos os serviços o mesmo padrão de diligência. O critério deve combinar probabilidade de uso, escala, finalidade econômica, sensibilidade dos dados, possibilidade de contato com terceiros e intensidade do controle da plataforma sobre visibilidade e recomendação. Assim, o ECA Digital funciona melhor como microssistema de deveres graduados do que como gatilho automático de responsabilidade civil (BRASIL, 2025a; ICO, 2022).

A noção de acesso provável impede que a incidência da Lei nº 15.211/2025 dependa apenas de declaração formal do fornecedor. Um serviço pode afirmar que não se dirige a menores e, ainda assim, usar linguagem, estética, influenciadores, mecânicas de jogo, músicas, desafios ou recompensas que atraem esse público. Nessa hipótese, a análise deve observar dados de uso, desenho da interface e padrões de interação. A proteção jurídica não se prende ao rótulo comercial do

produto, mas à realidade de sua circulação social (BRASIL, 2025a; COMITÊ GESTOR DA INTERNET NO BRASIL, 2026).

A análise judicial deve reconstruir o caminho entre público provável, funcionalidade e dano. Não basta afirmar que adolescentes usam a internet de modo intenso; é necessário mostrar que aquele serviço, naquela configuração, alcançava menores e que a funcionalidade discutida contribuiu para o risco. Esse método torna a aplicação do ECA Digital mais precisa e reduz o perigo de decisões baseadas apenas em preocupação social genérica.

Do ponto de vista da responsabilidade civil, o acesso provável vincula dever e causalidade. A plataforma só pode ser cobrada por deveres especiais quando havia base concreta para reconhecer que menores seriam alcançados. Se essa base existia e o risco era previsível, a omissão passa a ser juridicamente mais relevante. Se a presença de menor era excepcional e imprevisível, a imputação objetiva perde força. Essa distinção preserva segurança jurídica e evita leitura ilimitada do microssistema.

A aferição de acesso não autoriza coleta desnecessária de documentos, biometria ou dados sensíveis. O desafio é equilibrar proteção e minimização de dados. A plataforma deve escolher métodos compatíveis com a gravidade do risco: em alguns casos, configurações protetivas e linguagem adequada bastam; em outros, controles mais robustos podem ser justificados. O ponto central é que a solução de idade não pode criar dano adicional à privacidade que pretendia proteger (BRASIL, 2018; ROSA; PIN, 2022).

A aplicação da Lei nº 15.211/2025 deve ser graduada. Serviços claramente voltados ao público infantil exigem proteção reforçada desde a concepção. Serviços de uso geral, mas com presença expressiva de adolescentes, demandam medidas proporcionais ao risco. Ambientes especializados sem sinal razoável de acesso por menores podem ter deveres menos intensos. Essa gradação evita tanto a irresponsabilidade por formalismo quanto a imposição uniforme de obrigações excessivas (BRASIL, 2025a; UNITED NATIONS, 2021).

O acesso provável pode ser demonstrado por múltiplos indicadores. Conteúdos com apelo juvenil, desafios virais, influenciadores populares entre adolescentes, jogos com interação social, vídeos curtos, compras internas e publicidade visualmente dirigida a menores podem funcionar como sinais. A plataforma que explora dados e métricas para direcionar publicidade ou recomendar conteúdo dificilmente pode alegar desconhecimento absoluto sobre o perfil aproximado de seu público. Essa contradição

é relevante para avaliar previsibilidade (COMITÊ GESTOR DA INTERNET NO BRASIL, 2026; DONEDA, 2020).

A noção de acesso provável por menores é uma das chaves de aplicação do ECA Digital. Ela impede que o fornecedor se proteja apenas por declaração formal de público adulto quando o próprio desenho do serviço, a linguagem, o conteúdo promovido, a estética ou as métricas de uso revelam presença relevante de adolescentes. A incidência do regime especial deve olhar para a realidade da circulação social do serviço, e não somente para sua classificação contratual (BRASIL, 2025a; ICO, 2022).

Em termos de aplicação prática, o juiz deve evitar decisões baseadas apenas na faixa etária declarada nos termos de uso. Deve investigar se havia evidências de uso por menores, se a plataforma tinha instrumentos para reconhecer esse uso e se adotou salvaguardas compatíveis. A prova pode incluir relatórios internos, estatísticas públicas, campanhas de marketing, linguagem do aplicativo, presença de conteúdos infantojuvenis e registros de denúncias envolvendo menores (COMITÊ GESTOR DA INTERNET NO BRASIL, 2026; BRASIL, 2025a).

A ideia de acesso provável impede que a incidência da lei dependa exclusivamente da classificação formal indicada nos termos de uso. Um serviço pode declarar-se destinado a adultos e, ao mesmo tempo, empregar linguagem, estética, publicidade ou funcionalidades que atraem público infantojuvenil. A análise deve considerar dados de utilização, campanhas promocionais, categorias de conteúdo, mecanismos de cadastro e conhecimento efetivo da composição do público. A proteção seria esvaziada se bastasse inserir uma cláusula etária sem adotar medidas coerentes para reduzir o uso previsível por menores ou adequar a experiência à presença desse grupo (BRASIL, 2025a; EUROPEAN COMMISSION, 2025).

O critério de probabilidade precisa ser aplicado com prudência. Não se exige certeza de que cada usuário seja menor, tampouco vigilância invasiva sobre toda pessoa conectada. O que se busca é avaliar se a plataforma possuía sinais objetivos e suficientes de acesso infantojuvenil e se respondeu a eles de maneira proporcional. Número expressivo de perfis jovens, conteúdos voltados a estudantes, linguagem infantilizada, presença de jogos e recursos de interação podem compor esse quadro. A conclusão deve resultar do conjunto de indícios, e não de presunção automática fundada na mera popularidade do serviço (ICO, 2022; BRASIL, 2025a).

A abrangência material do ECA Digital também deve ser definida pela função exercida pela plataforma. Serviços de recomendação, publicidade, mensageria, jogos, vídeo e compartilhamento de imagens apresentam riscos distintos. Por isso, a incidência da lei não conduz a um catálogo uniforme de obrigações. O dever relevante pode ser limitar perfilamento, aprimorar denúncia, restringir contato de desconhecidos, ajustar privacidade inicial ou oferecer informação adequada. Essa leitura funcional aproxima a norma da realidade tecnológica e evita que empresas muito diferentes sejam avaliadas por um padrão indiferenciado de diligência (FUNDAÇÃO GETULIO VARGAS, 2025; INSTITUTO ALANA, 2026).

A análise de acesso provável também deve considerar o comportamento esperado das famílias. Nem sempre os responsáveis conseguem supervisionar todas as interações digitais, especialmente em plataformas de uso contínuo e interfaces desenhadas para permanência. A existência de controle parental pode ser relevante, mas não exonera a plataforma de deveres próprios quando ela estrutura o ambiente, coleta dados e conhece padrões de uso. O dever jurídico deve ser distribuído conforme capacidade real de prevenção de cada agente.

O acesso provável não se confunde com mera possibilidade abstrata. A incidência reforçada deve apoiar-se em sinais objetivos, como linguagem, temas, personagens, presença em lojas classificadas para adolescentes, campanhas de marketing, estatísticas de uso e facilidade de cadastro. A plataforma não pode ser considerada infantil apenas porque qualquer menor poderia acessá-la, mas também não pode afastar a lei por declaração formal incompatível com a realidade do público.

A aferição deve ser periódica. Serviços mudam funcionalidades, adquirem novos usuários e alteram campanhas. Uma plataforma inicialmente voltada a adultos pode tornar-se popular entre adolescentes. O dever de revisão impede que classificação histórica seja usada indefinidamente. Métricas agregadas e pesquisas de audiência podem revelar mudança sem exigir identificação individual de todos os usuários.

A gradação etária é necessária porque infância e adolescência não formam grupo homogêneo. Medidas adequadas a crianças pequenas podem ser excessivas para adolescentes mais velhos, cuja autonomia progressiva merece respeito. O design deve oferecer níveis de proteção, explicações e controles compatíveis com desenvolvimento. Essa gradação também melhora proporcionalidade de aferição etária e reduz coleta desnecessária de documentos.

Em serviços de alto risco, a simples autodeclaração pode ser insuficiente. Em serviços de baixo risco, exigir documento oficial pode ser desproporcional. Entre esses extremos existem estimativas de idade, confirmação parental, sinais comportamentais e verificações por terceiros. Cada mecanismo possui margens de erro, riscos de exclusão e impactos sobre privacidade. A escolha deve ser documentada e revisada conforme evidências de efetividade.

A falsidade deliberada do usuário pode funcionar como elemento de excludente, mas não automaticamente. Se o serviço foi desenhado para atrair menores, possui ampla presença infantil e utiliza apenas campo de data de nascimento facilmente contornável, a declaração falsa não rompe por completo o nexo. A análise deve considerar se a plataforma adotou barreiras compatíveis com o risco e se a conduta do usuário foi realmente exclusiva.

2.5 *Safety by design*, aferição de idade e privacidade por padrão

Safety by design representa a ideia de que segurança e proteção de menores devem integrar a concepção e a operação do serviço, e não apenas aparecer como resposta posterior ao dano. Em plataformas digitais, isso envolve avaliar riscos antes da oferta ou alteração de funcionalidades, adaptar padrões de privacidade, reduzir incentivos nocivos, facilitar denúncias e documentar respostas. A prevenção deixa de ser recomendação abstrata e passa a ser critério de diligência (ICO, 2022; BRASIL, 2025a).

A proteção por desenho não exige tecnologia perfeita. Ela exige que a plataforma demonstre planejamento proporcional ao risco que conhece ou deveria conhecer. Em serviços com grande presença de adolescentes, por exemplo, recomendações automatizadas, publicidade, interação com desconhecidos e exposição de imagem devem ser examinadas previamente. A ausência de avaliação mínima pode revelar falha organizacional quando o dano se relaciona a risco previsível e administrável (EUROPEAN COMMISSION, 2025).

A aferição de idade deve ser tratada com cautela. Métodos excessivamente invasivos podem ampliar coleta de dados pessoais e criar novos riscos à privacidade. Métodos frágeis, por outro lado, podem tornar ineficaz a proteção. O desafio jurídico é exigir mecanismos proporcionais, adequados ao tipo de serviço e ao risco envolvido, sem transformar a proteção de menores em vigilância generalizada. A LGPD e o

princípio da minimização de dados são essenciais nessa calibragem (BRASIL, 2018; ROSA; PIN, 2022).

A privacidade por padrão é especialmente importante porque crianças e adolescentes podem não compreender plenamente as consequências de exposição pública, compartilhamento de localização, perfilamento ou publicidade comportamental. Configurações iniciais mais protetivas, linguagem clara e limitação de coleta desnecessária reduzem a transferência indevida de riscos ao usuário vulnerável. Tais medidas também facilitam a avaliação posterior de diligência da plataforma (UNITED NATIONS, 2021; DONEDA, 2020).

A responsabilidade civil surge quando a falha de desenho se relaciona com o dano. Um padrão de conta pública para menores, a recomendação insistente de conteúdos inadequados, a ausência de canal de denúncia acessível ou a falta de resposta documentada podem revelar descumprimento de dever proativo. Contudo, a imputação exige demonstrar que a medida omitida era exigível, tecnicamente possível e relacionada ao resultado lesivo (TEPEDINO; TERRA; GUEDES, 2024).

O direito comparado é útil nesse tópico porque oferece exemplos de operacionalização. *Age Appropriate Design Code*, *Digital Services Act* e *Online Safety Act* indicam formas de avaliação de risco, transparência e deveres de mitigação. A dissertação utiliza esses parâmetros apenas como apoio interpretativo, pois a obrigação concreta deve ser extraída do direito brasileiro, especialmente da Constituição, ECA, LGPD, Marco Civil e ECA Digital (UNIÃO EUROPEIA, 2022; UNITED KINGDOM, 2023).

A lógica de *safety by design* também reforça a dimensão preventiva da responsabilidade civil. Se o serviço tem meios razoáveis para reduzir risco previsível antes que o dano ocorra, a análise não pode ficar limitada à indenização posterior. Medidas preventivas e inibitórias tornam-se relevantes, sobretudo quando a falha decorre de desenho sistêmico e pode atingir número indeterminado de menores (BRASIL, 1985; BRASIL, 1990b).

Nessa linha, *safety by design*, aferição de idade e privacidade por padrão funcionam como critérios para verificar a qualidade da organização do serviço. Eles não produzem responsabilidade automática, mas ajudam a demonstrar se a plataforma atuou de modo diligente diante de público vulnerável e risco previsível.

A aferição de idade exige cuidado adicional. Soluções intrusivas podem gerar coleta excessiva de dados biométricos ou documentos, o que contraria a própria

finalidade protetiva. A técnica adequada deve ser proporcional ao risco do serviço: em alguns casos bastam configurações por padrão e autodeclaração acompanhada de sinais de uso; em outros, pode haver necessidade de método mais robusto, desde que minimizado, transparente e auditável. O critério civil relevante é verificar se a plataforma escolheu solução compatível com o risco que ela própria criou ou explorou (BRASIL, 2018; FERNANDES; TEFFÉ; BRANCO, 2024).

Safety by design significa deslocar a proteção para o desenho do produto. Em vez de depender exclusivamente da reação da família ou da ordem judicial posterior, a plataforma deve incorporar salvaguardas desde a configuração do serviço. Isso inclui padrões de privacidade mais restritivos para menores, limitação de contato indesejado, interfaces menos persuasivas, redução de recomendação nociva e avisos adequados à idade. A responsabilidade civil se conecta a esse ponto quando o dano revela falha previsível em uma decisão de desenho que estava sob controle do fornecedor (ICO, 2022; BRASIL, 2025a).

A vinculação entre *safety by design* e responsabilidade civil depende de nexo. Uma plataforma não responde simplesmente porque poderia ter desenhado o serviço de modo diferente. Responde quando a alternativa omitida era razoável, compatível com o risco e relacionada ao dano sofrido. Essa exigência impede decisões retrospectivas excessivas, nas quais toda lesão seria vista como prova automática de defeito do serviço. A análise deve considerar tecnologia disponível, custo proporcional, gravidade do risco e efeito sobre outros direitos.

O direito comparado contribui porque mostra que proteção por desenho não é exigência vaga. O *Age Appropriate Design Code*, o *Digital Services Act* e o *Online Safety Act* trabalham com avaliação de risco, mitigação, transparência e deveres documentados. Esses modelos não substituem a legislação brasileira, mas confirmam que o dever preventivo pode ser operacionalizado por rotinas internas verificáveis. A utilidade comparada está em oferecer método, não fundamento autônomo de condenação (UNIÃO EUROPEIA, 2022; UNITED KINGDOM, 2023).

A ausência de desenho seguro pode ser avaliada como falha organizacional quando o dano decorre de risco previsível. Por exemplo, a configuração pública por padrão de perfil de menor, associada a contato aberto com desconhecidos e resposta tardia a denúncia, pode demonstrar encadeamento entre desenho, vulnerabilidade e dano. A responsabilidade, nesse caso, não se funda na existência abstrata de

tecnologia, mas na omissão de salvaguardas razoáveis diante de risco conhecido (FRAZÃO, 2021; SCHREIBER, 2015).

A aferição de idade deve ser calibrada por risco. Em ambiente de baixo risco, técnicas menos intrusivas podem ser suficientes. Em funcionalidades de maior impacto, como contato com desconhecidos, publicidade comportamental sensível, compras internas ou recomendação de conteúdo potencialmente prejudicial, mecanismos adicionais podem ser necessários. O critério não é a coleta máxima de dados, mas a escolha menos invasiva capaz de produzir proteção efetiva (ROSA; PIN, 2022; FERNANDES; TEFFÉ; BRANCO, 2024).

A privacidade por padrão tem importância especial em serviços frequentados por crianças e adolescentes. Configurações iniciais públicas, geolocalização visível, perfilamento amplo e compartilhamento facilitado de imagem podem transferir ao usuário vulnerável uma carga decisória que ele não está preparado para assumir. A proteção adequada consiste em inverter o padrão: deixar a opção mais segura como configuração inicial e exigir escolha consciente para ampliar exposição, sempre com linguagem compreensível (BRASIL, 2018; UNITED NATIONS, 2021).

Safety by design exige incorporar proteção no desenho do serviço. Em vez de esperar a consumação do dano, a plataforma deve avaliar previamente se suas funcionalidades de recomendação, contato, publicidade, exposição de imagem ou coleta de dados podem afetar menores. Essa avaliação não precisa eliminar todo risco, mas deve produzir escolhas documentáveis: padrões de privacidade, limites de interação, canais de denúncia, avisos adequados à idade e revisão de funcionalidades de maior impacto (ICO, 2022; BRASIL, 2025a).

A privacidade por padrão deve dialogar com a experiência concreta do usuário. Uma configuração pode ser tecnicamente protetiva, mas ineficaz se o fluxo de cadastro induz o menor a ampliar exposição sem compreensão. Padrões escuros, botões destacados para compartilhamento e linguagem ambígua podem enfraquecer a proteção formal. O dever de cuidado exige observar não apenas a regra escrita, mas a jornada real de uso, especialmente quando a interface é desenhada para maximizar interação (COHEN, 2019; BRASIL, 2018).

A proteção por desenho exige que a segurança seja considerada no momento de criação da funcionalidade, e não apenas depois da ocorrência de danos. Isso envolve revisar configurações iniciais, visibilidade de perfis, possibilidade de contato por desconhecidos, localização, compartilhamento de imagens e coleta de dados. O

ponto não é eliminar escolhas do usuário, mas evitar que a opção mais invasiva ou arriscada seja adotada automaticamente por pessoas que talvez não compreendam suas consequências. Configurações protetivas por padrão preservam autonomia progressiva porque permitem alteração consciente, ao mesmo tempo que reduzem exposição involuntária (ICO, 2022; FERNANDES; TEFFÉ; BRANCO, 2024).

A aferição de idade apresenta tensão particular entre proteção e privacidade. Métodos muito frágeis podem ser facilmente contornados; métodos excessivamente intrusivos podem exigir documentos, biometria ou tratamento adicional de dados sensíveis. A solução juridicamente adequada deve observar necessidade, adequação, minimização e segurança. Em alguns serviços, autodeclaração associada a sinais de uso e controles graduais pode ser suficiente; em outros, a gravidade do risco poderá justificar verificação mais robusta. A escolha precisa ser fundamentada e compatível com a LGPD, evitando que a proteção da infância produza coleta desnecessária (BRASIL, 2018; BRASIL, 2022; BRASIL, 2023).

Também integram a proteção por desenho os chamados padrões manipulativos de interface. Botões visualmente assimétricos, caminhos complexos para recusar publicidade, estímulos repetidos ao compartilhamento e recompensas por exposição pública podem reduzir a liberdade real de escolha. Quando direcionados a menores, esses mecanismos devem ser avaliados à luz da vulnerabilidade cognitiva e informacional. A responsabilidade civil não decorre de qualquer técnica de *design* persuasivo, mas pode surgir quando a arquitetura dificulta deliberadamente a opção segura, amplia risco conhecido e contraria deveres de informação, privacidade ou melhor interesse (MIRAGEM, 2019; BENJAMIN; MARQUES; BESSA, 2022).

A proteção por desenho também deve ser documentada. Não basta afirmar que a plataforma possui política de segurança; é necessário demonstrar como a política se traduz em fluxos de produto, testes, respostas e revisões. Relatórios de avaliação de risco, registros de incidentes, critérios de redução de alcance e histórico de ajustes podem ser decisivos para demonstrar diligência. Em sua ausência, a alegação de cuidado permanece abstrata e perde força probatória diante de danos previsíveis.

O *safety by design* começa na definição de requisitos do produto. Equipes jurídicas, técnicas e de experiência do usuário devem identificar riscos antes do lançamento, e não somente após incidentes. A documentação dessa etapa permite verificar se o melhor interesse foi considerado e quais alternativas foram descartadas.

A ausência de qualquer avaliação em serviço amplamente usado por menores pode revelar falha de governança, especialmente quando o risco era conhecido no setor.

Padrões de privacidade devem reduzir exposição inicial. Perfis de menores não deveriam tornar localização, contatos ou histórico visíveis sem escolha informada. Configurações protetivas por padrão não impedem autonomia, pois podem ser ajustadas conforme idade e contexto, mas evitam que a opção mais perigosa seja imposta a quem ainda não compreende suas consequências. Essa lógica está presente na LGPD e nos referenciais comparados (BRASIL, 2018; ICO, 2022).

O desenho também deve evitar padrões manipulativos. Contagens regressivas, recompensas aleatórias, notificações insistentes e obstáculos para encerrar sessão podem explorar impulsividade. Nem toda técnica de engajamento é ilícita, mas sua combinação com público infantil e coleta intensiva de dados exige avaliação. A responsabilidade dependerá de demonstração de risco e dano, não da simples presença de elementos lúdicos.

A aferição etária deve ser acompanhada de minimização. Solicitar documento, biometria ou imagem facial para todo serviço pode criar base de dados mais perigosa do que o risco que se pretendia reduzir. Alternativas menos invasivas devem ser preferidas quando suficientes. Se a verificação envolver terceiro, contratos e auditorias precisam assegurar finalidade limitada, segurança e eliminação dos dados após a conclusão.

Além da privacidade, a segurança por desenho abrange resiliência contra invasões, sequestro de contas e exposição acidental. Crianças podem reutilizar senhas, compartilhar dispositivos ou aceitar contatos sem avaliar riscos. Autenticação adaptada, alertas claros e recuperação segura podem reduzir danos. A falha civil deve ser examinada conforme padrões técnicos disponíveis e gravidade previsível, sem presumir invulnerabilidade absoluta.

2.6 Obrigações proativas, deveres de resposta e proteção de dados

As obrigações proativas do ECA Digital deslocam o foco da simples reação posterior para a organização anterior do serviço. A plataforma deve avaliar riscos, estruturar canais de denúncia, documentar respostas, adotar padrões de privacidade, limitar práticas incompatíveis com a idade provável do usuário e fornecer informação compreensível. Esses deveres só têm relevância civil quando podem ser vinculados

a uma falha concreta e a um dano juridicamente reconhecível (BRASIL, 2025a; FRAZÃO, 2021).

O dever de resposta é um dos pontos centrais. Em danos digitais, o tempo de reação pode definir a extensão da lesão, pois conteúdos, imagens e interações se multiplicam rapidamente. Uma denúncia envolvendo menor, exposição íntima, assédio ou recomendação perigosa exige canais acessíveis, prazos razoáveis, rastreabilidade e comunicação adequada. A demora injustificada ou a ausência de documentação pode comprometer a defesa da plataforma e reforçar a inferência de falha (SAFERNET BRASIL, 2025).

A proteção de dados dialoga diretamente com a responsabilidade civil. Crianças e adolescentes são titulares de dados e sujeitos em desenvolvimento, o que exige cuidado especial com coleta, perfilamento, publicidade comportamental e compartilhamento. O tratamento de dados não deve ser analisado apenas como questão administrativa ou regulatória, pois pode compor a cadeia causal de danos ligados à exposição, manipulação comercial, discriminação ou perda de privacidade (BRASIL, 2018; DONEDA, 2020).

A obrigação proativa não deve ser confundida com monitoramento ilimitado. A plataforma deve adotar medidas proporcionais ao risco e compatíveis com liberdade de expressão, privacidade e devido processo. Em alguns contextos, a resposta adequada será remover ou reduzir alcance; em outros, preservar prova, comunicar responsáveis, ajustar recomendação, restringir publicidade ou revisar padrões de interface. O conteúdo do dever depende da funcionalidade e do risco concreto (BRASIL, 2014a; UNITED NATIONS, 2021).

A documentação é elemento decisivo. Se a plataforma afirma ter adotado medidas de prevenção e resposta, deve ser capaz de demonstrar políticas, registros, fluxos de atendimento e critérios aplicados. A ausência de documentação não gera responsabilidade automática, mas pode influenciar a distribuição do ônus da prova e a avaliação de causalidade quando o dano é plausível e os dados decisivos estavam sob controle do fornecedor (BRASIL, 2015a; MULHOLLAND, 2009).

A relação de consumo reforça deveres de transparência e segurança. Plataformas que oferecem serviços a menores ou os alcançam de modo previsível devem comunicar riscos de forma compreensível, evitar práticas abusivas e garantir mecanismos efetivos de resposta. Essa leitura não substitui o ECA Digital, mas o

complementa no diálogo das fontes, especialmente quando o serviço explora atenção, dados ou publicidade (MARQUES, 2012; MIRAGEM, 2019).

No plano coletivo, obrigações proativas podem justificar tutela inibitória e medidas estruturais. Se a falha não é isolada, mas decorre de política de *design*, ausência de canal adequado ou padrão reiterado de resposta insuficiente, a solução individual pode ser insuficiente. O direito civil contemporâneo admite que a responsabilidade também cumpra função preventiva e organizadora de riscos (ROSENVALD, 2017; BRASIL, 1985).

Nesse estágio da análise, verifica-se que deveres proativos, resposta e proteção de dados são o núcleo operacional do ECA Digital. Eles fornecem parâmetros para verificar se a plataforma atuou de modo compatível com a proteção integral. A partir deles, os capítulos seguintes poderão examinar fundamentos civis, tensão com o Marco Civil e critérios dogmáticos de imputação.

A proteção de dados acrescenta outro plano de análise. Dados de crianças e adolescentes não são apenas insumos comerciais; podem revelar hábitos, localização, interesses, fragilidades emocionais e padrões de consumo. O tratamento inadequado pode ampliar riscos de perfilamento, publicidade exploratória e contato abusivo. Por isso, a responsabilização deve examinar finalidade, necessidade, transparência, retenção, compartilhamento e segurança das informações, articulando LGPD e ECA Digital sem reduzir o caso a simples política de privacidade (BRASIL, 2018; DONEDA, 2020).

A obrigação proativa não se esgota em publicar termos de uso. Ela exige procedimento real de prevenção e resposta: identificar riscos recorrentes, oferecer canal acessível de denúncia, preservar registros mínimos, responder em prazo compatível com a gravidade e revisar funcionalidades quando incidentes revelarem falhas sistêmicas. O descumprimento desses passos pode evidenciar defeito na prestação do serviço, especialmente quando a plataforma tinha conhecimento ou deveria ter conhecimento do padrão lesivo (BRASIL, 2025a; FRAZÃO, 2022).

A leitura conjunta de obrigações proativas, deveres de resposta e proteção de dados prepara a passagem para os fundamentos civil-constitucionais. O ponto comum é que a plataforma possui posição de controle sobre ambiente, informação e resposta. Essa posição não gera garantia universal, mas impõe dever de demonstrar diligência compatível com a vulnerabilidade do público e com a previsibilidade do risco.

No plano coletivo, obrigações proativas permitem superar a lógica de casos isolados. Falhas recorrentes de moderação, ausência de canal acessível, publicidade incompatível com idade ou sistema de recomendação perigoso podem exigir tutela inibitória ou obrigação de fazer. A função da responsabilidade civil não é apenas compensar vítimas passadas, mas reduzir repetição de risco quando a falha decorre da própria organização do serviço (BRASIL, 1985; ROSENVALD, 2017).

A documentação da resposta é elemento probatório indispensável. Se a plataforma recebeu alerta, denúncia ou sinal interno de risco, deve ser capaz de indicar quando tomou conhecimento, que setor avaliou a ocorrência, que medida foi adotada e por que determinada providência foi considerada suficiente. A falta de registro não equivale automaticamente à culpa, mas enfraquece a defesa quando o risco era grave e a informação estava sob controle do fornecedor (BRASIL, 2015a; MULHOLLAND, 2009).

A proteção de dados não é tema lateral. Dados de menores podem revelar hábitos, localização, interesses, fragilidades emocionais e padrões de consumo. Quando utilizados para personalização, publicidade ou recomendação, esses dados podem compor a cadeia de risco que antecede o dano. A análise civil deve verificar finalidade, necessidade, transparência, retenção, compartilhamento e segurança, em diálogo com a LGPD e com a proteção integral (BRASIL, 2018; DONEDA, 2020).

O dever de resposta deve ser medido pela gravidade e pela urgência. Denúncias de exposição íntima, contato abusivo, indução a autolesão, exploração comercial indevida ou tratamento inadequado de dados não podem receber o mesmo tratamento de reclamações comuns de usabilidade. A resposta precisa ser tempestiva, rastreável e compreensível para usuários e responsáveis. Quando a plataforma não demonstra o fluxo adotado, aumenta-se a dificuldade de afastar a inferência de falha (SAFERNET BRASIL, 2025).

Os deveres proativos podem ser compreendidos como um ciclo de governança. Antes do incidente, a plataforma deve identificar riscos, definir salvaguardas e treinar equipes; durante o funcionamento, precisa monitorar sinais relevantes sem vigilância indiscriminada; diante de denúncia, deve classificar urgência, preservar evidências e adotar medida proporcional; depois do evento, convém revisar procedimentos e documentar aprendizados. Essa sequência permite avaliar a diligência de modo concreto. A responsabilidade não se baseia na simples existência de política interna,

mas na correspondência entre o risco previsível e as medidas efetivamente incorporadas à operação (BRASIL, 2025a; BRASIL, 2026a).

O dever de resposta exige atenção à temporalidade. Em situações de exposição íntima, contato predatório ou ameaça grave, algumas horas podem alterar significativamente o alcance do dano. Em conflitos menos urgentes, resposta imediata pode ser tecnicamente desnecessária e até gerar remoções precipitadas. A plataforma deve possuir critérios de priorização transparentes, canais acessíveis e mecanismos de revisão. A demora será juridicamente relevante quando incompatível com a natureza do risco, com a ciência disponível e com a capacidade operacional do fornecedor, e não apenas porque a vítima desejava solução instantânea (BRASIL, 2025a; SAFERNET BRASIL, 2025).

A proteção de dados atravessa todas essas obrigações porque recomendação, publicidade e aferição etária dependem de informações pessoais. O tratamento de dados de menores deve respeitar finalidade, necessidade, segurança e melhor interesse, com linguagem compreensível e limites à reutilização. Dados coletados para verificar idade não podem ser automaticamente convertidos em insumo publicitário; registros de denúncia devem ser preservados pelo tempo necessário, mas protegidos contra acesso indevido. A integração entre ECA Digital e LGPD torna a governança de dados parte do próprio dever de cuidado das plataformas (BRASIL, 2018; MENDES; DONEDA, 2018; ROSA; PIN, 2022).

As obrigações proativas do ECA Digital têm natureza organizacional. Elas exigem que a plataforma pense o serviço antes do dano, durante a ocorrência do risco e depois do alerta recebido. Isso envolve prevenção, monitoramento proporcional, comunicação adequada, documentação e resposta. A responsabilidade civil objetiva aparece quando tais deveres deixam de ser simples orientação institucional e se conectam a uma falha concreta que contribuiu para dano a criança ou adolescente (BRASIL, 2025a; FRAZÃO, 2021).

A implementação institucional do ECA Digital depende da autoridade administrativa competente. O Decreto nº 12.622/2025 designou a Agência Nacional de Proteção de Dados como autoridade administrativa autônoma de proteção de crianças e adolescentes em ambientes digitais. A Lei nº 15.352/2026, resultante da conversão da medida provisória que reestruturou a ANPD, consolidou seu regime jurídico como agência reguladora, reforçando sua autonomia e sua capacidade de normatização e fiscalização. Para a responsabilidade civil, atos administrativos não

substituem a prova do dano e do nexo, mas podem esclarecer o conteúdo mínimo do dever objetivo e a previsibilidade da conduta empresarial (BRASIL, 2025d; BRASIL, 2026b).

A resposta a denúncias deve combinar triagem e escalonamento. Comunicações sobre risco imediato à vida, exploração sexual ou ameaça a escola exigem prioridade distinta de reclamações comuns. Sistemas automatizados podem auxiliar a classificação, mas decisões com elevado impacto devem admitir revisão humana. O tempo de resposta deve ser medido a partir da gravidade e da clareza do sinal, não por prazo uniforme para qualquer ocorrência.

A preservação de evidências integra o dever proativo. Remover conteúdo sem conservar registros mínimos pode inviabilizar investigação e reparação. A plataforma deve equilibrar retenção, privacidade e obrigação legal, preservando identificadores, horários, histórico de moderação e dados de alcance pelo período necessário. A medida é especialmente importante quando a vítima é menor e pode demorar a relatar o ocorrido.

A transparência dos canais de resposta deve incluir informação sobre recebimento, decisão e possibilidade de recurso. Respostas automáticas genéricas geram insegurança e dificultam controle. Não se exige revelar detalhes que facilitem evasão de sistemas, mas é necessário oferecer justificativa compreensível. A ausência de explicação pode agravar dano e impedir que a vítima adote outras providências.

Obrigações de proteção de dados devem ser integradas à moderação. Uma denúncia pode conter imagens íntimas, documentos ou informações de saúde. O canal precisa restringir acesso, criptografar transmissão e evitar reutilização para treinamento ou publicidade. O tratamento é legítimo quando necessário à proteção, mas permanece sujeito a finalidade, segurança e melhor interesse (BRASIL, 2018; ROSA; PIN, 2022).

A governança administrativa iniciada pelo Decreto nº 12.622/2025 e reforçada pela transformação da ANPD em agência reguladora oferece espaço para padrões setoriais, orientação técnica e fiscalização. A Agência pode articular proteção de dados e segurança digital por meio de regulamentos, guias e procedimentos de monitoramento. Esses instrumentos não geram indenização automática, mas constituem referências relevantes para avaliar o dever objetivo, desde que

compatíveis com a lei e aplicáveis ao período do fato (BRASIL, 2025d; BRASIL, 2026b).

A articulação entre dados pessoais e dever de resposta aparece em situações de perfilamento. Se a plataforma utiliza dados para recomendar, segmentar ou ranquear conteúdos, deve ser capaz de explicar, em termos acessíveis, como reduz riscos a menores. A proteção de dados não se limita ao consentimento; envolve finalidade, necessidade, minimização e segurança. Quando o tratamento informacional contribui para exposição indevida, a responsabilidade civil pode dialogar com a LGPD sem depender exclusivamente de sanção administrativa (BRASIL, 2018; DONEDA, 2020).

3 FUNDAMENTOS CIVIL-CONSTITUCIONAIS DA RESPONSABILIDADE DAS PLATAFORMAS

A Lei nº 15.211/2025 não opera de forma isolada. Seus deveres adquirem sentido quando articulados à prioridade absoluta, à dignidade da pessoa humana, aos direitos da personalidade e à função social da responsabilidade civil. A reconstrução civil-constitucional proposta neste capítulo evita duas leituras igualmente insuficientes: reduzir o ECA Digital a um conjunto administrativo de obrigações técnicas ou transformá-lo em autorização genérica para indenizar. O objetivo é mostrar como valores constitucionais se convertem em pressupostos civis de imputação, preservadas a exigência de dano, de nexo e de identificação da falha própria do serviço (BRASIL, 1988; TEPEDINO; TERRA; GUEDES, 2024).

Sob o enfoque civil-constitucional, o bem jurídico afetado não se limita ao patrimônio ou à honra em sentido tradicional. Danos digitais infantojuvenis podem comprometer privacidade, identidade, autonomia progressiva, integridade psíquica e oportunidades futuras. Reconhecer essa pluralidade não dispensa prova. A centralidade da pessoa exige examinar a repercussão concreta da prática sobre o desenvolvimento, ao passo que a segurança jurídica impõe distinguir desconfortos ordinários, riscos socialmente toleráveis e lesões juridicamente relevantes (MORAES, 2003; MACHADO, 2003).

A diligência da plataforma inclui a qualidade da comunicação mantida com usuários e responsáveis. Em ocorrências envolvendo menores, devem existir informações compreensíveis sobre o recebimento da denúncia, a providência adotada e os meios de contestação ou complementação. A ausência de retorno pode prolongar a exposição, comprometer a preservação da prova e impedir atuação rápida da família. Transparência procedimental, portanto, não é cortesia empresarial, mas componente do dever de cuidado em ambiente de risco (BRASIL, 2025a; SAFERNET BRASIL, 2025).

3.1 Art. 227 da Constituição Federal e proteção integral

O art. 227 da Constituição Federal estabelece prioridade absoluta à criança e ao adolescente e vincula família, sociedade e Estado à proteção de direitos fundamentais. No ambiente digital, essa prioridade não deve ser lida como autorização para responsabilização automática, mas como parâmetro de interpretação dos deveres de cuidado. A proteção integral exige que a atividade

econômica digital seja compatibilizada com desenvolvimento, dignidade, privacidade, saúde e segurança de pessoas em formação (BRASIL, 1988; BRASIL, 1990a; GONÇALVES; LARA; SILVA, 2026).

A eficácia do art. 227 não se limita às políticas públicas estatais. Plataformas digitais de grande escala participam da organização de espaços sociais relevantes, especialmente quando regulam visibilidade, interação, publicidade, dados e permanência de conteúdos. Por isso, a prioridade constitucional pode irradiar efeitos sobre relações privadas, orientando a interpretação de deveres civis e consumeristas aplicáveis aos serviços digitais (MORAES, 2003; MARQUES, 2012).

Essa compreensão exige proporcionalidade. A proteção integral não impõe bloqueio indiscriminado de acesso, vigilância permanente ou censura genérica. O que se exige é que a plataforma, ao explorar serviço provavelmente acessado por menores, adote medidas compatíveis com o risco criado ou ampliado. A Constituição fornece o fundamento axiológico; a lei civil, o CDC, a LGPD, o Marco Civil e o ECA Digital fornecem os instrumentos de concretização (BRASIL, 2002; BRASIL, 2018; BRASIL, 2025a).

O art. 227 também reforça a dimensão preventiva da responsabilidade civil. Em danos digitais, a reparação posterior pode ser insuficiente, porque a exposição de imagem, a circulação de dados e a recomendação nociva podem gerar efeitos persistentes. A prioridade absoluta, nesse cenário, justifica maior atenção a deveres de prevenção, documentação e resposta, sem dispensar prova do dano e do nexo causal.

A contribuição do dispositivo constitucional para a construção aqui proposta é, portanto, dupla. Ele fundamenta a intensidade do cuidado diante de menores e impede que a vulnerabilidade seja tratada como dado secundário. Ao mesmo tempo, exige que a imputação continue juridicamente controlada, pois a proteção integral só se realiza de modo legítimo quando articulada a deveres concretos e verificáveis.

Sob essa leitura, evita tanto a privatização total da proteção quanto a neutralização da responsabilidade empresarial. A Constituição não autoriza transferir às plataformas todo dano que ocorre *online*, mas também não permite ignorar que serviços digitais de grande escala podem condicionar acesso a informação, consumo, imagem e sociabilidade. A prioridade absoluta opera como vetor de interpretação para definir intensidade do dever de segurança, urgência da resposta e relevância da prova técnica em cada caso.

O art. 227 da Constituição tem papel estruturante porque transforma a proteção infantojuvenil em prioridade constitucional, e não em escolha política eventual. Em ambiente digital, essa prioridade deve orientar a interpretação dos deveres privados quando a atividade econômica atinge diretamente pessoas em desenvolvimento. A plataforma não assume a função da família nem do Estado, mas integra a sociedade chamada a proteger crianças e adolescentes quando explora serviço com capacidade de organizar riscos relevantes (BRASIL, 1988; MACHADO, 2003).

A proteção integral ainda legitima medidas de caráter coletivo. Se determinada arquitetura de serviço expõe um grupo indeterminado de menores a risco previsível, a resposta não deve depender apenas de ações individuais posteriores. Tutelas inibitórias, ajustes de interface, transparência e deveres de documentação são instrumentos compatíveis com a prioridade absoluta, desde que proporcionais e vinculados a risco demonstrável (BRASIL, 1985; ROSENVALD, 2017).

A leitura constitucional também influencia a interpretação do Marco Civil da Internet. A liberdade de expressão e a proteção contra remoção arbitrária de conteúdos são valores relevantes, mas não podem ser isolados da prioridade constitucional de crianças e adolescentes. Quando a controvérsia envolve dever próprio de segurança, proteção de dados ou desenho de serviço, a análise constitucional deve ir além da simples tensão entre conteúdo de terceiro e ordem judicial específica (BRASIL, 2014a; BRASIL, 2025a).

O art. 227 não autoriza responsabilização automática. O dispositivo impõe finalidade protetiva, mas a imputação civil continua exigindo conduta atribuível, dano e nexo. Essa distinção é essencial para evitar que a prioridade absoluta seja usada como substituto da análise dogmática. A proteção constitucional deve reforçar o dever de prevenção, orientar a distribuição da prova e densificar o padrão de cuidado, mas não eliminar a necessidade de demonstrar a relação entre falha e dano (TEPEDINO; TERRA; GUEDES, 2024).

A prioridade absoluta também qualifica a noção de risco. Em atividades digitais, riscos toleráveis para adultos podem exigir cautelas adicionais quando o serviço alcança menores. Exposição pública, contato com desconhecidos, publicidade segmentada e recomendação insistente de conteúdo sensível devem ser avaliados segundo sua repercussão sobre sujeitos em formação. O risco da atividade não é abstrato; ele depende do público atingido e do modo como o serviço organiza a experiência (AZEVEDO; TORRES, 2023).

A proteção integral tem função estruturante na responsabilidade civil porque define a finalidade da tutela. Se o dano atinge pessoa em desenvolvimento, a resposta jurídica não pode limitar-se à reparação patrimonial tardia. É necessário considerar privacidade, imagem, reputação, saúde mental, autonomia progressiva e continuidade do desenvolvimento. Esses bens jurídicos justificam uma leitura preventiva e protetiva da responsabilidade, sem dispensar os elementos de imputação (BRASIL, 1990a; ROSENVALD, 2017).

O art. 227 da Constituição Federal não atua apenas como enunciado programático. Ele estabelece prioridade absoluta para crianças e adolescentes e orienta a interpretação de todo o sistema infraconstitucional. Em ambiente digital, essa prioridade exige que liberdade econômica, inovação, expressão e tratamento de dados sejam lidos à luz da condição peculiar de desenvolvimento. A consequência não é afastar outros direitos, mas organizar sua ponderação de modo a impedir que a vulnerabilidade infantojuvenil seja tratada como aspecto secundário (BRASIL, 1988; MACHADO, 2003).

Daí por que a Constituição não substitui a análise técnica das plataformas, mas orienta sua avaliação jurídica. O juiz deve perguntar de que modo determinada escolha de *design*, moderação, coleta de dados ou resposta afetou criança ou adolescente em sua condição peculiar de desenvolvimento. Essa pergunta constitucionaliza a análise do risco sem abandonar os pressupostos clássicos da responsabilidade civil.

A utilização do art. 227 como fundamento central exige cuidado metodológico. O dispositivo deve aparecer em diálogo com regras infraconstitucionais e com a dogmática da responsabilidade civil. Se for invocado sozinho, pode gerar fundamentação aberta demais. Se for ignorado, a análise perde a especialidade do sujeito protegido. A construção proposta adota a via intermediária: o art. 227 define finalidade e intensidade de cuidado, enquanto Código Civil, CDC, LGPD, Marco Civil e ECA Digital especificam deveres e limites.

A proteção integral também evita fragmentação do dano. Lesões digitais raramente atingem apenas um bem jurídico isolado. A exposição de imagem pode envolver honra, privacidade, dados, saúde mental e convivência escolar; uma publicidade exploratória pode afetar consumo, autonomia e formação de preferências. O art. 227 autoriza enxergar essa multiplicidade sem reduzir o caso a categoria

patrimonial estreita. A amplitude da proteção, contudo, deve vir acompanhada de prova suficiente do impacto.

No plano hermenêutico, o art. 227 funciona como vetor de interpretação. Diante de dúvida sobre o alcance de deveres de informação, segurança, privacidade ou resposta, a solução deve privilegiar a leitura que melhor proteja o desenvolvimento infantojuvenil sem anular outros direitos fundamentais. Essa operação não é preferência moral; decorre de comando constitucional expresso. O julgador deve fundamentar como esse vetor incide no caso concreto e quais limites preservam proporcionalidade.

A prioridade absoluta também influencia a leitura da boa-fé objetiva. Relações digitais envolvendo menores não podem ser tratadas como simples adesão contratual a termos extensos e abstratos. A Constituição impõe que fornecedores, Estado, família e sociedade compartilhem a tarefa de proteção, cada qual na medida de sua esfera de atuação. Assim, uma plataforma que organiza ambiente de interação deve ajustar sua conduta ao padrão constitucional reforçado, especialmente quando dispõe de meios técnicos para reduzir riscos previsíveis.

A proteção integral, por fim, não deve ser lida apenas como proteção contra danos. Ela também envolve promoção de desenvolvimento, participação e acesso seguro ao ambiente digital. Por isso, a resposta jurídica não deve simplesmente excluir crianças e adolescentes da internet, mas exigir que o ecossistema digital seja estruturado com salvaguardas compatíveis. A responsabilidade objetiva por violação de deveres proativos busca exatamente esse equilíbrio entre participação e proteção.

O art. 227 também ajuda a definir a gravidade da omissão. Em conflito comum entre adultos, certa demora ou falha de informação pode ter efeitos limitados; em dano digital envolvendo menor, a mesma falha pode ampliar exposição, constrangimento e vulnerabilidade. A prioridade constitucional atua como critério para medir urgência e adequação da resposta, especialmente em denúncias de violência, exploração, assédio ou divulgação de imagem.

A prioridade absoluta prevista no art. 227 produz efeitos sobre a interpretação e sobre a decisão. No plano interpretativo, orienta a escolha entre leituras possíveis das normas civis e digitais, favorecendo aquela que concretiza proteção sem suprimir direitos de participação. No plano decisório, exige que o julgador explicite como considerou idade, gravidade do risco, urgência e impacto sobre o desenvolvimento. A prioridade não elimina ponderação, mas impede que interesses econômicos ou

conveniências administrativas sejam tratados como equivalentes quando colidem com proteção básica de crianças e adolescentes (BRASIL, 1988; MACHADO, 2003).

A eficácia horizontal dos direitos fundamentais permite exigir diligência de agentes privados que estruturam espaços relevantes de convivência social. Plataformas não exercem função estatal, mas controlam regras de acesso, visibilidade, interação e coleta de dados capazes de afetar direitos da personalidade. Essa posição justifica deveres de proteção compatíveis com sua atividade. O fundamento constitucional, contudo, precisa ser mediado por normas civis e infraconstitucionais; não se responsabiliza diretamente com base em princípio abstrato, mas pela violação de dever concretizado no sistema jurídico (TEPEDINO; TERRA; GUEDES, 2024; FRAZÃO, 2021).

A proteção integral também inclui o direito de participar do ambiente digital. Medidas que simplesmente afastam menores da internet podem reduzir riscos imediatos, mas comprometer acesso à informação, educação, expressão e convivência. O art. 227 deve, portanto, sustentar soluções que combinem segurança e inclusão. Configurações apropriadas, linguagem acessível, controle progressivo e canais de ajuda tendem a ser mais compatíveis com a Constituição do que proibições indiscriminadas. Essa compreensão reforça o caráter qualitativo da diligência exigida das plataformas (UNITED NATIONS, 2021; BRASIL, 2024).

A prioridade absoluta também possui dimensão institucional. Ela exige que políticas privadas de plataformas sejam compatíveis com a relevância pública da proteção infantojuvenil, sobretudo quando a atividade empresarial alcança milhões de usuários. A Constituição não transforma empresas em Estado, mas impede que a organização econômica do ambiente digital ignore consequências previsíveis sobre menores. Essa leitura justifica exigir processos internos de avaliação e resposta sempre que a plataforma se beneficiar da escala de interação.

A prioridade constitucional deve ser interpretada em conjunto com a Convenção sobre os Direitos da Criança, promulgada no Brasil pelo Decreto nº 99.710/1990. O princípio do melhor interesse exige que decisões sobre serviços digitais considerem, de maneira demonstrável, os efeitos sobre pessoas em desenvolvimento. Não se trata de fórmula retórica capaz de afastar automaticamente outros direitos, mas de critério de decisão que obriga o fornecedor e o julgador a justificar por que determinada arquitetura, política de moderação ou prática de dados é compatível com a proteção da criança (BRASIL, 1990c; UNITED NATIONS, 2021).

3.2 Estatuto da Criança e do Adolescente e sujeito em desenvolvimento

O Estatuto da Criança e do Adolescente concretiza a proteção integral ao reconhecer crianças e adolescentes como sujeitos de direitos em condição peculiar de desenvolvimento. Essa condição é decisiva para a análise de ambientes digitais, porque o menor não interage com publicidade, recomendação, exposição de imagem e coleta de dados com o mesmo repertório crítico de um adulto (BRASIL, 1990a; MACHADO, 2003).

A ideia de sujeito em desenvolvimento não deve ser usada para negar autonomia. Ela orienta uma proteção compatível com a autonomia progressiva, na qual a criança e o adolescente participam da vida digital, mas com salvaguardas proporcionais à idade, à maturidade e ao risco. A dissertação não defende exclusão do ambiente online, e sim condições de participação mais seguras e transparentes (UNITED NATIONS, 2021).

O ECA fornece parâmetros relevantes para interpretar deveres de plataformas. A proteção contra exploração, negligência, violência, exposição indevida e práticas abusivas ganha novas formas no ambiente digital. Assédio, exposição de imagem, manipulação comercial, perfilamento e recomendação de conteúdo nocivo são manifestações contemporâneas de riscos que o Estatuto já buscava enfrentar em outros contextos.

A condição peculiar de desenvolvimento também altera a análise probatória. O menor e sua família podem identificar o resultado lesivo, mas raramente conseguem reconstruir a cadeia técnica que levou à exposição ou à recomendação. Por isso, a tutela de sujeitos em desenvolvimento deve considerar a assimetria informacional sem transformar vulnerabilidade em presunção absoluta de responsabilidade (MULHOLLAND, 2009; BRASIL, 2015a).

O ECA, lido em diálogo com o ECA Digital, reforça a necessidade de deveres preventivos. A plataforma não responde por qualquer evento *online*, mas deve justificar sua conduta quando o dano envolve risco previsível, público menor e funcionalidade sob sua esfera de organização. Essa leitura aproxima proteção integral e responsabilidade civil sem dissolver os limites de imputação.

No plano civil, a condição peculiar de desenvolvimento altera a avaliação da previsibilidade do dano. Um recurso de interação que para adultos representa mera conveniência pode, para menores, facilitar assédio, exposição indevida ou

manipulação comercial. O dever da plataforma é considerar essa diferença no desenho do serviço e na resposta a incidentes. A omissão só ganha relevância indenizatória quando a falha do serviço se vincula ao risco que o sistema protetivo buscava evitar.

O ECA contribui para a dissertação ao lembrar que a criança e o adolescente são sujeitos de direitos, não objetos passivos de tutela. Isso é relevante porque a proteção digital não pode significar exclusão da vida *online*. A noção de sujeito em desenvolvimento exige medidas capazes de preservar participação, expressão e aprendizagem, mas com salvaguardas adequadas à idade e à vulnerabilidade concreta. O equilíbrio entre autonomia e proteção é uma das bases da imputação objetiva aqui proposta (BRASIL, 1990a; MACIEL, 2024a).

A articulação entre ECA e ECA Digital permite deslocar o debate da reação individual para a governança do ambiente. O Estatuto fornece a categoria do sujeito em desenvolvimento; a Lei nº 15.211/2025 acrescenta deveres voltados ao contexto tecnológico. A responsabilidade civil utiliza ambas as fontes para definir padrão de cuidado e avaliar se o serviço adotou medidas compatíveis com a vulnerabilidade do usuário menor (BRASIL, 1990a; BRASIL, 2025a).

O sujeito em desenvolvimento demanda linguagem adequada. Termos de uso extensos e obscuros, políticas de dados técnicas e canais de denúncia complexos podem ser formalmente existentes, mas materialmente ineficazes para o público infantojuvenil. O dever de informação exige comunicação compatível com o destinatário, especialmente quando a plataforma utiliza design persuasivo, notificações e mecanismos de retenção direcionados à permanência do usuário (BRASIL, 1990b; MIRAGEM, 2019).

A autonomia progressiva deve ser considerada com equilíbrio. Proteger não significa impedir toda participação digital de adolescentes, especialmente porque a internet também é espaço de aprendizado, expressão e sociabilidade. O desafio é permitir participação em ambiente com riscos administráveis e informação adequada. Medidas excessivamente restritivas podem prejudicar acesso à cultura e à comunicação; medidas insuficientes transferem ao menor a carga de riscos que poderiam ser reduzidos pela plataforma (UNITED NATIONS, 2021).

O ECA também reforça a participação da família, da sociedade, do Estado e dos agentes econômicos na proteção. As plataformas digitais, quando estruturam ambientes massivos de interação, não substituem pais ou responsáveis, mas integram

o ecossistema de proteção. A responsabilidade parental não exclui o dever do fornecedor de oferecer mecanismos adequados de segurança, denúncia e privacidade quando o serviço alcança menores de modo previsível (BRASIL, 1990a; FRAZÃO, 2021).

A noção de desenvolvimento é central para medir o dano. Lesões digitais podem afetar autoestima, convivência, privacidade, reputação e capacidade de autodeterminação informacional. Muitas vezes, tais efeitos não se manifestam imediatamente como prejuízo econômico, mas como dano moral, dano à imagem, exposição indevida ou sofrimento psíquico. A responsabilidade civil precisa reconhecer essa especificidade sem transformar todo desconforto *online* em dano indenizável (MACIEL, 2024a; ROSSATO; LÉPORE; CUNHA, 2024).

O Estatuto da Criança e do Adolescente concretiza a proteção integral ao reconhecer crianças e adolescentes como sujeitos de direitos. Essa concepção impede que o menor seja visto apenas como destinatário passivo de cuidado familiar ou estatal. No ambiente digital, o sujeito em desenvolvimento também é usuário, consumidor, titular de dados, participante de redes e destinatário de conteúdos. Essa pluralidade reforça a necessidade de articular ECA, CDC, LGPD, Marco Civil e ECA Digital (BRASIL, 1990a; BRASIL, 1990b; BRASIL, 2018).

O diálogo entre ECA e ECA Digital permite atualizar a proteção sem romper com sua matriz. O novo estatuto digital não cria a proteção da infância; ele a desloca para um ambiente tecnológico específico. A base continua sendo a proteção integral e a prioridade absoluta, mas agora aplicada a recomendação automatizada, dados, interface, moderação e resposta. Essa continuidade fortalece o argumento de que a responsabilidade objetiva por violação de deveres proativos é desenvolvimento do sistema, não ruptura arbitrária.

O ECA também reforça a necessidade de linguagem compreensível. Crianças e adolescentes são titulares de direitos, mas nem sempre conseguem interpretar textos jurídicos complexos ou fluxos de consentimento digital. Plataformas que utilizam termos técnicos para práticas intensas de coleta de dados ou publicidade dirigida devem adaptar sua comunicação. A falta de informação adequada pode funcionar como falha autônoma ou como elemento que agrava outras falhas do serviço.

A atuação das plataformas deve ser analisada em conjunto com políticas públicas e atuação familiar, mas sem transferir integralmente o dever de prevenção

para responsáveis. Famílias nem sempre conhecem algoritmos, políticas de dados ou mecanismos de moderação. Quando a plataforma concentra conhecimento técnico e capacidade de intervenção, ela não pode reduzir sua obrigação a avisos genéricos. A corresponsabilidade prevista no sistema de proteção integral exige repartição realista de deveres.

A categoria de sujeito em desenvolvimento exige olhar temporal. Determinados danos digitais podem produzir efeitos futuros, inclusive sobre reputação, relações sociais e formação psíquica. Uma exposição pública aparentemente passageira pode permanecer indexada, compartilhada ou arquivada. O ECA permite compreender que o tempo do dano digital não coincide com o tempo da postagem inicial. Essa característica justifica medidas rápidas de contenção e preservação de provas.

O ECA também fortalece a ideia de prevenção. A proteção de crianças e adolescentes não deve ser acionada apenas após o dano consumado; deve orientar políticas e práticas destinadas a impedir violências e violações previsíveis. Em ambiente digital, essa perspectiva se traduz em deveres de desenho seguro, canais de denúncia, linguagem adequada e mecanismos de resposta. A responsabilidade civil absorve essa diretriz ao reconhecer que omissões preventivas podem ser juridicamente relevantes quando conectadas ao dano.

O ECA contribui ainda para afastar leituras meramente patrimoniais. A criança e o adolescente têm direito à dignidade, respeito, liberdade e convivência, bens que podem ser diretamente atingidos por práticas digitais. A responsabilidade civil deve reconhecer que lesões a esses bens podem exigir reparação e medidas inibitórias, desde que demonstrada conexão com falha da plataforma.

A atuação preventiva exigida pelo ECA deve ser compatível com a realidade tecnológica. Não basta recomendar acompanhamento familiar quando a própria plataforma cria fluxos de comunicação opacos, conteúdos personalizados e mecanismos de retenção contínua. O fornecedor possui conhecimento técnico que a família não possui. Daí a necessidade de deveres de cooperação, informação e resposta que complementem, e não substituam, o papel dos responsáveis.

A condição de sujeito em desenvolvimento exige reconhecer diferenças internas entre infância e adolescência. Uma criança pequena, um adolescente de treze anos e um jovem próximo da maioridade não possuem a mesma capacidade de compreensão, decisão e resistência a estratégias persuasivas. O dever de cuidado deve ser graduado conforme idade provável, natureza do serviço e risco envolvido.

Essa graduação evita paternalismo uniforme e permite respeitar autonomia progressiva, sem transferir ao menor a responsabilidade integral por escolhas moldadas por arquitetura opaca ou informação insuficiente (BRASIL, 1990a; MACIEL, 2024a).

O ECA também oferece categorias relevantes para a resposta ao dano, como preservação da imagem, dignidade, respeito e proteção contra exploração. No ambiente digital, essas garantias alcançam circulação de fotografias, exposição de rotina, tratamento de dados e interações públicas. A aplicação não depende de reproduzir literalmente situações previstas na década de 1990; o estatuto deve ser interpretado de maneira evolutiva, mantendo sua finalidade protetiva diante de novas formas de vulneração. O ECA Digital complementa essa trajetória ao especificar deveres ligados à infraestrutura tecnológica (ISHIDA, 2024; ROSSATO; LÉPORE; CUNHA, 2024).

A participação da família permanece relevante, mas não pode ser utilizada como excludente automática. Responsáveis possuem deveres de orientação e acompanhamento, porém muitas funcionalidades são desenhadas para funcionar fora de sua percepção e dependem de informações controladas pelo fornecedor. A eventual falha parental deve ser analisada concretamente e pode, em situações excepcionais, influenciar a causalidade ou a extensão da reparação. Não é juridicamente adequado presumir que a presença de responsáveis elimina o dever profissional de segurança de quem oferece serviço em escala (NUCCI, 2024; FRAZÃO, 2021).

O sujeito em desenvolvimento também deve ser compreendido em sua dimensão relacional. Crianças e adolescentes constroem vínculos, pertencimento e reconhecimento por meio de interações digitais. Quando uma plataforma falha diante de exposição pública, assédio ou manipulação de dados, o dano pode atingir não apenas uma esfera interna, mas a posição social do menor perante escola, família e comunidade. Essa especificidade reforça a necessidade de tutela sensível ao contexto.

3.3 Responsabilidade subjetiva, responsabilidade objetiva e atividade de risco

A responsabilidade civil brasileira convive com modelos subjetivos e objetivos. A responsabilidade subjetiva permanece vinculada à culpa, enquanto a objetiva se apoia em hipóteses legais ou na atividade que, por sua natureza, implica risco para

direitos de terceiros. O art. 927, parágrafo único, do Código Civil é central para a presente pesquisa porque permite examinar se a organização econômica e técnica de plataformas acessadas por menores pode justificar imputação baseada no risco (BRASIL, 2002; CAVALIERI FILHO, 2024).

A aplicação da responsabilidade objetiva às plataformas exige cautela. Não basta afirmar que internet envolve risco ou que toda plataforma é economicamente poderosa. É necessário identificar a atividade específica, o risco juridicamente relevante e a relação entre esse risco e o dano. Uma rede social que recomenda conteúdos, coleta dados e define padrões de visibilidade não exerce a mesma função de mero suporte técnico de conexão. O grau de controle importa para a imputação (TEPEDINO; TERRA; GUEDES, 2024).

A teoria do risco deve ser adaptada ao ambiente digital. O risco não está apenas na existência da tecnologia, mas na forma como o serviço organiza fluxos de informação, incentivos de permanência, publicidade e resposta a incidentes. Quando esse modelo alcança crianças e adolescentes, a previsibilidade do dano e a possibilidade de mitigação ganham relevância maior. A responsabilidade objetiva, nesse contexto, é uma técnica de alocação de riscos próprios da atividade.

A construção aqui defendida não elimina a responsabilidade subjetiva. Há situações em que a culpa, a negligência ou a omissão específica continuarão sendo elementos relevantes. A proposta é reconhecer que determinados danos infantojuvenis em plataformas podem ser tratados por responsabilidade objetiva quando o dever violado decorre do risco organizado pela atividade e não apenas de falha moral individual do fornecedor (SCHREIBER, 2015; ROSENVALD, 2017).

A qualificação da responsabilidade objetiva serve para evitar excessos. Ela exige incidência do regime protetivo, dever concreto, risco previsível, falha verificável, dano e nexo. Assim, a atividade de risco não se converte em garantia universal; ela orienta a distribuição dos custos do dano quando a plataforma cria ou amplia riscos que estava em melhor posição de prevenir ou documentar.

A atividade de risco, nesse contexto, não se confunde com toda atividade digital. O risco juridicamente relevante aparece quando escala, opacidade, recomendação, coleta de dados, contato com terceiros e monetização de atenção tornam insuficiente a postura meramente reativa. O art. 927, parágrafo único, do Código Civil fornece uma chave dogmática, mas sua incidência deve ser demonstrada

pela natureza da operação e pela relação com o dano alegado, não pela simples presença da internet (TEPEDINO; TERRA; GUEDES, 2024).

A distinção entre culpa e risco deve ser manejada com precisão. A responsabilidade objetiva não elimina a investigação sobre o fato; ela desloca o centro da análise da culpa psicológica para a atividade, o dever de segurança e o nexo causal. Em plataformas digitais, isso significa perguntar se o serviço, pela forma como foi desenhado e explorado, criou ou ampliou risco típico a menores. A resposta não depende apenas de saber se um empregado agiu com negligência, mas de verificar se a organização do serviço era adequada ao público previsível (BRASIL, 2002; CAVALIERI FILHO, 2024).

A atividade de risco deve ser conectada ao dano discutido. Não basta afirmar que redes sociais são perigosas em abstrato; é necessário mostrar que a funcionalidade discutida aumentou risco específico. A recomendação de conteúdo autolesivo, a exposição pública por padrão ou a publicidade comportamental sensível são exemplos de riscos que podem ser avaliados objetivamente. A imputação depende de descrição precisa do mecanismo que contribuiu para a lesão.

O CDC também contribui para a responsabilidade objetiva quando há relação de consumo. Serviços gratuitos do ponto de vista monetário podem envolver remuneração indireta por dados, atenção ou publicidade. Nesses casos, deveres de segurança, informação e adequação do serviço tornam-se relevantes. A criança ou adolescente, como consumidor hipervulnerável, exige padrão reforçado de proteção, mas ainda sujeito à análise de defeito, dano e nexo (BRASIL, 1990b; MIRAGEM, 2019).

A qualificação do risco pode ser organizada por cinco indicadores: probabilidade de ocorrência, magnitude potencial do dano, assimetria informacional, capacidade de controle e possibilidade de externalização do prejuízo. Nenhum desses fatores, isoladamente, basta. A combinação entre eles permite distinguir serviço que apenas participa da vida social digital de atividade que administra risco especial e previsível. Em relação a menores, a avaliação deve considerar ainda idade provável, intensidade da exposição e dificuldade de reversão do dano.

A responsabilidade objetiva proposta nesta dissertação funda-se na teoria do risco criado, e não na do risco integral. Ela exige prova de dano e nexo, ainda que admita inferências e distribuição dinâmica quando a informação esteja sob controle da plataforma. Sua especificidade decorre da necessidade de apontar dever proativo

descumprido, risco criado ou ampliado e relação entre falha do serviço e dano. Sem esses filtros, a responsabilidade objetiva perderia densidade dogmática (FARIAS; ROSENVALD; BRAGA NETTO, 2023).

A incidência do art. 927, parágrafo único, deve ser examinada por funcionalidade, e não por uma classificação global da empresa. A mesma plataforma pode atuar como mera hospedeira em uma situação, como agente de recomendação em outra e como intermediária publicitária em uma terceira. O risco da atividade varia conforme o módulo do serviço que participou do evento. Essa leitura funcional evita declarar toda a plataforma perigosa e permite atribuir responsabilidade apenas ao segmento efetivamente relacionado ao dano.

A objetivação também modifica a distribuição do debate processual. À parte autora cabe indicar o serviço utilizado, a funcionalidade relevante, o dano e os indícios de conexão. À plataforma compete esclarecer políticas, registros, testes e salvaguardas sob seu domínio quando tais elementos forem necessários à verificação do risco. Não se trata de dispensar a prova constitutiva, mas de impedir que a estrutura técnica concentre todas as informações decisivas no fornecedor e torne a tutela inviável (BRASIL, 2015a; MULHOLLAND, 2009).

A distinção entre risco permitido e risco proibido é decisiva. A vida digital envolve riscos sociais inevitáveis, como críticas, conflitos e exposição moderada. O risco juridicamente relevante surge quando o fornecedor amplia perigos evitáveis, explora vulnerabilidade, omite resposta ou descumpre dever proativo. A atividade de risco, portanto, não é qualquer atividade digital, mas a atividade digital organizada de modo incompatível com a proteção de menores.

O debate sobre risco deve evitar determinismo tecnológico. Algoritmos, sistemas de recomendação e métricas de engajamento não são perigosos por natureza. Seu risco depende de finalidade, configuração, público atingido e salvaguardas adotadas. A responsabilidade civil deve rejeitar tanto a demonização da tecnologia quanto a neutralização completa do seu efeito jurídico. O centro da análise é a escolha empresarial concreta.

A responsabilidade objetiva por violação de deveres proativos também se aproxima da noção de defeito do serviço. O serviço digital pode ser defeituoso quando não oferece a segurança legitimamente esperada para seu público, considerando idade provável, finalidade, riscos e informação fornecida. Essa segurança não é

absoluta; é segurança razoável. A pergunta passa a ser se a plataforma adotou medidas compatíveis com o risco que sua atividade produziu ou administrou.

A atividade de risco pode ser intensificada pela escala. Um serviço utilizado por milhões de usuários, com recomendação automatizada e coleta massiva de dados, possui capacidade de produzir danos em extensão superior à de interações pontuais. A escala não gera ilicitude, mas aumenta a relevância da governança. Quanto maior o alcance e o controle técnico, maior deve ser a capacidade de demonstrar mecanismos de prevenção e resposta proporcionais ao risco.

É útil distinguir defeito de organização e incidente inevitável. O primeiro existe quando políticas, desenho, fluxos de resposta ou controles de segurança são inadequados ao risco conhecido; o segundo ocorre apesar de estrutura razoável e atuação diligente. A responsabilidade objetiva pode alcançar o defeito organizacional sem exigir identificação de empregado culpado, mas não transforma qualquer falha pontual ou evento imprevisível em dever de reparar.

A diferença entre risco ordinário e risco ampliado pode ser testada por raciocínio contrafactual: o dano teria alcance semelhante se a plataforma não tivesse recomendado, segmentado, impulsionado ou mantido configuração insegura? A resposta não precisa demonstrar certeza matemática, mas deve apoiar-se em fatos verificáveis. Quando a funcionalidade empresarial altera materialmente a probabilidade ou a extensão da lesão, o risco deixa de ser mero reflexo da convivência social e passa a integrar a atividade organizada.

A culpa continua relevante como categoria auxiliar, embora não seja o eixo da argumentação. Condutas negligentes podem demonstrar falha de organização e reforçar a imputação objetiva, mas a ausência de culpa subjetiva individual de funcionários não afasta necessariamente o defeito do serviço. Em atividades complexas, a falha pode ser sistêmica, decorrente de política empresarial ou omissão estrutural, e não de ato pessoal isolado.

Responsabilidade subjetiva e objetiva podem aparecer de forma subsidiária ou concorrente na mesma demanda. A decisão judicial deve indicar qual fundamento sustenta cada dever: culpa por omissão concreta, defeito do serviço, risco da atividade, violação de proteção de dados ou descumprimento de obrigação especial. Essa explicitação evita decisões que utilizem simultaneamente vários regimes sem definir seus pressupostos e impede duplicidade de reparação.

Escala, lucratividade e complexidade tecnológica funcionam como elementos de contexto, não como fundamentos autônomos. Eles podem demonstrar capacidade de prevenção, acesso a dados e potencial de difusão, mas precisam ser vinculados à funcionalidade discutida. Uma grande plataforma não responde apenas por ser grande; responde quando sua escala ou seus sistemas contribuíram para o risco e quando medidas proporcionais estavam ao seu alcance.

A plataforma pode afastar a imputação mediante prova de que o risco não era típico, de que adotou salvaguardas compatíveis, de que reagiu em tempo razoável ou de que o dano decorreu de causa externa suficiente. Essa possibilidade de demonstração é parte da qualificação do modelo objetivo. A responsabilidade concentra-se na gestão do risco, mas permanece aberta à análise de diligência, inevitabilidade e ruptura do nexo.

A teoria do risco também cumpre função distributiva. Quando o fornecedor organiza atividade capaz de gerar benefícios econômicos e controla os instrumentos de mitigação, é coerente que suporte os custos dos danos tipicamente associados à falha de sua estrutura. Essa distribuição não se baseia em punição pelo lucro, mas na posição de quem pode conhecer, reduzir, documentar e internalizar o risco com menor custo social.

A autoria de terceiro não encerra a análise quando o dano depende de mecanismos próprios do serviço. Uma ofensa isolada pode permanecer atribuída ao usuário; a mesma mensagem, quando segmentada, impulsionada ou reiteradamente recomendada, pode envolver contribuição autônoma da plataforma. O julgador deve separar a criação do conteúdo da organização de sua circulação para identificar responsabilidades proporcionais.

Fortuito interno e fortuito externo oferecem critério adicional. Fraudes, abusos e tentativas de burlar controles podem integrar o risco normal de serviços que operam em escala e conectam desconhecidos, especialmente quando são recorrentes e tecnicamente detectáveis. Eventos absolutamente estranhos à atividade, inevitáveis mesmo diante de salvaguardas adequadas, podem romper o nexo. A classificação depende da relação do evento com a arquitetura e com a previsibilidade do serviço.

O CDC oferece outra via de objetivação quando há relação de consumo e defeito do serviço. A gratuidade monetária não exclui remuneração indireta por dados e publicidade. O defeito é avaliado pela segurança legitimamente esperada, considerando informação, modo de fornecimento e riscos previsíveis. Para menores,

a expectativa de segurança é influenciada por proteção integral e pela apresentação do serviço como adequado a determinada idade.

A responsabilidade objetiva não dispensa ilicitude ou defeito. O dano decorrente de risco inerente informado e adequadamente reduzido pode não ser imputável. A análise deve comparar o serviço oferecido com alternativas razoáveis e com promessas feitas ao usuário. Controles parentais anunciados, por exemplo, integram a expectativa e podem gerar responsabilidade se forem meramente aparentes.

A escolha entre regimes não deve ocorrer apenas pelo rótulo da ação. O mesmo fato pode envolver Código Civil, CDC, LGPD e ECA Digital. O diálogo das fontes permite coordenação, evitando duplicidade de indenização e lacunas. O julgador deve explicitar qual norma fundamenta cada dever e por que o regime objetivo se aplica ao caso concreto.

3.4 Função social da responsabilidade civil e deveres preventivos

A responsabilidade civil contemporânea não se limita à reparação patrimonial posterior. Ela também desempenha funções preventiva, distributiva e ordenadora de condutas. Em danos digitais envolvendo crianças e adolescentes, essa dimensão é essencial porque a reparação posterior pode não recompor integralmente lesões à imagem, privacidade, reputação e desenvolvimento emocional (ROSENVALD, 2017; SCHREIBER, 2015).

A função preventiva não significa punição antecipada nem controle absoluto da inovação. Ela exige que o agente econômico, conhecendo riscos previsíveis e dispondo de meios proporcionais de mitigação, organize sua atividade de modo compatível com direitos fundamentais. Para plataformas digitais, isso pode envolver avaliação de risco, privacidade por padrão, canais de denúncia, respostas documentadas e adaptação de funcionalidades a públicos vulneráveis (FRAZÃO, 2021).

A função social da responsabilidade civil dialoga com a proteção integral porque desloca parte da preocupação para o desenho do serviço. Quando a plataforma lucra com atenção, dados e circulação de conteúdo, não pode tratar a segurança de menores como elemento externo à atividade. A prevenção se torna componente da própria organização econômica, e sua ausência pode revelar falha relevante para imputação civil.

Essa função preventiva também possui dimensão coletiva. Falhas de *design*, publicidade inadequada, ausência de canal de denúncia ou padrões inseguros de privacidade podem atingir número indeterminado de menores. Nesses casos, a tutela inibitória e coletiva pode ser mais adequada do que a simples indenização individual, pois atua sobre a fonte do risco (BRASIL, 1985; BRASIL, 1990b).

A contribuição da função social para a presente pesquisa é mostrar que a responsabilidade objetiva aqui defendida não serve apenas para reparar, mas para induzir governança adequada de riscos. O objetivo é alinhar atividade econômica, proteção integral e deveres de diligência, preservando a proporcionalidade e a análise do nexo causal.

Essa função preventiva precisa ser controlada juridicamente. O juiz não deve impor deveres vagos ou tecnologicamente impossíveis, nem substituir a governança da plataforma por intuição pessoal sobre segurança. A decisão deve indicar qual medida era razoavelmente exigível, por que sua ausência aumentou o risco e como ela se relaciona com o dano. Esse cuidado preserva a função social sem converter a responsabilidade civil em instrumento de regulação ilimitada.

A função social da responsabilidade civil aparece com especial intensidade nos danos digitais porque a reparação posterior muitas vezes não recompõe integralmente a situação da vítima. Conteúdos replicados, dados compartilhados, reputação abalada e exposição psicológica podem persistir mesmo após remoção. Daí a importância de deveres preventivos: a responsabilidade civil não serve apenas para pagar indenização, mas também para induzir práticas de segurança, documentação e resposta proporcional (ROSENVALD, 2017; SCHREIBER, 2015).

Cabe indagar se os deveres proativos instituídos pelo ECA Digital não seriam, em substância, os próprios deveres anexos derivados da boa-fé objetiva. A aproximação é pertinente e produtiva. Desde a compreensão da relação obrigacional como processo, a doutrina civilista reconhece que o vínculo não se esgota na prestação principal: dele irradiam deveres laterais de proteção, informação e cooperação, cuja fonte é a boa-fé objetiva (art. 422 do Código Civil; art. 4º, inciso III, e art. 51, inciso IV, do Código de Defesa do Consumidor).

O conteúdo material das obrigações impostas pela Lei nº 15.211/2025 – segurança desde a concepção, avaliação prévia de risco, privacidade por padrão, transparência, canais acessíveis de denúncia e resposta documentada a incidentes – corresponde, ponto a ponto, a essa tríade: proteger a integridade do usuário, informá-

lo de modo compreensível e cooperar para a realização da finalidade legítima do serviço. Nesse sentido, o ECA Digital não cria deveres estranhos à tradição do direito civil brasileiro; ele tipifica, em legislação especial e para um ambiente determinado, aquilo que a boa-fé objetiva já autorizava extrair da relação entre plataforma e usuário (COUTO E SILVA, 2006; MARTINS-COSTA, 2018; BENJAMIN; MARQUES; BESSA, 2022).

A identificação, contudo, não pode ser integral, e é justamente a diferença que interessa a esta pesquisa. Quanto à fonte, os deveres anexos são implícitos e dependem da concreção judicial de uma cláusula geral, ao passo que os deveres proativos são típicos e legalmente previstos, o que reduz a margem de discricionariedade e torna a exigência verificável *ex ante*. Quanto ao âmbito de incidência, o dever anexo pressupõe relação obrigacional, ainda que decorrente de contato social, enquanto o dever proativo recai sobre a organização da atividade e protege inclusive crianças que não figuram como contratantes, situação frequente diante da incapacidade civil e do uso de contas de terceiros. Quanto à consequência do descumprimento, por fim, a violação de dever anexo produz efeitos no interior da relação obrigacional de que emana: submete-se ao regime do inadimplemento e alcança, em regra, apenas os sujeitos daquele vínculo. A violação de dever proativo, ao contrário, caracteriza defeito do serviço e gera responsabilidade oponível a qualquer vítima, ainda que estranha a toda relação contratual com o fornecedor. (CONSELHO DA JUSTIÇA FEDERAL, 2012). A distinção é decisiva no objeto desta pesquisa, em que a criança lesada frequentemente sequer poderia ter contratado.

Longe de enfraquecer a hipótese aqui defendida, a matriz da boa-fé objetiva a reforça: confirma que o descumprimento de deveres de conduta pode gerar responsabilidade sem juízo de reprovabilidade subjetiva. A natureza objetiva da imputação, todavia, não decorre da boa-fé, mas do risco da atividade e do defeito do serviço (art. 927, parágrafo único, do Código Civil; art. 14 do Código de Defesa do Consumidor). À boa-fé objetiva cabem as funções interpretativa e integrativa – identificar, densificar e delimitar o dever exigível –; à teoria do risco cabe determinar o regime de imputação. Essa divisão de tarefas evita que a cláusula geral seja mobilizada como fundamento autônomo de condenação e preserva a controlabilidade da matriz decisória proposta nesta dissertação (MARTINS-COSTA, 2018; TEPEDINO; TERRA; GUEDES, 2024).

A função social também exige coerência institucional. Plataformas que lucram com escala, dados e atenção devem internalizar custos razoáveis de proteção, sobretudo quando alcançam crianças e adolescentes. Essa internalização não é punição à atividade econômica; é forma de impedir que o ônus do risco seja transferido integralmente às vítimas vulneráveis. A responsabilidade civil opera, assim, como mecanismo de ordenação da atividade e de prevenção de danos evitáveis.

Em danos massificados, a prevenção possui dimensão coletiva. Falhas sistêmicas de recomendação, ausência de moderação adequada ou desenho inseguro de privacidade não atingem apenas uma vítima. A tutela inibitória e as obrigações de fazer podem ser mais adequadas do que respostas puramente indenizatórias. Isso aproxima responsabilidade civil, processo coletivo e proteção integral, sem dispensar o controle de proporcionalidade (BRASIL, 1985; ROSENVALD, 2017).

A função preventiva se conecta ao dever de informação. Para que famílias e adolescentes possam agir, é necessário compreender riscos, configurações de privacidade, canais de denúncia e efeitos da exposição digital. Informação incompreensível ou escondida não cumpre função preventiva real. Assim, a responsabilidade civil pode considerar a qualidade da comunicação oferecida pela plataforma, especialmente quando o serviço utiliza design persuasivo ou linguagem voltada a jovens (BRASIL, 1990b; MIRAGEM, 2019).

Deveres preventivos devem ser proporcionais. Não se exige da plataforma onisciência tecnológica nem eliminação absoluta de riscos. Exige-se que ela identifique riscos previsíveis, documente medidas adotadas e responda de modo compatível com sua capacidade técnica e econômica. Essa proporcionalidade é indispensável para preservar inovação e liberdade comunicativa sem sacrificar a proteção de menores (BRASIL, 2014a; BRASIL, 2025a).

A função preventiva não elimina a função reparatória. Quando o dano se consuma, a vítima continua tendo direito à reparação adequada. O ponto é reconhecer que certos riscos digitais exigem resposta anterior ou concomitante, sob pena de a indenização chegar tarde demais. Uma imagem íntima de adolescente, uma recomendação reiterada de conteúdo autolesivo ou a exploração comportamental de dados pode produzir lesões que não se recompõem integralmente por pagamento posterior (SAFERNET BRASIL, 2025).

A responsabilidade civil contemporânea não se limita à compensação econômica posterior ao dano. Sua função social inclui prevenção, redistribuição de riscos e indução de comportamentos diligentes em atividades complexas. No contexto digital, essa função é especialmente relevante porque a reparação posterior pode ser insuficiente diante da velocidade de circulação de imagens, dados e conteúdos. A tutela civil deve considerar formas de impedir repetição do dano e aperfeiçoar a organização do serviço (ROSENVALD, 2017; SCHREIBER, 2015).

A prevenção, por fim, aproxima responsabilidade civil e governança digital. O objetivo não é transformar o juiz em administrador da plataforma, mas permitir que a decisão civil reconheça quando a falha de governança foi juridicamente relevante. A resposta pode ser indenizatória, inibitória ou estrutural, conforme a natureza do risco e o tipo de dano. Essa flexibilidade é necessária em ambiente tecnológico mutável.

Deveres preventivos podem assumir forma graduada. Para riscos leves, avisos e ajustes de configuração podem bastar. Para riscos moderados, canais de denúncia e limitação de alcance podem ser exigíveis. Para riscos graves, envolvendo exploração sexual, autolesão ou exposição íntima, respostas prioritárias e preservação de prova tornam-se indispensáveis. Essa gradação evita soluções únicas e melhora a qualidade dogmática da imputação.

A função preventiva também dialoga com transparência. Sem informação mínima sobre políticas de recomendação, privacidade e resposta, usuários e responsáveis não conseguem agir de modo informado. A transparência não exige revelação de segredos industriais em todos os casos, mas requer explicação suficiente sobre riscos e medidas de proteção. Em litígio, essa explicação pode ser controlada pelo juiz com preservação de confidencialidade quando necessário.

A prevenção deve ser institucionalizada, não improvisada. Plataformas de grande escala não podem depender apenas de reação casuística a incidentes graves. Políticas internas, treinamentos, fluxos de denúncia, revisão de funcionalidades e relatórios de risco são sinais de diligência. A falta de organização pode demonstrar que a empresa tratou risco previsível como evento excepcional, embora sua própria operação indicasse exposição recorrente de menores.

A função social da responsabilidade civil também se manifesta na distribuição dos custos da atividade. Se uma plataforma obtém benefício econômico de dados, atenção e interação, é coerente que suporte custos razoáveis de prevenção e governança. Essa lógica evita externalização de riscos a crianças, famílias e sistema

público de proteção. A responsabilidade civil não paralisa a atividade econômica; ela exige que a atividade internalize riscos previsíveis que ajuda a organizar.

A função social da responsabilidade civil não deve ser vista como argumento de expansão ilimitada. Ela orienta a correção de riscos injustamente transferidos, mas permanece limitada por proporcionalidade, causalidade e previsibilidade. O modelo defendido é preventivo sem ser absoluto: exige cuidado onde há controle e risco reconhecível, mas rejeita punição por eventos impossíveis de prever ou evitar.

A prevenção também se conecta ao dever de preservar evidências. Em danos digitais, a perda de registros pode impedir reconstrução do fato e frustrar tutela judicial. O fornecedor que controla *logs*, denúncias e decisões de moderação deve manter documentação compatível com a gravidade do risco e com a legislação aplicável. Essa preservação serve à vítima, à defesa da própria plataforma e ao controle judicial.

A função preventiva da responsabilidade civil ganha relevo quando a reparação posterior não restitui plenamente a vítima. Imagens podem ser copiadas, dados podem circular por tempo indeterminado e recomendações nocivas podem produzir efeitos antes que qualquer decisão judicial seja proferida. A possibilidade de responsabilização incentiva investimentos em desenho seguro, treinamento e canais de resposta. Esse efeito preventivo não deve ser confundido com punição abstrata: a medida precisa guardar relação com o risco demonstrado e com a capacidade do fornecedor de evitar sua repetição (ROSENVALD, 2017; FRAZÃO, 2021).

A função social também exige distribuir custos de forma coerente. Quando uma empresa organiza atividade lucrativa e controla elementos técnicos inacessíveis aos usuários, não é razoável transferir integralmente às famílias o custo de falhas previsíveis. Ao mesmo tempo, impor indenização por qualquer comportamento de terceiro poderia encarecer serviços, estimular remoção excessiva e restringir participação. O equilíbrio está em atribuir o custo do dano a quem criou ou ampliou o risco relevante, preservando excludentes quando a plataforma demonstrar diligência compatível (FARIAS; ROSENVALD; BRAGA NETTO, 2023).

Deveres preventivos podem ser concretizados por medidas distintas da indenização. Ajuste de configuração, preservação de registros, melhoria de canal, informação ao usuário, revisão de publicidade ou limitação de recomendação podem responder melhor à causa do problema. A escolha do remédio deve considerar se a falha é individual, procedimental ou sistêmica. Essa pluralidade aproxima a responsabilidade civil de sua função social, pois não se limita a monetizar a lesão,

mas busca reorganizar comportamentos e reduzir a repetição de danos (ROSENVALD, 2017; BRASIL, 1985).

O dever preventivo pode ser compreendido como dever de aprendizagem institucional. A plataforma que recebe denúncias reiteradas sobre determinado risco deve ajustar fluxos, revisar funcionalidades e melhorar comunicação. Se incidentes semelhantes continuam ocorrendo sem aperfeiçoamento, a omissão deixa de ser episódica e passa a revelar falha de governança. A responsabilidade civil pode considerar essa reincidência como elemento de agravamento.

3.5 Hipervulnerabilidade digital, relação de consumo e diálogo das fontes

A hipervulnerabilidade digital de crianças e adolescentes resulta da combinação entre idade, desenvolvimento, assimetria informacional, dependência de mediação familiar e opacidade técnica das plataformas. O menor pode usar o serviço de modo ativo, mas não compreende plenamente a lógica de recomendação, coleta de dados, publicidade comportamental e circulação permanente de informações (AZEVEDO; TORRES, 2023).

A relação de consumo amplia a análise porque muitas plataformas oferecem serviços aparentemente gratuitos em troca de dados, atenção e exposição publicitária. O usuário passa a integrar um mercado de consumo digital no qual a vulnerabilidade não é apenas econômica, mas técnica e informacional. Quando esse usuário é criança ou adolescente, a vulnerabilidade é reforçada e exige deveres mais intensos de segurança e informação (BRASIL, 1990b; MIRAGEM, 2019).

O diálogo das fontes é necessário porque nenhuma norma resolve sozinha o problema. A Constituição fornece a prioridade absoluta; o ECA define a proteção integral; o Código Civil disciplina responsabilidade; o CDC reforça segurança e informação; a LGPD regula dados; o Marco Civil preserva garantias digitais; e o ECA Digital densifica deveres proativos. A coordenação dessas fontes impede tanto a fragmentação quanto a aplicação isolada de um único regime (MARQUES, 2012).

A hipervulnerabilidade não dispensa a prova. Ela justifica maior rigor no dever de cuidado e maior atenção à distribuição da informação, mas a imputação continua dependente de conduta juridicamente relevante. O julgador deve identificar se a plataforma estava em melhor posição para prevenir, explicar ou documentar o dano. Essa análise transforma vulnerabilidade em critério de equilíbrio, não em presunção absoluta.

No campo digital, a vulnerabilidade também é dinâmica. Ela varia conforme idade, tipo de serviço, grau de exposição, funcionalidade utilizada e capacidade de supervisão. Por isso, a responsabilidade não pode ser uniforme para todos os ambientes. Uma rede social aberta, uma plataforma de vídeos, um jogo conectado e um aplicativo de mensagens exigem critérios próprios de diligência.

O resultado do diálogo das fontes é uma matriz de análise mais precisa. Em vez de perguntar genericamente se a plataforma deve responder, o julgador deve verificar qual fonte define o dever, qual funcionalidade criou o risco, qual vulnerabilidade estava presente e que prova está disponível. Essa matriz sustenta a imputação objetiva sem reduzir o debate a *slogans* protetivos.

O diálogo das fontes impede que ECA, CDC, LGPD, Marco Civil e ECA Digital sejam aplicados como sistemas isolados. Cada diploma responde a uma dimensão do problema: proteção integral, segurança do serviço, dados pessoais, liberdade de expressão e deveres proativos. A tarefa dogmática é coordenar essas fontes para que uma norma não anule a finalidade da outra. Assim, o CDC reforça vulnerabilidade e defeito do serviço; a LGPD disciplina dados; o Marco Civil delimita cautelas sobre conteúdo; e o ECA Digital especializa a proteção de menores (MARQUES, 2012).

A hipervulnerabilidade digital não deriva apenas da idade. Ela resulta da soma entre desenvolvimento incompleto, assimetria informacional, opacidade algorítmica, dependência social da conectividade e dificuldade de prova. Crianças e adolescentes podem não compreender que suas interações alimentam perfis, recomendações e publicidade. Esse quadro justifica leitura reforçada do dever de informação e segurança, especialmente quando a plataforma explora economicamente dados ou atenção (AZEVEDO; TORRES, 2023; BENJAMIN; MARQUES; BESSA, 2022).

Do ponto de vista processual, a hipervulnerabilidade influencia o acesso à prova. Famílias podem não conhecer mecanismos de recomendação, critérios de segmentação ou histórico interno de denúncias. A distribuição dinâmica do ônus da prova funciona como instrumento de equilíbrio, mas deve ser aplicada com cuidado. O juiz precisa indicar quais informações são relevantes, quem as controla e como sua ausência interfere na reconstrução do fato (BRASIL, 2015a; MULHOLLAND, 2009).

A publicidade dirigida a menores evidencia a necessidade do diálogo das fontes. O mesmo fato pode envolver relação de consumo, tratamento de dados, exploração de vulnerabilidade, dever de cuidado e proteção integral. Se a publicidade utiliza dados comportamentais para induzir consumo ou permanência excessiva, a

análise não deve se limitar a uma única lei. A pluralidade normativa é a própria condição de compreensão do dano (BRASIL, 1990b; BRASIL, 2018; INSTITUTO ALANA, 2026).

A hipervulnerabilidade não dispensa a demonstração do dano. Ela qualifica o padrão de cuidado, influencia a distribuição da prova e orienta a extensão da tutela, mas não substitui a análise de causalidade. Esse ponto é decisivo para diferenciar proteção reforçada de paternalismo jurídico ilimitado. A responsabilidade objetiva exige que a vulnerabilidade esteja conectada a uma falha do serviço e ao dano alegado (TEPEDINO; TERRA; GUEDES, 2024).

O diálogo das fontes evita escolhas excludentes entre microssistemas. O ECA define finalidade protetiva; o CDC reforça segurança e informação; a LGPD disciplina dados pessoais; o Marco Civil preserva garantias digitais; o Código Civil estrutura responsabilidade; e o ECA Digital densifica deveres proativos. A interpretação isolada de qualquer diploma produziria respostas incompletas. A solução deve articular as fontes conforme o risco discutido (MARQUES, 2012; BRASIL, 2025a).

A relação de consumo pode existir mesmo sem pagamento direto. Plataformas aparentemente gratuitas extraem valor de atenção, dados, publicidade ou compras internas. O usuário menor, nesse contexto, participa de uma relação econômica, ainda que não perceba claramente sua contrapartida. O CDC contribui ao impor deveres de segurança, informação, prevenção de práticas abusivas e adequação do serviço ao destinatário vulnerável (BENJAMIN; MARQUES; BESSA, 2022; MIRAGEM, 2019).

A hipervulnerabilidade digital combina idade, assimetria informacional, dependência tecnológica e dificuldade probatória. Crianças e adolescentes não apenas possuem menor maturidade para avaliar riscos, mas também interagem com sistemas opacos que coletam dados, personalizam conteúdo e definem visibilidade. Essa vulnerabilidade ampliada justifica o diálogo entre proteção integral, direito do consumidor, proteção de dados e responsabilidade civil (AZEVEDO; TORRES, 2023; BRASIL, 1990b).

A utilização das fontes deve ser funcional. Não se cita CDC apenas para afirmar vulnerabilidade, nem LGPD apenas para mencionar dados. Cada fonte deve cumprir papel específico: o CDC define relação de consumo e segurança; a LGPD trata dados; o ECA define proteção integral; o Marco Civil disciplina intermediários; o ECA Digital densifica deveres proativos. Essa organização melhora a fundamentação e reduz repetições.

A hipervulnerabilidade reforça a necessidade de controle de publicidade. Crianças e adolescentes podem ser mais suscetíveis a mensagens comerciais personalizadas, especialmente quando a publicidade se mistura a entretenimento, influenciadores ou jogos. A plataforma que permite segmentação de anúncios a partir de dados de comportamento deve demonstrar cautelas específicas. O CDC e a proteção integral oferecem base para essa exigência de cuidado.

O diálogo das fontes também resolve aparentes conflitos entre LGPD e ECA Digital. A proteção de menores pode exigir aferição de idade e adaptação de funcionalidades, mas a LGPD impõe minimização e segurança no tratamento. A solução não é escolher uma lei contra a outra; é buscar método proporcional que proteja sem coletar dados excessivos. Esse exemplo mostra por que a interpretação isolada produz respostas deficientes.

A relação de consumo permite analisar expectativas legítimas de segurança. Um serviço amplamente utilizado por adolescentes gera expectativa de que a plataforma ofereça mecanismos mínimos de proteção e resposta. Essa expectativa é maior quando a própria plataforma promove recursos de segurança ou afirma possuir ambiente adequado. A desconformidade entre promessa institucional e prática efetiva pode revelar falha informacional ou defeito do serviço.

A hipervulnerabilidade digital não decorre apenas da idade. Ela envolve baixa transparência técnica, assimetria de informação, dependência de plataformas para sociabilidade e dificuldade de deixar o serviço sem prejuízo de participação social. O adolescente pode formalmente escolher usar determinada aplicação, mas essa escolha ocorre dentro de ambiente desenhado para engajamento e coleta de dados. O direito deve considerar essa realidade sem negar a autonomia progressiva.

A relação de consumo ajuda a tratar a confiança depositada no serviço. Quando a plataforma apresenta ambiente seguro, comunidade protegida ou controle parental eficiente, cria expectativa legítima nos responsáveis. Se essa promessa não corresponde à prática, a falha informacional pode integrar a análise de responsabilidade. A publicidade institucional do serviço, portanto, também pode ser elemento de prova sobre o padrão de segurança esperado.

A hipervulnerabilidade digital pode aumentar em situações de deficiência, sofrimento psíquico, exclusão social ou baixa alfabetização midiática. A plataforma nem sempre conhecerá essas características individualmente, mas deve considerar que seu público inclui perfis vulneráveis diversos. Medidas de linguagem clara,

denúncia acessível e redução de práticas persuasivas excessivas beneficiam o conjunto dos usuários e reforçam a proteção de quem está em condição mais sensível.

A hipervulnerabilidade digital resulta da sobreposição de fatores. À vulnerabilidade própria da idade somam-se assimetria informacional, opacidade algorítmica, dependência social do serviço e dificuldade de produzir prova. Essa combinação não torna o menor incapaz de toda escolha, mas demonstra que consentimentos, cliques e configurações não podem ser interpretados como manifestação plenamente informada em qualquer contexto. O fornecedor deve considerar a compreensão real do público e evitar práticas que explorem impulsividade, medo de exclusão ou dificuldade de antecipar consequências (AZEVEDO; TORRES, 2023; MIRAGEM, 2019).

A relação de consumo é relevante mesmo quando não há pagamento direto. Dados, atenção e exposição publicitária podem integrar a lógica econômica do serviço, enquanto a plataforma define unilateralmente regras e funcionalidades. Nessa hipótese, os deveres de informação, segurança e adequação dialogam com a proteção integral e com a LGPD. A incidência do CDC não dispensa análise do caso concreto, mas oferece instrumentos para avaliar defeito do serviço, risco legitimamente esperado e vulnerabilidade do destinatário (BENJAMIN; MARQUES; BESSA, 2022; MARQUES; BENJAMIN; MIRAGEM, 2020).

O diálogo das fontes evita escolher um diploma e excluir os demais. O Marco Civil disciplina aspectos da responsabilidade de provedores; a LGPD cuida do tratamento de dados; o CDC protege o destinatário do serviço; o ECA e a Constituição estabelecem prioridade; o ECA Digital especifica deveres no ambiente tecnológico. A solução deve coordenar essas normas conforme o problema discutido. Em caso de publicidade comportamental, por exemplo, proteção de dados e consumo assumem centralidade; em remoção de conteúdo, as garantias do Marco Civil ganham maior peso (MARQUES, 2012; BRASIL, 2018).

O diálogo das fontes também permite resolver conflitos entre autonomia e proteção. O adolescente pode querer participar de redes, publicar conteúdo e interagir com pares. O sistema jurídico não deve impedir essa participação, mas exigir que ela ocorra em ambiente com informação e segurança razoáveis. Assim, autonomia progressiva e proteção integral são conciliadas por meio de deveres proporcionais de design, privacidade e resposta.

A aproximação entre proteção de dados e defesa do consumidor mostra que a privacidade não é interesse meramente individual isolado. Em relações digitais assimétricas, o tratamento de dados estrutura ofertas, recomendações e oportunidades de exposição, o que torna a transparência e a finalidade elementos da qualidade do serviço. Para crianças e adolescentes, a violação desses deveres pode repercutir simultaneamente em autonomia informacional, consumo e desenvolvimento, justificando leitura coordenada entre LGPD, CDC e ECA Digital (MENDES, 2014; MENDES; DONEDA, 2018).

A prevenção possui valor autônomo porque alguns danos não podem ser integralmente revertidos. A imagem íntima replicada, a exposição de localização ou o contato com aliciador podem produzir consequências mesmo após remoção. A tutela inibitória atua antes da consolidação, exigindo probabilidade de ilícito e medida proporcional. Ela não depende de dano já consumado, mas precisa de descrição concreta da ameaça.

A função preventiva também orienta incentivos econômicos. Se a plataforma internaliza custos de riscos que poderia reduzir, tende a investir em segurança. Contudo, indenizações desproporcionais podem favorecer remoção excessiva e exclusão de usuários. A calibragem deve considerar gravidade, capacidade de prevenção, benefício econômico e comportamento posterior. Medidas estruturais podem ser mais eficazes do que valores punitivos isolados.

O dever de advertir integra a prevenção. Informações sobre compartilhamento público, compras, contato com desconhecidos e uso de dados precisam aparecer no momento da decisão, em linguagem adequada. Termos extensos aceitos no cadastro não substituem avisos contextuais. A falha informacional pode contribuir para o dano quando a criança ou o responsável teria adotado conduta diferente com informação clara.

A função social também alcança cooperação com autoridades e entidades de proteção. Protocolos para risco imediato, preservação de prova e comunicação devem respeitar legalidade e privacidade. A ausência de canal institucional pode atrasar respostas críticas. Por outro lado, compartilhamento indiscriminado de dados viola direitos; a cooperação deve possuir base jurídica e controle.

A reparação precisa considerar medidas não pecuniárias. Retificação, remoção, desindexação, comunicação a usuários atingidos e custeio de apoio podem ser adequados. A escolha depende do dano e da vontade da vítima. Em casos com

menores, exposição adicional decorrente do próprio processo deve ser evitada por sigilo, anonimização e limitação da publicidade dos autos.

3.6 Presunção de causalidade e ônus da prova em danos digitais complexos

Danos digitais complexos desafiam a causalidade tradicional porque a lesão pode decorrer de múltiplos fatores: ato de terceiro, recomendação automatizada, falha de denúncia, ausência de privacidade por padrão, demora de resposta e circulação externa. A responsabilidade civil precisa reconhecer essa complexidade sem abandonar o nexo causal. O problema é determinar se a falha da plataforma foi juridicamente relevante para criar, ampliar ou conservar o risco que se concretizou (SCHREIBER, 2015; TEPEDINO; TERRA; GUEDES, 2024).

A presunção de causalidade deve ser relativa. Ela não decorre automaticamente da idade da vítima nem da existência de dano. Surge quando há indícios de falha, assimetria informacional e controle empresarial de dados essenciais. Nesses casos, a plataforma pode ser chamada a demonstrar como funcionavam seus sistemas, que resposta foi adotada e por que o dano não se relaciona à sua conduta (MULHOLLAND, 2009).

A distribuição dinâmica do ônus da prova é instrumento adequado para lidar com essa assimetria. A família pode apresentar narrativa, capturas de tela, protocolos de denúncia e efeitos do dano. A plataforma, por sua vez, possui *logs*, métricas, histórico de moderação e documentação interna. A prova deve ser distribuída conforme a capacidade real de cada parte produzir os elementos relevantes (BRASIL, 2015a).

Essa redistribuição deve respeitar contraditório e proporcionalidade. Não se pode exigir da plataforma prova impossível, nem aceitar alegações genéricas da vítima sem base mínima. O equilíbrio está em exigir colaboração técnica quando houver plausibilidade do dano e indicação de que a informação decisiva está sob controle do fornecedor.

A causalidade também pode ser analisada por campos de risco. Se o dano ocorreu dentro do risco criado ou ampliado pela atividade da plataforma, a imputação ganha força. Se o evento é totalmente estranho ao serviço, imprevisível ou decorrente de fato exclusivo de terceiro, a responsabilidade pode ser afastada. Essa distinção preserva a coerência da imputação objetiva.

Diante desses fundamentos, observa-se que presunção relativa e distribuição dinâmica não são atalhos para condenação. São técnicas para impedir que a opacidade técnica torne inviável a proteção de menores. Sua legitimidade depende de base fática, dever identificável, possibilidade de prova contrária e vínculo com o risco organizado pela plataforma.

Essas técnicas, porém, não autorizam condenação sem base fática. A vítima deve apresentar narrativa plausível do dano, indicar o serviço envolvido, a funcionalidade relevante e a relação provável com a falha alegada. A plataforma, por sua vez, deve demonstrar registros de resposta, políticas aplicadas, medidas de prevenção e limites técnicos. A presunção opera como mecanismo de equilíbrio informacional, não como substituto absoluto do nexo causal.

A causalidade em danos digitais raramente é linear. Um dano pode resultar de publicação de terceiro, recomendação automatizada, demora de resposta, ausência de bloqueio, falha de privacidade e circulação posterior em outros ambientes. Exigir da vítima a reconstrução integral dessa cadeia pode inviabilizar a tutela. Por isso, presunções relativas e distribuição dinâmica do ônus da prova são instrumentos úteis quando há indícios mínimos de falha e a informação técnica está concentrada na plataforma (MULHOLLAND, 2009; BRASIL, 2015a).

Sob o ângulo teórico, a presunção de causalidade é instrumento de racionalização probatória, não atalho condenatório. Ela se justifica quando a plataforma controla informações que poderiam esclarecer a cadeia do dano e não as apresenta adequadamente. Ainda assim, a decisão deve explicar por que os indícios são suficientes, que dever foi descumprido e como a falha se relaciona ao resultado lesivo.

A causalidade também deve considerar riscos concorrentes. Comportamento de terceiro, atuação da vítima, falha familiar, caso fortuito e omissão da plataforma podem coexistir. A responsabilidade civil não precisa ignorar essa pluralidade; pode admitir concorrência causal, redução de indenização ou exclusão quando o dano decorrer exclusivamente de fato externo. A análise deve distinguir contribuição relevante da plataforma de mera presença passiva no ambiente digital (CAVALIERI FILHO, 2024).

A prova digital exige cuidado com autenticidade, contexto e preservação. Capturas isoladas podem ser insuficientes quando não permitem identificar data, alcance, repetição ou resposta. Por outro lado, exigir da vítima prova técnica completa

do algoritmo pode inviabilizar a tutela. O equilíbrio está em combinar indícios externos apresentados pela vítima com dever de explicação da plataforma sobre elementos internos sob seu controle (MULHOLLAND, 2009).

A distribuição dinâmica do ônus da prova possui papel central porque os dados decisivos costumam estar sob controle empresarial. A família pode apresentar capturas de tela, relatos, datas, protocolos e consequências do dano; a plataforma deve explicar seus registros, fluxos de resposta e critérios gerais de funcionamento quando esses elementos forem relevantes. Essa técnica não transfere integralmente a prova para o fornecedor, mas ajusta o processo à realidade informacional do litígio (BRASIL, 2015a; MULHOLLAND, 2009).

A presunção relativa de causalidade só é legítima quando vinculada a elementos concretos. Denúncia reiterada não respondida, ausência de *logs*, descumprimento de política de segurança, recomendação persistente ou falha de preservação de evidências podem justificar inferência desfavorável à plataforma. Porém, a presunção deve admitir prova em contrário e não pode converter-se em condenação automática sempre que houver dano a menor (TEPEDINO; TERRA; GUEDES, 2024).

A causalidade em danos digitais complexos raramente aparece de forma linear. O dano pode resultar da combinação entre conteúdo de terceiro, recomendação automatizada, demora de resposta, coleta de dados e comportamento de usuários. A dificuldade não autoriza presunção absoluta, mas exige técnicas de reconstrução adequadas. O nexo deve ser analisado por indícios, documentação disponível, domínio informacional e plausibilidade do encadeamento (MULHOLLAND, 2009; BRASIL, 2015a).

A colaboração processual da plataforma deve ser compatível com sua posição profissional. Empresas que exploram ambientes digitais de grande escala possuem equipes, sistemas e registros aptos a esclarecer fatos. Quando se recusam genericamente a produzir informações, aumentam a assimetria que caracteriza o dano digital. A cooperação não significa renúncia a defesa, mas cumprimento do dever processual de contribuir para a verdade possível.

A prova por indícios merece atenção especial. Em ambientes digitais, a vítima pode não demonstrar diretamente cada etapa técnica, mas pode apresentar sequência temporal coerente, *prints*, protocolos, testemunhos e efeitos observados. Esses elementos formam base para exigir explicação da plataforma. A decisão deve

avaliar se os indícios apontam para falha plausível, e não exigir certeza técnica impossível desde o início da demanda.

Essa base prepara o enfrentamento do Marco Civil porque mostra que a discussão não deve ser reduzida ao seu art. 19. O regime de conteúdo de terceiro é importante, mas não esgota falhas próprias de arquitetura, proteção de dados e resposta institucional. O capítulo seguinte analisará justamente como compatibilizar o regime geral da internet com a especialidade protetiva do ECA Digital.

A consequência prática do capítulo é estabelecer que o dever de cuidado não é abstrato. Ele nasce da posição concreta do fornecedor diante do ambiente que organiza. Quando a plataforma conhece seu público, monetiza atenção, controla dados e define a circulação de conteúdo, sua omissão pode ter relevância civil. Quando não controla o risco, não tem ciência qualificada ou enfrenta evento externo inevitável, os limites da imputação devem ser preservados.

A presunção de causalidade deve operar como técnica excepcional de reconstrução, e não como substituição completa da prova. Sua aplicação exige indícios de que a plataforma controlava a funcionalidade relevante, que houve descumprimento de dever e que o dano é compatível com o risco criado. A partir desse núcleo mínimo, pode-se exigir do fornecedor explicação sobre registros, recomendações, denúncias e medidas de mitigação. Se a vítima não apresenta nenhuma conexão plausível entre serviço e dano, a opacidade tecnológica não basta para inverter automaticamente o resultado do processo (MULHOLLAND, 2009; BRASIL, 2015a).

A distribuição dinâmica do ônus probatório deve ser específica. O juiz precisa indicar qual fato depende de informação sob controle da plataforma e quais documentos são necessários para esclarecê-lo. Ordens genéricas de apresentação de todos os dados podem violar privacidade de terceiros, segredos empresariais e proporcionalidade. Relatórios agregados, perícia sob sigilo, amostras técnicas e preservação de logs relacionados ao caso oferecem alternativas menos invasivas. A técnica processual deve reduzir assimetria sem converter a fase probatória em punição antecipada (BRASIL, 2015a; SARLET *et al*., 2021).

A preservação tempestiva de evidências é decisiva porque registros digitais podem ser apagados ou substituídos por rotinas automáticas. A ciência de denúncia grave pode gerar dever de conservar informações relacionadas ao alcance, à resposta e à moderação, respeitados limites temporais e de proteção de dados. Se a empresa,

após provocação adequada, elimina elementos indispensáveis sem justificativa, o comportamento pode influenciar a valoração da prova. A consequência, contudo, deve ser fundamentada e relacionada ao prejuízo concreto causado à reconstrução dos fatos (BRASIL, 2018; BRASIL, 2025a).

A articulação entre os fundamentos civil-constitucionais demonstra que a responsabilidade das plataformas não depende de um único diploma. O núcleo da argumentação está na convergência entre prioridade absoluta, proteção integral, risco da atividade, relação de consumo, proteção de dados e técnica probatória. Essa convergência torna possível exigir das plataformas uma postura de governança sem desorganizar o sistema geral de responsabilidade civil.

A causalidade pode ser analisada por camadas. A primeira identifica o evento inicial; a segunda, os mecanismos de amplificação; a terceira, a resposta após ciência; a quarta, os efeitos individuais. Essa decomposição evita atribuir todo o dano à plataforma ou ignorar sua contribuição. Em uma campanha de assédio, o autor cria conteúdo, usuários replicam, o algoritmo amplia e a demora prolonga. Cada camada pode gerar responsabilidade proporcional.

Logs e métricas devem ser interpretados com cautela. Alcance elevado não prova, sozinho, que o algoritmo causou o dano, pois compartilhamentos orgânicos também influenciam. A comparação entre tráfego recomendado e direto, mudanças após impulsionamento e comportamento de contas pode oferecer indícios. Perícia deve formular perguntas funcionais e não exigir reprodução impossível de sistemas dinâmicos.

A presunção relativa é adequada quando três condições coexistem: plausibilidade da narrativa, controle exclusivo da prova e resistência injustificada à exibição. Ela deve ser específica sobre o fato presumido, como recebimento de denúncia ou uso de impulsionamento. Não pode presumir simultaneamente dever, violação, dano e nexo. A delimitação preserva contraditório e incentiva conservação documental.

A distribuição dinâmica deve ser decidida antes do encerramento da instrução, permitindo que a parte cumpra o encargo. Decisões-surpresa que invertem o ônus apenas na sentença violam devido processo. O juiz deve indicar quais documentos são esperados e por que estão sob controle da empresa. A vítima continua responsável por demonstrar dano e fornecer elementos mínimos de identificação.

A prova pericial pode ser complementada por auditorias independentes, relatórios de transparência e pesquisas. Fontes agregadas não substituem dados do caso, mas ajudam a avaliar plausibilidade. A combinação de evidências técnicas, testemunhais e documentais é mais adequada do que busca por prova única. Essa abordagem corresponde à natureza multifatorial dos danos digitais.

A decisão judicial deve explicar o raciocínio probatório. Não basta declarar que a plataforma detinha informações ou que a vítima era vulnerável. É preciso indicar quais informações eram relevantes, por que estavam sob controle do fornecedor, quais indícios foram apresentados e de que modo a ausência de esclarecimento autoriza inferência causal. Esse cuidado aumenta legitimidade e reduz risco de responsabilização automática.

A análise causal também deve considerar o comportamento posterior da plataforma. Uma falha inicial pode ser mitigada por resposta rápida e eficaz; uma falha menor pode ser agravada por demora injustificada ou ausência de documentação. O nexo não é apenas relação entre tecnologia e dano, mas cadeia entre risco, alerta, conduta institucional e resultado. Essa visão temporal é mais adequada a ambientes digitais.

O ônus da prova pode incluir dever de exibição de documentos ou informações técnicas. Relatórios, *logs*, políticas de moderação e registros de denúncia podem ser apresentados sob sigilo processual quando envolverem segredo empresarial ou dados de terceiros. A confidencialidade não deve impedir a instrução, mas pode exigir medidas de proteção. Essa solução preserva prova, privacidade e contraditório.

A presunção relativa também precisa ser calibrada pelo tipo de dano. Em exposição íntima, o tempo de resposta e a redução de alcance podem ser centrais. Em recomendação algorítmica, a repetição e os critérios gerais de ranqueamento ganham importância. Em publicidade comportamental, a segmentação e os dados utilizados tornam-se relevantes. Cada hipótese demanda prova diferente, o que impede modelos decisórios padronizados.

A complexidade causal não pode ser pretexto para negar tutela. Se a vítima demonstra exposição, denúncia, resposta insuficiente e dano plausível, a plataforma pode ser chamada a esclarecer o funcionamento do serviço. A dificuldade técnica deve ser enfrentada com ferramentas processuais, não com indeferimento automático. O processo civil fornece instrumentos para adequar a prova à distribuição real de informações entre as partes.

A decisão sobre ônus da prova deve ser motivada. O juiz precisa explicar por que determinada informação é acessível à plataforma, por que a vítima não a poderia obter e como ela influencia a solução do caso. Esse dever de motivação impede inversões automáticas e fortalece a legitimidade da técnica probatória em ambiente digital.

A presunção relativa de causalidade deve ser especialmente cuidadosa em danos emocionais. É possível que fatores externos concorram para o sofrimento da vítima. A plataforma responderá quando sua falha for contribuição juridicamente relevante, não quando houver mera coincidência temporal. Laudos, registros de exposição, denúncias e comportamento posterior podem auxiliar a reconstrução do vínculo.

4 REGIME GERAL DO MARCO CIVIL DA INTERNET, TEMAS 987 E 533 DO STF E A ESPECIALIDADE PROTETIVA DO ECA DIGITAL

A relação entre a tutela infantojuvenil e as garantias do Marco Civil da *Internet* não pode ser reduzida a uma escolha entre diplomas incompatíveis. A norma aplicável depende do comportamento atribuído à plataforma. Quando a controvérsia se limita à permanência de conteúdo produzido por terceiro, o art. 19 ocupa posição central. Se o caso envolve recomendação, desenho, publicidade, tratamento de dados ou falha de um canal próprio, examina-se uma conduta institucional que pode atrair fundamentos distintos. Essa distinção funcional organiza o diálogo normativo e evita tanto a ampliação indiscriminada quanto a restrição excessiva da responsabilidade (SOUZA; LEMOS, 2016; FRAZÃO, 2022).

Os Temas 987 e 533 da repercussão geral devem ser compreendidos a partir das questões efetivamente submetidas ao Supremo Tribunal Federal. A redefinição dos limites do art. 19 repercute sobre liberdade de expressão, remoção de conteúdo e segurança jurídica, mas não oferece resposta automática para deveres de proteção de dados, segurança por desenho ou publicidade dirigida. O capítulo utiliza esses precedentes como marcos de coordenação e preserva a incidência especial do ECA Digital quando o dano é relacionado a comportamento próprio da plataforma (BRASIL, 2025b; BRASIL, 2025c).

Nos litígios que envolvem sistemas algorítmicos, a prova útil não se confunde com a revelação integral da arquitetura técnica do serviço. Dados agregados sobre alcance, sequência de recomendações, tempo de resposta, aplicação de filtros e histórico de denúncias podem ser suficientes para esclarecer a controvérsia. A instrução deve buscar informação proporcional ao objeto do processo, evitando tanto a opacidade absoluta quanto uma devassa técnica sem relação com o dano alegado.

4.1 Art. 19 do Marco Civil da Internet e ordem judicial específica

O art. 19 do Marco Civil da Internet foi concebido para evitar responsabilização automática de provedores por conteúdos gerados por terceiros e para preservar liberdade de expressão, segurança jurídica e devido processo. A regra da ordem judicial específica atua como filtro contra remoções privadas excessivas e contra imposição de dever genérico de monitoramento (BRASIL, 2014a; SOUZA; LEMOS, 2016).

Essa disciplina continua relevante para a dissertação. Quando a pretensão se funda apenas na permanência de conteúdo produzido por terceiro, o art. 19 estabelece parâmetro importante para definir quando a plataforma passa a responder civilmente. O regime geral, porém, não resolve todas as hipóteses de dano digital, especialmente quando o problema envolve falha própria de arquitetura, recomendação, publicidade, dados ou resposta institucional.

A distinção entre conteúdo de terceiro e conduta própria do serviço é decisiva. A plataforma não se torna autora da postagem alheia por organizar o ambiente; mas pode praticar conduta juridicamente relevante quando amplia alcance, induz permanência, ignora alertas consistentes, falha em canal de denúncia ou não adota padrões proporcionais de segurança em serviço acessado por menores (TEFFÉ, 2015; FRAZÃO, 2022).

O ECA Digital não deve ser interpretado como revogação do Marco Civil. A leitura mais consistente é a de diálogo entre regimes. O Marco Civil protege garantias comunicativas e processuais; o ECA Digital densifica deveres especiais quando o público infantojuvenil está envolvido. O conflito aparente se reduz quando se pergunta qual é a conduta imputada: não remoção de conteúdo de terceiro ou descumprimento de dever próprio de cuidado.

A ordem judicial específica também não impede tutelas urgentes ou medidas preventivas quando houver base legal e risco relevante. O ponto é que a intervenção deve ser delimitada, proporcional e vinculada ao dever violado. A proteção de menores não autoriza ordens vagas, mas pode justificar resposta mais intensa quando o risco é previsível e a plataforma possui meios concretos de mitigação.

A regulação da internet brasileira também precisa ser compreendida como processo institucional em permanente tensão entre desenvolvimento, liberdade e proteção. Melo (2018), ao examinar a neutralidade da rede, demonstra que escolhas regulatórias não são neutras em relação à distribuição de poder entre usuários, empresas e Estado. Essa leitura ajuda a compreender por que o art. 19 não pode ser analisado isoladamente: a regra de responsabilidade integra uma arquitetura regulatória mais ampla, na qual incentivos econômicos e capacidades técnicas moldam o alcance efetivo dos direitos.

A literatura recente também evidencia que o desafio contemporâneo não se limita à retirada de conteúdos. Almeida e Penaforte (2025) relacionam o Marco Civil às novas formas de circulação de desinformação e aos limites da responsabilidade de

provedores, enquanto Castro (2023) mostra, em campo específico, como a imputação por atos de terceiros exige distinguir hospedagem, controle e participação funcional do serviço. Essas contribuições reforçam a necessidade de separar omissão diante de conteúdo alheio, atuação própria de amplificação e descumprimento de dever autônomo.

No mesmo sentido, o Recurso Especial nº 1.783.269/MG oferece parâmetro relevante para situações envolvendo crianças e adolescentes, pois o Superior Tribunal de Justiça reconheceu que a proteção do menor pode exigir leitura sistemática do Marco Civil e do Estatuto da Criança e do Adolescente. O precedente não autoriza responsabilização automática, mas confirma que a especialidade protetiva e a gravidade do dano devem influenciar a definição do dever de resposta da plataforma (BRASIL, 2021; PEREIRA; LARA, 2022).

Com isso, o art. 19 funciona como limite e ponto de partida. Ele impede responsabilização genérica por conteúdo de terceiro, mas não imuniza a plataforma por falhas próprias de organização. A proposta de responsabilidade objetiva por falha própria de organização depende precisamente dessa distinção.

A compatibilização com o ECA Digital exige distinguir pedido de remoção de conteúdo e dever de segurança do serviço. Se a discussão é apenas a postagem ilícita de terceiro, o art. 19 permanece central. Se a discussão envolve falha de canal de denúncia, ausência de salvaguarda para menores, tratamento de dados ou ampliação algorítmica do risco, a análise passa a abranger deveres próprios da plataforma. Essa distinção evita tanto a erosão do Marco Civil quanto a neutralização da proteção especial.

A especificidade da ordem judicial cumpre função processual e tecnológica. A decisão deve permitir a identificação do conteúdo ou da funcionalidade atingida e indicar a providência esperada. Em ambientes dinâmicos, a simples referência a uma URL pode ser insuficiente quando há republicação automatizada ou rede de contas; por outro lado, ordens genéricas de bloqueio podem alcançar material lícito. A técnica decisória deve combinar precisão, exequibilidade e proporcionalidade.

A ordem judicial específica não deve ser utilizada como escudo para ausência de governança. O provedor pode não responder por conteúdo de terceiro antes de ordem nas hipóteses do art. 19, mas ainda pode ser questionado por falhas na organização do serviço que não dependam da identificação prévia de um conteúdo

específico. Essa separação preserva o núcleo do Marco Civil e permite concretizar a proteção infantojuvenil.

A causa de pedir organiza a incidência das normas. Pretensões baseadas exclusivamente na permanência de postagem de terceiro permanecem próximas do art. 19. Demandas sobre perfilamento, publicidade, recomendação, desenho inseguro ou falha de canal de denúncia exigem a indicação de dever autônomo. Essa classificação deve constar desde a petição inicial e ser enfrentada na decisão, pois define prova, defesa e modalidade de tutela.

O art. 21 do Marco Civil, embora específico, demonstra que o próprio sistema admite tratamento diferenciado para certos danos sensíveis. A lógica de proteção de intimidade e exposição de imagens revela que a lei não adotou neutralidade absoluta em todos os casos. A interpretação sistemática deve reconhecer essa abertura, especialmente quando o ECA Digital acrescenta deveres especiais para crianças e adolescentes (BRASIL, 2014a; BRASIL, 2025a).

A ordem judicial específica possui função procedimental. Ela delimita o conteúdo a ser removido, reduz incerteza para o provedor e protege contra censura privada. Contudo, a existência dessa regra não impede que a plataforma tenha deveres próprios de arquitetura, privacidade, proteção de dados e resposta a incidentes envolvendo menores. A responsabilidade por descumprimento desses deveres não se confunde necessariamente com responsabilidade por conteúdo de terceiro (TEFFÉ, 2015; MEDEIROS, 2020).

A dificuldade surge quando o dano não decorre apenas da permanência do conteúdo, mas da forma como o serviço o organiza. Recomendação algorítmica, impulsionamento, publicidade associada, falha de denúncia e ausência de preservação de registros podem deslocar a análise para a conduta institucional da plataforma. Nesses casos, o art. 19 não deve ser ignorado, mas também não pode absorver todos os deveres de segurança e prevenção previstos em outros microssistemas (FRAZÃO, 2022; BRASIL, 2025a).

Os deveres da plataforma podem surgir em momentos distintos. Antes de qualquer aviso, existem obrigações gerais de segurança, privacidade, transparência e governança compatíveis com o serviço. Após notificação qualificada, podem surgir deveres de registrar, avaliar risco, preservar prova, reduzir alcance ou encaminhar o caso. Depois da ordem judicial, incide obrigação específica de cumprimento. A

separação temporal evita tratar toda ciência como equivalente e melhora a análise do nexo.

A natureza da falha também determina a resposta jurídica. Conteúdo específico pode exigir indisponibilização; recomendação nociva pode justificar desamplificação; tratamento irregular de dados pode demandar bloqueio ou eliminação; publicidade abusiva pode exigir interrupção da campanha; falha estrutural pode requerer ajuste de processo. A indenização é apenas uma das consequências possíveis e deve corresponder ao dano efetivamente demonstrado.

A proteção de menores exige cuidado especial na aplicação do art. 19. A exigência de ordem judicial não pode impedir medidas internas proporcionais para riscos graves e evidentes, como canais de denúncia acessíveis ou políticas de redução de alcance. Ao mesmo tempo, a proteção infantojuvenil não autoriza remoção indiscriminada de conteúdo lícito. O equilíbrio depende de diferenciar moderação voluntária, dever legal e responsabilidade civil.

É necessário separar fundamento de responsabilidade e técnica de tutela. O art. 19 pode limitar a indenização fundada na ausência de remoção, mas não impede medidas preventivas ou probatórias baseadas em outros deveres legais. Do mesmo modo, a existência de dever de segurança não autoriza automaticamente retirar manifestação cuja ilicitude dependa de ponderação judicial. Cada providência deve guardar correspondência com a norma e com o risco alegado.

Mesmo quando a remoção depende de ordem judicial, a preservação de evidências pode ser exigível antes dela. *Logs* de denúncia, histórico de alcance, registros de impulsionamento e decisões de moderação são perecíveis e podem desaparecer por rotinas automáticas. A manutenção temporária desses elementos, dentro dos limites da LGPD e do Marco Civil, não antecipa juízo sobre ilicitude; apenas assegura que o processo disponha de informação suficiente.

A interpretação do art. 19 deve levar em conta seu contexto histórico. O dispositivo surgiu em momento de preocupação com remoção privada excessiva, insegurança dos intermediários e riscos à liberdade de expressão. Essa finalidade continua válida. Contudo, a transformação das plataformas em ambientes de recomendação, publicidade e coleta de dados exige distinguir o problema original da hospedagem passiva de conteúdo de novos riscos ligados à organização ativa da experiência.

A plataforma pode adotar medidas voluntárias de segurança sem que isso configure reconhecimento automático de responsabilidade. Incentivar boas práticas não deve punir quem modera de forma diligente. A responsabilidade deve recair sobre omissões relevantes ou medidas inadequadas, não sobre o simples fato de a empresa possuir política de proteção. Esse ponto é essencial para evitar efeito desestimulante.

A ordem judicial específica possui importância probatória, pois delimita ciência inequívoca do provedor. Porém, a ciência também pode surgir de outros modos em situações de risco grave, especialmente quando há canal próprio de denúncia ou monitoramento interno. A construção aqui defendida não elimina a exigência legal, mas reconhece que deveres próprios da plataforma podem existir independentemente de ordem quando não se trata apenas de remover conteúdo.

A diferenciação entre remover e deixar de recomendar oferece solução menos restritiva em alguns casos. Conteúdo cuja ilicitude ainda é controvertida pode permanecer acessível sem ser promovido a usuários menores ou vulneráveis, desde que exista base técnica e jurídica para a redução de alcance. Essa alternativa não substitui a ordem judicial quando necessária, mas demonstra que a governança da circulação admite medidas graduais entre inércia e exclusão total.

O art. 19 também deve ser interpretado em conjunto com a exceção de conteúdos de nudez e atos sexuais de caráter privado prevista no próprio Marco Civil. Essa exceção revela que o legislador reconheceu graus diferentes de urgência e gravidade. Em matéria infantojuvenil, essa lógica reforça a necessidade de canais rápidos para riscos graves, sempre distinguindo remoção de conteúdo, preservação de prova e responsabilidade indenizatória.

A proteção infantojuvenil exige resposta graduada conforme a clareza da ilicitude e a gravidade do risco. Exploração sexual, aliciamento ou incentivo direto à automutilação justificam atuação rápida e preservação imediata de prova. Críticas, sátiras e controvérsias políticas demandam maior cautela. O fato de o usuário ser menor intensifica o dever de avaliação, mas não elimina contexto, contraditório e liberdade de expressão.

A notificação extrajudicial pode desempenhar funções diferentes. Em certas hipóteses, não basta para gerar responsabilidade pela manutenção do conteúdo; em outras, demonstra ciência de risco, ativa dever de preservar prova, exige resposta em canal especializado ou revela que a empresa continuou impulsionando material reconhecidamente nocivo. O efeito jurídico depende do tipo de dano e do dever

invocado. Essa diferenciação evita tanto a substituição indiscriminada da ordem judicial quanto a irrelevância absoluta de comunicações privadas em situações graves (FRAZÃO, 2022; MEDEIROS, 2020).

A interpretação do art. 19 deve ainda considerar a tutela de urgência. Em danos que se multiplicam rapidamente, a demora pode comprometer a utilidade da decisão. Ordens específicas podem indicar URL, perfil, conteúdo ou funcionalidade, mas precisam ser tecnicamente exequíveis e proporcionais. Bloqueios amplos, filtros genéricos e vigilância prévia podem afetar conteúdos lícitos; medidas excessivamente estreitas podem ser ineficazes. A proteção adequada exige diálogo entre precisão jurídica e funcionamento técnico da plataforma (SOUZA; LEMOS, 2016; PEREIRA; LARA, 2022).

A notificação privada pode produzir efeitos múltiplos sem substituir automaticamente a ordem judicial. Ela pode demonstrar ciência, acionar protocolo de emergência, exigir preservação de registros, interromper impulsionamento ou iniciar revisão interna. Seu efeito indenizatório dependerá da qualidade da comunicação, da natureza do conteúdo, do dever invocado e do tempo de resposta. Essa leitura evita tanto a irrelevância absoluta da notificação quanto sua conversão em ordem privada de censura.

A revisão do Marco Civil também precisa considerar a mudança do ambiente informacional. Almeida e Penaforte observam que a circulação de desinformação, discursos de ódio e práticas de manipulação desafia um modelo concebido para uma etapa anterior da internet, exigindo atualização que preserve liberdade de expressão, pluralidade e proteção dos usuários. Para esta dissertação, a contribuição é útil porque mostra que a responsabilidade não pode ser resolvida apenas pela oposição entre remoção e não remoção; ela deve alcançar transparência, governança e resposta proporcional quando a infraestrutura favorece a propagação de riscos (ALMEIDA; PENAFORTE, 2025).

A experiência de outros regimes de notificação também oferece uma cautela metodológica. Embora Castro examine infrações autorais, sua comparação entre *notice and takedown*, *notice and stay down* e *notice and notice* evidencia que o desenho do procedimento altera o equilíbrio entre vítima, usuário e intermediário. A transposição para danos infantojuvenis não é automática, mas permite sustentar que notificações devem ter critérios, contraditório quando compatível com a urgência, preservação de evidências e resposta diferenciada segundo a gravidade. O dever de

tratamento da denúncia é mais preciso do que uma obrigação abstrata de monitoramento universal (CASTRO, 2023).

4.2 Tema 987 da repercussão geral

O Tema 987 da repercussão geral foi julgado pelo Supremo Tribunal Federal em conjunto com o Tema 533, com conclusão do mérito em 26 de junho de 2025. O Tribunal reconheceu a inconstitucionalidade parcial e progressiva do art. 19 do Marco Civil da Internet e estruturou regime diferenciado segundo a natureza do conteúdo, a forma de ciência do provedor e a existência de atuação própria ou falha sistêmica. O julgamento não suprimiu integralmente a exigência de ordem judicial, mas afastou sua utilização como condição universal de responsabilização (BRASIL, 2025b; BRASIL, 2025c).

A tese fixada preserva o art. 19 em determinados campos, mas afasta sua aplicação como barreira universal à responsabilização. A distinção central passa a ser a natureza do conteúdo, o papel da plataforma, o conhecimento sobre a ilicitude e a existência de dever próprio de atuação. Isso aproxima a jurisprudência constitucional da premissa desenvolvida neste trabalho: a imputação não decorre da simples existência de dano no ambiente digital, mas da identificação de uma posição de controle acompanhada por obrigação juridicamente exigível.

Em relação ao conteúdo gerado por terceiros, a decisão reconhece que a ordem judicial continua relevante, sobretudo quando a ilicitude depende de apreciação contextual ou de ponderação entre direitos da personalidade e liberdade de expressão. Entretanto, o Tribunal admitiu hipóteses nas quais a notificação extrajudicial, a manifesta ilicitude ou o envolvimento direto do provedor podem produzir dever de indisponibilização sem a espera de comando judicial. Essa flexibilização não elimina a necessidade de precisão: a comunicação deve permitir localizar o conteúdo, compreender o risco e avaliar a providência adequada (BRASIL, 2025b; TEFFÉ, 2015).

A inconstitucionalidade parcial do art. 19 também precisa ser compreendida à luz de sua finalidade histórica. O dispositivo buscou impedir que intermediários removessem conteúdos por receio de condenação, criando proteção à liberdade de expressão e à inovação. O STF não rejeitou esse objetivo, mas entendeu que a regra, aplicada de maneira absoluta, poderia converter-se em insuficiência protetiva diante de ilícitos graves e de modelos de negócio capazes de ampliar alcance e persistência.

O resultado é um regime mais diferenciado, no qual a proteção da expressão convive com deveres de cuidado proporcionais.

Para a proteção de crianças e adolescentes, a relevância do Tema 987 é particularmente intensa. Conteúdos que estimulem automutilação, exploração sexual, violência contra escolas ou outras práticas gravemente lesivas podem exigir resposta imediata, especialmente quando a plataforma dispõe de sinais claros e meios técnicos para contenção. A condição peculiar de desenvolvimento não autoriza monitoramento ilimitado, mas eleva a exigência de diligência quando a ilicitude é manifesta e o risco de dano irreversível é concreto (BRASIL, 1988; BRASIL, 1990a; BRASIL, 2025b).

O julgamento permite distinguir três planos de responsabilidade. No primeiro, discute-se a postagem de terceiro cuja ilicitude depende de avaliação judicial; nesse caso, a ordem específica mantém função importante. No segundo, o conteúdo é manifestamente ilícito ou se enquadra em categoria de risco qualificado, tornando possível exigir atuação independente de decisão prévia. No terceiro, o dano decorre de ato próprio do provedor, como impulsionamento, publicidade, recomendação ou desenho inseguro; nessa hipótese, o art. 19 não deve servir de escudo para conduta empresarial autônoma.

Essa tripartição evita que a controvérsia seja reduzida à oposição entre responsabilidade automática e imunidade. A responsabilidade objetiva defendida neste trabalho opera sobretudo nos planos em que há dever próprio, risco organizado e capacidade concreta de prevenção. Nos casos de conteúdo de terceiro sem contribuição estrutural do serviço, os filtros do Marco Civil e da jurisprudência constitucional continuam relevantes. A coerência depende de identificar a fonte do dano antes de escolher o regime de imputação.

O Tema 987 também fortalece a análise da ciência do provedor. A ciência não é categoria binária. Pode resultar de notificação específica, de denúncias reiteradas, de identificação automática confiável, de decisão administrativa ou da própria participação da plataforma na difusão do conteúdo. Quanto maior a clareza do sinal e a gravidade do risco, menor a justificativa para inércia. Em contrapartida, comunicações genéricas ou disputas interpretativas complexas podem exigir cautela, contraditório e delimitação judicial.

No campo probatório, a decisão reforça a importância de documentação. A plataforma deve ser capaz de demonstrar quando recebeu a informação, quais medidas adotou, que critérios utilizou e em quanto tempo respondeu. A vítima, por

sua vez, deve individualizar o fato, o dano e os indícios de conexão com o serviço. A distribuição dinâmica do ônus da prova não dispensa alegação mínima, mas impede que registros exclusivamente empresariais sejam usados como barreira à tutela jurisdicional (BRASIL, 2015a; MULHOLLAND, 2009).

Um exemplo ajuda a concretizar o regime. Se um usuário publica crítica contundente cuja ilicitude é controvertida, a plataforma não deve ser compelida a remover automaticamente sob pena de indenização. Situação diversa ocorre quando recebe denúncia precisa sobre vídeo que expõe sexualmente adolescente, confirma a existência do material e permanece inerte. Mais distinta ainda é a hipótese em que o próprio sistema recomenda repetidamente esse vídeo a perfis de menores. Cada cenário possui grau diferente de controle, previsibilidade e contribuição causal.

A decisão do STF também tem dimensão institucional. Ao reconhecer omissão parcial do legislador, o Tribunal formulou parâmetros transitórios e preservou espaço para futura disciplina legislativa. O ECA Digital integra essa evolução normativa ao estabelecer deveres específicos de proteção infantojuvenil. A lei especial não revoga a tese constitucional, mas oferece critérios adicionais para determinar quando o serviço deveria antecipar riscos, adaptar desenho, limitar exposição ou responder a denúncias.

Em 17 de junho de 2026, o Supremo Tribunal Federal concluiu o julgamento dos embargos de declaração nos Recursos Extraordinários vinculados aos Temas 987 e 533. A Corte aperfeiçoou a formulação da tese e estabeleceu prazo de 60 dias para implementação das medidas estruturais impostas aos provedores. Os embargos não substituíram o núcleo do julgamento de 2025; esclareceram sua operacionalização e consolidaram os deveres de autorregulação, transparência, canais de atendimento e resposta compatíveis com o novo regime (BRASIL, 2026c).

A aplicação do Tema 987 ao ECA Digital exige coordenação, não sobreposição. O julgador deve primeiro identificar se a pretensão se refere a conteúdo de terceiro, a falha sistêmica, a tratamento de dados, a publicidade, a recomendação ou a ausência de resposta. Em seguida, deve verificar qual dever legal incidia e se a conduta da plataforma contribuiu causalmente para o dano. Somente depois é possível definir se a ordem judicial prévia era necessária ou se havia obrigação autônoma de atuação.

O julgamento também impõe limite à generalização do dever de monitoramento. A proteção reforçada de menores não autoriza vigilância indiscriminada de comunicações privadas nem filtragem total de conteúdos legítimos.

Medidas preventivas devem observar adequação, necessidade, transparência e proporcionalidade. Ferramentas de detecção, sistemas de denúncia e controles de recomendação podem ser exigíveis em certas atividades, mas sua avaliação deve considerar o tipo de serviço, a escala, o risco e os efeitos sobre direitos fundamentais.

Na perspectiva da função social do direito, o Tema 987 desloca o debate para a qualidade da governança. A plataforma que organiza circulação de informação em grande escala não pode invocar neutralidade absoluta quando suas escolhas técnicas interferem no alcance de conteúdos. Ao mesmo tempo, a sociedade preserva interesse em espaços de expressão plural e em regras previsíveis. A decisão constitucional procura equilibrar essas dimensões mediante critérios de conhecimento, diligência, gravidade e contribuição própria.

A decisão permite afirmar, em caráter intermediário, que o Tema 987 fornece base constitucional para superar a leitura rígida do art. 19 sem instaurar responsabilidade integral. Sua contribuição para esta dissertação está em reconhecer que a proteção jurídica depende da natureza do ilícito e da função exercida pela plataforma. Quando o dano infantojuvenil decorre de dever próprio descumprido, recomendação, publicidade, tratamento de dados ou inércia diante de risco manifesto, a responsabilidade pode ser examinada fora do modelo restrito de ordem judicial específica, preservados o dano, o nexo e as excludentes cabíveis.

A proteção contra conteúdos graves também exige distinguir obrigação de indisponibilização e obrigação de impedir recomendação. Um material pode permanecer acessível por endereço específico enquanto deixa de ser promovido a usuários vulneráveis, ou pode exigir remoção completa diante de ilicitude manifesta. A decisão adequada depende da natureza do direito, da certeza jurídica e do risco de propagação. Essa gradação oferece alternativas menos restritivas do que remoção universal em controvérsias complexas.

O Tema 987 repercute ainda sobre mecanismos de busca e indexação. A responsabilidade de uma rede social que recomenda conteúdo não é idêntica à de ferramenta que apenas apresenta resultado solicitado. Contudo, mesmo motores de busca podem possuir deveres específicos quando recebem ordem ou notificação qualificada sobre materiais gravemente ilícitos. A análise funcional impede aplicação indistinta da tese a serviços com arquiteturas diversas.

Em litígios envolvendo crianças, a preservação da identidade merece consideração autônoma. A retirada do conteúdo não basta se decisões judiciais, URLs

ou resultados de busca continuarem expondo nome e imagem. Medidas de anonimização e desindexação podem integrar a tutela, desde que não apaguem informações de interesse público legítimo. O equilíbrio exige avaliar idade, tempo transcorrido e finalidade da manutenção.

A jurisprudência constitucional também influencia acordos privados de moderação. Termos de uso podem proibir conteúdos além do mínimo legal, mas sua aplicação deve ser transparente e não discriminatória. Quando a plataforma promete proteção específica e falha sistematicamente, essa promessa integra a expectativa de segurança. O Tema 987 não impede responsabilidade contratual ou consumerista por descumprimento de compromisso próprio.

A controvérsia constitucional pode ser lida à luz do constitucionalismo digital. Maciel (2024b) sustenta que o exame do art. 19 deve articular responsabilidade de intermediários com liberdade de expressão, privacidade e demais garantias constitucionais, evitando soluções que tratem um desses valores como absoluto. Essa perspectiva reforça a necessidade de distinguir conteúdo cuja ilicitude depende de juízo contextual, falha própria da plataforma e risco sistêmico. O Tema 987, portanto, não autoriza abandono das garantias do Marco Civil, mas exige que elas sejam compatibilizadas com deveres de proteção adequados à arquitetura contemporânea dos serviços (MACIEL, 2024b).

4.3 Tema 533 da repercussão geral

O Tema 533 da repercussão geral, relacionado ao RE 1.057.258, tinha como objeto originário o dever de empresa hospedeira fiscalizar e retirar conteúdo ofensivo independentemente de intervenção judicial. O recurso foi julgado em conjunto com o Tema 987, razão pela qual sua análise deve partir da tese integrada construída pelo Supremo, e não de um regime autônomo restrito a publicidade ou automação. Dentro desse regime conjunto, anúncios pagos, impulsionamentos e redes artificiais receberam tratamento específico por envolverem participação econômica ou técnica mais intensa do provedor (BRASIL, 2025b; BRASIL, 2025c).

A tese conjunta estabelece presunção relativa de responsabilidade quando conteúdos ilícitos são veiculados mediante anúncios ou impulsionamentos pagos, bem como quando sua difusão ocorre por redes artificiais. A justificativa é funcional: nessas hipóteses, o provedor não se limita a armazenar manifestação espontânea de

terceiro, mas oferece infraestrutura de amplificação, segmentação ou monetização que pode integrar a cadeia de produção do risco (BRASIL, 2025b; BRASIL, 2025c).

A presunção não equivale a condenação automática. O provedor pode afastar a imputação se demonstrar atuação diligente e tempestiva para tornar o conteúdo indisponível. Esse desenho desloca o debate probatório: diante de publicidade paga ou disseminação inorgânica, cabe à empresa apresentar registros de contratação, critérios de aprovação, sinais de risco, medidas de detecção e tempo de resposta. A responsabilidade continua vinculada à possibilidade de controle e à qualidade da diligência (BRASIL, 2025c; BRASIL, 2026c).

Em matéria infantojuvenil, a publicidade paga assume contornos próprios. Uma campanha que explore aparência infantil, prometa vantagens inadequadas ou conduza menores a práticas perigosas não pode ser analisada como simples fala de usuário. A plataforma participa da segmentação, da entrega e da remuneração do anúncio. A Resolução CONANDA nº 163/2014 e o CDC reforçam o dever de impedir exploração da inexperiência, enquanto o ECA Digital intensifica a atenção a serviços provavelmente acessados por crianças (BRASIL, 2014b; BRASIL, 1990b).

É necessário distinguir publicidade orgânica, conteúdo patrocinado e impulsionamento pago. A publicação espontânea de usuário pode permanecer no regime de conteúdo de terceiro. O conteúdo patrocinado envolve relação comercial e critérios de distribuição definidos pela plataforma. O impulsionamento acrescenta decisão de ampliar alcance a públicos selecionados. Essas diferenças afetam previsibilidade, controle e nexo causal, devendo constar da fundamentação judicial.

As redes artificiais de distribuição também exigem análise específica. Robôs, contas coordenadas e mecanismos automatizados podem produzir falsa popularidade, acelerar ataques ou direcionar materiais nocivos a grupos vulneráveis. Quando a plataforma identifica padrões inorgânicos e dispõe de instrumentos razoáveis de contenção, a omissão pode representar falha própria. A tese conjunta dos Temas 987 e 533 reconhece que a disseminação artificial não é equivalente à circulação espontânea entre usuários (BRASIL, 2025b; BRASIL, 2025c).

Considere-se a hipótese de anúncio pago que oferece desafio perigoso a adolescentes e utiliza segmentação por faixa etária. Se a plataforma aprova a campanha, recebe remuneração e a distribui a perfis de menores, sua participação é direta. Para afastar responsabilidade, não basta alegar autoria de terceiro; é necessário demonstrar controles prévios compatíveis, reação imediata após

identificação e medidas para impedir republicação. O regime evidencia a ligação entre modelo de negócio e dever de segurança.

Em outro cenário, contas automatizadas difundem montagem ofensiva contra adolescente. A plataforma recebe denúncias específicas, detecta comportamento coordenado e demora a desativar a rede. A causalidade não se limita ao primeiro autor da montagem: a amplificação automatizada e a inércia podem aumentar extensão e duração do dano. A responsabilidade deve ser graduada conforme a contribuição de cada agente, evitando tanto concentração indevida quanto fragmentação que inviabilize reparação.

O Tema 533 também valoriza a diligência como categoria verificável. Diligência não é declaração genérica em termos de uso. Envolve políticas de aprovação de anúncios, rastreabilidade do contratante, mecanismos de detecção, canais acessíveis de denúncia, preservação de registros e resposta em tempo compatível com o risco. Em casos envolvendo menores, o tempo é elemento material: poucas horas de circulação podem produzir reprodução massiva e efeitos duradouros.

A possibilidade de exclusão da responsabilidade pela prova de atuação diligente não converte o regime em responsabilidade subjetiva com culpa presumida. O que se afere não é a reprovabilidade da conduta empresarial nem estado psicológico interno da pessoa jurídica, mas a conformidade objetiva do serviço com padrões verificáveis de prevenção e resposta, isto é, a existência ou a inexistência de defeito na acepção do art. 14, § 3º, inciso I, do Código de Defesa do Consumidor. Demonstrar que o serviço ofereceu a segurança legitimamente esperada equivale a negar o defeito, e não a provar ausência de culpa. Ao mesmo tempo, a excludente impede que a presunção se transforme em responsabilidade integral, pois permite demonstrar que o dano decorreu de evento inevitável ou de conduta externa não controlável apesar das medidas adequadas.

A articulação com o art. 21 do Marco Civil também é relevante. Conteúdos que violem intimidade sexual possuem regime especial de indisponibilização após notificação. Quando a vítima é criança ou adolescente, o ECA, a legislação penal e o ECA Digital reforçam a necessidade de resposta rápida e preservação de prova. O Tema 533 não elimina essas normas específicas; integra-as em um sistema no qual gravidade, ciência e controle definem o dever de agir.

A tese fixada pelo Supremo deve ser aplicada com atenção à liberdade de expressão. Nem todo conteúdo impulsionado é ilícito, e a plataforma não pode ser

obrigada a censurar previamente opiniões legítimas apenas porque foram patrocinadas. A presunção depende da existência de conteúdo ilícito e da relação com mecanismos pagos ou artificiais. A análise deve individualizar a ilicitude, o dano e a atuação do provedor, preservando contraditório e fundamentação.

O julgamento conjunto também reconhece deveres de transparência. A vítima precisa saber se o conteúdo foi impulsionado, quem contratou a publicidade e quais critérios de distribuição foram utilizados, respeitados sigilo e proteção de dados. Sem essas informações, torna-se difícil demonstrar alcance e contribuição causal. A ordem judicial pode determinar exibição de registros, e a resistência injustificada deve ser considerada na distribuição do ônus probatório (BRASIL, 2015a).

A referência a anúncios pagos e redes artificiais não corresponde ao objeto exclusivo do Tema 533. Ela resulta da tese comum firmada no julgamento conjunto dos Recursos Extraordinários. Essa precisão é importante porque o Tema 533 conserva sua origem na discussão sobre fiscalização e retirada de conteúdo ofensivo, enquanto o regime final articula essa controvérsia com a revisão constitucional do art. 19 examinada no Tema 987 (BRASIL, 2025b; BRASIL, 2025c; BRASIL, 2026c).

A leitura conjunta permite organizar o sistema em dois eixos complementares. O primeiro redefine quando a ordem judicial específica permanece necessária e quando a ciência extrajudicial, a ilicitude manifesta ou o ato próprio da plataforma podem gerar dever de agir. O segundo atribui maior rigor às situações em que a empresa participa economicamente ou tecnicamente da amplificação. Em ambos, a imputação depende da identificação da ilicitude, do controle disponível, da diligência demonstrada e da contribuição causal do serviço.

Para os tribunais, a aplicação do Tema 533 pode ser organizada em cinco perguntas: o conteúdo é ilícito? Houve pagamento, impulsionamento ou disseminação artificial? A plataforma possuía controle técnico sobre a distribuição? Adotou medidas diligentes em tempo razoável? Qual foi a contribuição dessa atuação para o dano? Essa sequência evita decisões baseadas apenas na gravidade abstrata e permite controlar a imputação.

O regime conjunto, portanto, fornece fundamento relevante para responsabilizar plataformas quando sua infraestrutura comercial ou automatizada amplia ilícitos contra crianças e adolescentes. A presunção ligada a anúncios, impulsionamentos e redes artificiais permanece relativa e pode ser afastada pela demonstração de controles prévios, resposta tempestiva e ausência de contribuição

causal relevante. O resultado não cria seguro universal contra danos *online*; ele impede que remuneração e amplificação sejam tratadas como juridicamente neutras.

A identificação do anunciante constitui elemento importante na publicidade paga. Plataformas devem adotar mecanismos razoáveis de autenticação e conservar dados suficientes para responsabilização, respeitando a LGPD. A ausência deliberada de rastreabilidade favorece abuso e pode demonstrar falha de governança. O dever não exige tornar dados públicos, mas possibilitar acesso por autoridade ou ordem judicial.

A presunção ligada a impulsionamento deve ser limitada ao conteúdo ilícito efetivamente promovido. Não se deve imputar à plataforma toda conduta posterior de usuários apenas porque houve anúncio inicial. O nexo precisa considerar alcance contratado, público atingido e continuidade da amplificação. Essa delimitação evita extensão ilimitada e permite quantificar contribuição.

Mecanismos artificiais de disseminação podem ser internos ou externos. Contas automatizadas podem operar por ferramentas fornecidas pela própria plataforma ou por agentes que burlam controles. A responsabilidade será mais intensa quando a empresa oferece ou monetiza a automação; será reduzida se comprovar detecção e reação adequadas diante de fraude externa sofisticada. A distinção é essencial para aplicar corretamente a excludente de diligência.

Para crianças e adolescentes, o dever de diligência em anúncios deve incluir categorias proibidas, linguagem etária, destino do *link* e práticas de coleta de dados. Auditorias periódicas podem verificar se filtros funcionam e se anunciantes contornam regras. A repetição de violações semelhantes revela que remoções isoladas são insuficientes e pode justificar obrigação estrutural de revisão do sistema.

4.4 Limites do afastamento da responsabilidade objetiva no regime geral

O afastamento da responsabilidade objetiva no regime geral de provedores não pode ser lido como proibição absoluta de imputação objetiva em qualquer hipótese digital. O regime geral busca evitar que a plataforma responda automaticamente por todo conteúdo de terceiro. Essa finalidade permanece legítima, mas não elimina situações em que a própria organização do serviço cria ou amplia risco juridicamente relevante (BRASIL, 2014a; TEFFÉ, 2015).

A diferença está no fundamento da pretensão. Quando se discute apenas conteúdo produzido por terceiro e ausência de remoção, o Marco Civil oferece filtro

específico. Quando se discute falha de *design*, publicidade dirigida a menor, ausência de privacidade por padrão, recomendação perigosa ou descumprimento de dever proativo, o fundamento passa a ser a conduta própria da plataforma. A imputação objetiva, se admitida, incide sobre essa conduta, não sobre autoria alheia.

Esse limite impede confusão entre especialidade protetiva e responsabilidade integral. O ECA Digital não transforma plataformas em seguradoras universais, nem autoriza ignorar liberdade de expressão, devido processo e causalidade. Ele apenas reforça a análise de deveres quando o serviço é direcionado a menores ou provavelmente acessado por eles. O regime especial deve dialogar com o geral, e não suprimi-lo (BRASIL, 2025a).

A imputação objetiva aqui proposta também depende da teoria do risco. O risco relevante deve estar ligado à atividade organizada pela plataforma: recomendação, coleta de dados, publicidade, moderação, resposta a denúncia ou desenho de interface. Se o dano decorre de evento externo, imprevisível e sem relação com o serviço, a imputação deve ser afastada. Se decorre de risco conhecido e administrável, a responsabilidade objetiva ganha fundamento (CAVALIERI FILHO, 2024).

Portanto, os limites do regime geral continuam importantes. Eles impedem responsabilização automática, preservam garantias e exigem definição do dever. A proposta da dissertação se constrói justamente dentro desses limites: não nega o Marco Civil, mas sustenta que a especialidade infantojuvenil pode justificar imputação objetiva quando houver falha própria da plataforma.

Também não se pode ignorar o risco inverso. Se toda omissão for tratada como falha própria da plataforma, o regime do art. 19 perderá função prática. O limite está em exigir demonstração da diferença entre hospedagem de conteúdo e organização do risco. A responsabilidade objetiva por violação de deveres proativos depende dessa fronteira: só haverá imputação especial quando a conduta institucional da plataforma tiver relevância causal e normativa para o dano sofrido pelo menor.

O regime geral de provedores não pode ser interpretado como imunidade ampla. A finalidade do Marco Civil não foi impedir qualquer responsabilização de plataformas, mas organizar a imputação em matéria de conteúdo de terceiro. Quando a pretensão indenizatória se volta contra conduta própria do serviço, como coleta indevida de dados, falha de segurança, recomendação nociva ou ausência de canal

adequado de denúncia, a análise deve dialogar com Código Civil, CDC, LGPD e ECA Digital (BRASIL, 2014a; FRAZÃO, 2022).

Assim, os limites do regime geral não podem ser confundidos com vazio regulatório. A plataforma possui zona de proteção contra imputações indevidas por conteúdo alheio, mas não imunidade para falhas próprias. A responsabilidade civil objetiva por falha própria do serviço ocupa precisamente esse espaço intermediário.

O ECA Digital reforça essa leitura ao criar ou densificar deveres especiais. Esses deveres não são incompatíveis com o Marco Civil; incidem sobre outra camada do problema. Enquanto o regime geral protege contra responsabilização automática por fala de terceiro, o regime especial orienta a organização do serviço quando menores são usuários previsíveis. A compatibilização está no recorte da conduta imputada.

O afastamento total da responsabilidade objetiva poderia produzir efeito indesejado: transferir integralmente às famílias o ônus de riscos tecnicamente administráveis pela plataforma. Em ambiente opaco, a vítima teria de provar mecanismos internos aos quais não possui acesso. Por isso, a interpretação equilibrada admite deveres de explicação, distribuição dinâmica da prova e presunções relativas quando a informação decisiva estiver sob controle do fornecedor (BRASIL, 2015a; MULHOLLAND, 2009).

Também é necessário diferenciar responsabilidade objetiva e responsabilidade sem nexo. Mesmo quando se admite incidência objetiva, continuam indispensáveis dano e relação causal. A plataforma não responde por todo acontecimento indesejado, mas pelo risco que criou, ampliou ou deixou de controlar dentro de sua esfera de atuação. Essa exigência preserva segurança jurídica e evita que a proteção infantojuvenil seja convertida em garantia universal (SCHREIBER, 2015; CAVALIERI FILHO, 2024).

O limite do afastamento está na causa de pedir. Se a pretensão se baseia apenas em conteúdo produzido por usuário, o art. 19 tem incidência direta. Se a demanda descreve falha de arquitetura, recomendação, publicidade dirigida, tratamento de dados ou omissão diante de risco conhecido a menores, o debate supera a simples não remoção. A responsabilidade objetiva pode ser discutida sem negar a função do Marco Civil (FRAZÃO, 2022; BRASIL, 2025a).

O regime geral da internet não deve ser lido como afastamento universal da responsabilidade objetiva. O Marco Civil buscou impedir responsabilização

automática por conteúdo de terceiro, mas não eliminou todos os deveres civis dos provedores. Plataformas continuam sujeitas a deveres de segurança, informação, proteção de dados, boa-fé e resposta adequada quando a causa do dano envolve conduta própria do serviço (BRASIL, 2014a; BRASIL, 1990b; BRASIL, 2018).

A construção aqui defendida, portanto, não propõe afastar o Marco Civil. Propõe delimitar seu alcance. O art. 19 continua sendo regra central para responsabilização por conteúdo de terceiro; o ECA Digital incide sobre deveres especiais de proteção infantojuvenil. A coordenação entre ambos é mais consistente do que a tentativa de escolher um diploma contra o outro.

A preservação do regime geral não impede medidas preventivas. O juiz pode reconhecer que a plataforma não responde por conteúdo específico antes de ordem judicial e, ao mesmo tempo, exigir melhoria de canal de denúncia ou documentação de risco em casos envolvendo menores. Essa distinção evita que a discussão fique presa à falsa alternativa entre imunidade absoluta e responsabilidade integral.

Os limites do regime geral também devem considerar a evolução tecnológica. Plataformas atuais não se limitam a armazenar conteúdo. Elas classificam, personalizam, recomendam, monetizam e avaliam risco. O direito não pode aplicar categorias de intermediação passiva a sistemas que organizam ativamente a experiência do usuário. Essa atualização interpretativa é necessária para manter coerência do sistema.

A fronteira entre regime geral e especial deve ser traçada pela conduta. Quando o dano resulta de fala de terceiro e a plataforma não contribuiu para sua amplificação, o art. 19 possui força. Quando o dano resulta de arquitetura insegura, falha de denúncia, tratamento de dados ou recomendação dirigida a menores, a plataforma participa por conduta própria. A imputação objetiva incide nessa segunda zona.

O afastamento da responsabilidade objetiva em certas hipóteses busca proteger a função de intermediação. Se toda plataforma respondesse automaticamente por todo conteúdo de usuário, haveria incentivo à remoção excessiva e ao controle privado amplo. Esse risco justifica cautela. Porém, a cautela não deve ser confundida com ausência total de deveres. O regime geral limita uma forma de imputação, não todas.

O regime geral também não impede responsabilidade por promessa de segurança não cumprida. Quando a plataforma afirma oferecer controle parental, moderação efetiva ou privacidade reforçada, essa comunicação cria expectativa. Se

o mecanismo é inexistente, inacessível ou meramente simbólico, pode haver falha informacional e defeito de serviço, independentemente de ordem judicial para remover conteúdo.

Outro limite do afastamento está na segurança do serviço. Se a plataforma falha em canal de denúncia, preservação de evidência ou resposta a risco grave, a discussão envolve qualidade do serviço prestado. O art. 19 não foi criado para isentar falhas de segurança próprias. A análise deve perguntar se a conduta discutida depende de juízo sobre conteúdo ou de avaliação de dever organizacional.

O afastamento da responsabilidade objetiva no regime geral não pode ser interpretado como imunidade ampla da atividade digital. A exclusão de uma hipótese de imputação por conteúdo de terceiro não impede a incidência do CDC, da LGPD ou do Código Civil quando o dano decorre de defeito próprio do serviço. A pergunta correta é qual risco se materializou. Se a plataforma não produziu nem ampliou o evento e cumpriu deveres aplicáveis, a responsabilização tende a ser indevida; se a arquitetura ou a omissão institucional contribuiu para o dano, outros fundamentos podem incidir (BRASIL, 1990b; BRASIL, 2002; BRASIL, 2018).

Também é necessário distinguir dever de monitoramento geral e dever de gestão de riscos conhecidos. Exigir leitura prévia de todas as comunicações seria incompatível com privacidade, escala e liberdade de expressão. Diferente é demandar que a empresa avalie funcionalidades próprias, responda a sinais consistentes, mantenha canais eficazes e reduza riscos associados a mecanismos que ela controla. A responsabilidade objetiva por violação de deveres proativos não pressupõe vigilância universal; ela se concentra na capacidade concreta de prevenção e na falha relacionada ao serviço oferecido (FRAZÃO, 2021; BALKIN, 2018).

Os limites devem proteger também pequenos provedores e serviços inovadores. Medidas proporcionais à escala, ao público e à capacidade técnica evitam que obrigações concebidas para grandes plataformas sejam aplicadas mecanicamente a agentes com estrutura diversa. Proporcionalidade, entretanto, não significa dispensa de proteção básica. Mesmo serviços menores devem oferecer informação honesta, segurança compatível e resposta a riscos graves quando alcançam crianças e adolescentes. A calibragem reduz barreiras indevidas sem criar zonas livres de responsabilidade (EUROPEAN COMMISSION, 2025; BRASIL, 2025a).

A leitura restritiva do regime geral deve ser evitada quando inviabiliza a proteção de dados. O art. 19 disciplina conteúdo de terceiro; ele não deve impedir responsabilização por coleta indevida, perfilamento abusivo ou publicidade incompatível com a idade. Essas condutas pertencem a outra camada normativa e precisam ser examinadas com base na LGPD, no CDC e no ECA Digital.

A especialidade protetiva também deve ser compatibilizada com inclusão e desenvolvimento digital. Melo (2022) adverte que a regulação da internet precisa enfrentar desigualdades persistentes de acesso e novas pressões regulatórias sem converter proteção em exclusão. Para crianças e adolescentes, isso significa que medidas de segurança devem ser proporcionais, acessíveis e transparentes, preservando oportunidades de participação digital ao mesmo tempo em que reduzem riscos previsíveis.

A controvérsia constitucional sobre o art. 19 igualmente exige atenção à liberdade de expressão e à proteção efetiva de direitos fundamentais. Maciel (2024b) sustenta que a avaliação da constitucionalidade da regra deve considerar o ambiente de governança privada das plataformas e a insuficiência de uma leitura que trate a intermediação digital como atividade puramente neutra. Essa contribuição dialoga com a solução adotada pelo STF ao substituir o modelo rígido por critérios graduados de ciência, diligência, gravidade e participação funcional.

O regime geral preserva função quando a plataforma não participa da criação, seleção ou amplificação. A mera possibilidade técnica de remover conteúdo não implica dever universal de monitorar. A distinção deve considerar desenho do serviço e informação disponível. Plataformas de mensageria privada, fóruns públicos e redes de recomendação possuem graus diferentes de interferência e não podem ser submetidas a regra única.

A notificação extrajudicial deve ser avaliada pela suficiência. Deve identificar URL, perfil, data e natureza do ilícito quando possível. Em situações de risco evidente a menor, exigências excessivamente formais podem frustrar proteção. A plataforma pode pedir complementação, mas não ignorar sinal claro. A diligência inclui orientar o denunciante sobre informação necessária.

O tempo razoável varia. Conteúdo sexual envolvendo menor ou ameaça concreta exige resposta imediata; disputa reputacional complexa pode demandar análise. Prazos internos rígidos não substituem avaliação de risco. A empresa deve

possuir escalas de prioridade e registrar justificativa para demora. O Judiciário, ao analisar, deve considerar volume, clareza, gravidade e recursos disponíveis.

A decisão do STF não extingue a ordem judicial específica. Ela permanece relevante para conteúdos cuja ilicitude depende de contexto, como crítica, sátira ou relato de interesse público. A flexibilização deve ser reservada a categorias definidas e a atos próprios. Essa cautela impede que proteção infantil seja usada para suprimir manifestações legítimas sobre políticas públicas ou instituições.

A responsabilidade por ato próprio inclui decisões comerciais e técnicas. A plataforma que vende anúncio, cria ferramenta de impulsionamento ou recomenda conteúdo não pode equiparar essas escolhas à mera hospedagem. O Marco Civil deve ser interpretado de modo funcional, preservando sua proteção quando o serviço é intermediário e afastando-a quando atua como agente da distribuição.

4.5 ECA Digital como *lex specialis* de proteção infantojuvenil

O ECA Digital pode ser compreendido como *lex specialis* quando o serviço digital envolve crianças e adolescentes de modo direto ou provável. Sua especialidade não decorre apenas do tema tecnológico, mas do sujeito protegido. A criança e o adolescente ocupam posição constitucional reforçada, e essa condição justifica densificação de deveres de prevenção, segurança, transparência e resposta no ambiente digital (BRASIL, 1988; BRASIL, 2025a; LOPES; NOVAIS, 2026).

A *lex specialis* não elimina as normas gerais. Ela orienta sua aplicação em situações específicas. Assim, o Código Civil continua estruturando responsabilidade; o CDC continua relevante para segurança e informação; a LGPD regula dados pessoais; o Marco Civil preserva garantias digitais; e o ECA Digital acrescenta deveres voltados à proteção infantojuvenil. O resultado é coordenação normativa, não substituição integral (MARQUES, 2012).

A especialidade do ECA Digital é particularmente importante quando o dano não deriva apenas de conteúdo de terceiro, mas de arquitetura, recomendação, publicidade, coleta de dados ou resposta institucional. Nesses casos, o art. 19 do Marco Civil não deve ser usado como resposta única, porque a conduta discutida pode ser própria da plataforma e anterior ou paralela à remoção de conteúdo.

A leitura como *lex specialis* também exige limites. A especialidade não autoriza responsabilidade sem nexo, nem dispensa identificação do dever violado. A plataforma deve responder quando sua organização do serviço contribui de modo

juridicamente relevante para o dano, e não simplesmente porque a vítima é menor. A força da proteção especial depende justamente da precisão dos critérios de imputação.

O ECA Digital, portanto, funciona como núcleo normativo de intensificação do cuidado. Ele transforma a prioridade constitucional em obrigações mais próximas da operação digital, permitindo avaliar se a plataforma adotou medidas compatíveis com a presença provável de menores. Essa função especial sustenta a proposta de imputação objetiva aqui defendida.

Com isso, a dissertação propõe leitura sistemática: Marco Civil como regime geral de garantias e conteúdo de terceiro; ECA Digital como regime especial de proteção infantojuvenil; Código Civil e CDC como bases de responsabilidade e segurança; LGPD como parâmetro de dados. Essa combinação permite proteger menores sem romper a coerência do sistema.

Tal leitura também confere utilidade ao microssistema. Se o ECA Digital fosse tratado apenas como repetição simbólica da proteção integral, pouco acrescentaria à responsabilidade civil. Sua função é transformar prioridade absoluta em deveres operacionais para serviços digitais: avaliação de risco, desenho seguro, resposta a incidentes, proteção de dados e transparência. A responsabilidade objetiva surge justamente quando esses deveres são descumpridos e o descumprimento se relaciona com dano concreto.

A qualificação do ECA Digital como lei especial não significa revogação do Marco Civil. A especialidade opera quando a situação envolve crianças e adolescentes em serviços digitais e quando o dano se conecta a deveres de proteção previstos ou densificados pela nova lei. Nesses casos, a interpretação deve partir da finalidade protetiva sem abandonar garantias de devido processo, liberdade de expressão e segurança jurídica. A lei especial especifica o dever; não elimina a necessidade de nexo (BRASIL, 2025a; MARQUES, 2012).

A conclusão alcançada é que o ECA Digital funciona como norma especial de orientação e densificação. Ele permite reconhecer deveres próprios em ambientes digitais frequentados por menores, mas deve ser aplicado em conjunto com os regimes gerais. Essa leitura evita conflito artificial e permite que a proteção infantojuvenil opere com segurança dogmática.

Cabe indagar se o ECA Digital, que opera por orientação e densificação, não estaria limitado a explicitar deveres que o sistema jurídico já continha, sem nada

acrescentar à responsabilidade civil. No plano do regime de imputação, a inovação é de fato reduzida. A responsabilidade objetiva por defeito do serviço já decorria do art. 14 do Código de Defesa do Consumidor; a vinculação de agentes econômicos privados à proteção integral já decorria do art. 227 da Constituição; e os deveres de proteção, informação e cooperação já podiam ser extraídos da boa-fé objetiva. Se a Lei nº 15.211/2025 fosse revogada, a construção defendida nesta dissertação não sucumbiria: voltaria apenas a depender da concreção judicial de cláusulas gerais, o que não fragiliza o argumento, mas demonstra que ele se apoia na estrutura do direito civil brasileiro, e não na contingência de um diploma recente (BRASIL, 1988; BRASIL, 1990b; MARTINS-COSTA, 2018).

Essa constatação, todavia, não conduz à conclusão de que a densificação seja juridicamente irrelevante. No regime da responsabilidade por defeito, densificar o dever é densificar o próprio suporte fático da imputação. O art. 14, § 1º, do Código de Defesa do Consumidor afere o defeito pela segurança que legitimamente se pode esperar do serviço. Quando a lei especial declara o que se deve esperar – avaliação prévia de risco, proteção desde a concepção, privacidade por padrão, canais acessíveis de denúncia e resposta documentada a incidentes –, ela deixa de ser exterior à responsabilidade civil e passa a preencher o conceito de defeito. A densificação, portanto, não altera a espécie de responsabilidade, mas incide sobre os seus pressupostos, que é precisamente onde esta pesquisa situa sua contribuição (BRASIL, 1990b; BRASIL, 2025a; TEPEDINO; TERRA; GUEDES, 2024).

Dessa incidência decorrem consequências verificáveis. A primeira é argumentativa: o dever deixa de ser construído caso a caso a partir de cláusula geral e passa a ser pressuposto legal, deslocando a discussão para a conformidade da conduta empresarial. A segunda diz respeito às excludentes: risco tipificado em lei é risco normativamente previsível, o que estreita a alegação de caso fortuito e de impossibilidade fática de prevenção. A terceira é probatória: a exigência de avaliações de risco, registros de resposta e documentação de governança produz material que antes simplesmente não existia, tornando praticável a distribuição dinâmica do ônus da prova examinada adiante. A quarta escapa à própria noção de densificação: o critério do serviço provavelmente acessado por crianças e adolescentes é norma de incidência sem correspondente anterior no ordenamento brasileiro, pois delimita o âmbito subjetivo dos deveres em vez de apenas detalhar seu conteúdo.

A resposta à objeção se completa quando se observa o movimento histórico em que a lei especial se insere. A passagem do Estado Liberal para o Estado Social deslocou o eixo do direito privado: a autonomia da vontade, antes concebida como espaço reservado à não intervenção, passou a conviver com normas cogentes destinadas a corrigir desequilíbrios estruturais entre as partes. Nesse paradigma, a intensidade da ingerência estatal nas relações privadas é proporcional a duas variáveis. A primeira é a importância do bem jurídico tutelado; a segunda, o grau de vulnerabilidade e de assimetria entre os sujeitos da relação. Quanto mais elevado o bem e mais acentuado o desnível, maior a legitimidade e a densidade da regulação. Foi essa lógica que produziu, no direito brasileiro, o Código de Defesa do Consumidor, o Estatuto da Criança e do Adolescente, o Estatuto da Pessoa Idosa e a Lei Brasileira de Inclusão da Pessoa com Deficiência, todos construídos sobre a premissa de que a igualdade formal é insuficiente diante de posições materialmente desiguais (BRASIL, 1990a; BRASIL, 1990b; BRASIL, 2003; BRASIL, 2015b; MORAES, 2003; MARQUES, 2012).

O ECA Digital é aplicação dessa mesma lógica ao ambiente digital. O bem jurídico tutelado é o desenvolvimento de pessoas em formação, ao qual o art. 227 da Constituição atribuiu prioridade absoluta. A assimetria, por sua vez, não é apenas econômica: soma-se a ela a desigualdade informacional e técnica decorrente da opacidade dos sistemas de recomendação, da coleta continuada de dados e do desenho de interfaces orientado à retenção da atenção. Diante desse quadro, a edição de estatuto próprio não constitui redundância, mas consequência coerente do paradigma. A intervenção legislativa se mostra necessária, porque a proteção não pode depender exclusivamente da concreção judicial de cláusulas gerais; compatível com o sistema, porque prolonga orientação protetiva já consolidada no direito privado brasileiro; e oportuna, porque enfrenta riscos que se tornaram estruturais antes de qualquer resposta normativa específica (BRASIL, 1988; MACHADO, 2003; MIRAGEM, 2019).

Reconhecer essa filiação reforça o argumento desenvolvido acima. Se a densificação incide sobre os pressupostos da imputação, é porque o legislador, ao declarar o que se espera do serviço, exerce função que o modelo do Estado Social lhe reserva: fixar por norma o padrão de conduta que a assimetria entre as partes impede de ser efetivamente negociado. A densificação, nesse sentido, não é gesto redundante do legislador, mas o modo próprio pelo qual a proteção se realiza em

relações estruturalmente desiguais (MARTINS-COSTA, 2018; TEPEDINO; TERRA; GUEDES, 2024).

O risco de uso retórico da especialidade, por outro lado, deve ser controlado. Invocar o ECA Digital sem indicar o dever violado, a funcionalidade envolvida, a medida esperada e o nexo causal seria insuficiente. A especialidade não substitui fundamentação; ela fornece critérios para fundamentar. Por isso, a dissertação propõe responsabilidade objetiva condicionada à violação de deveres, e não responsabilidade ilimitada (TEPEDINO; TERRA; GUEDES, 2024).

A especialidade também afeta o padrão probatório. Se a plataforma opera serviço provavelmente acessado por menores, deve demonstrar que avaliou riscos, adotou medidas proporcionais e respondeu adequadamente a incidentes. Essa exigência não decorre de presunção automática de culpa, mas da posição de controle sobre ambiente, dados e documentação. A *lex specialis* torna mais denso o dever de explicar a governança do serviço.

O diálogo das fontes é indispensável para evitar sobreposição desordenada. O ECA Digital pode definir deveres especiais; a LGPD disciplina tratamento de dados; o Marco Civil regula responsabilidade por conteúdo de terceiro e garantias de internet; o CDC reforça segurança e informação; o Código Civil fornece categorias de imputação. A *lex specialis* não absorve tudo, mas coordena a interpretação quando a infância está no centro do conflito (BRASIL, 2018; BRASIL, 1990b; BRASIL, 2002).

A especialidade se justifica pela condição da vítima e pela natureza do ambiente. Crianças e adolescentes não são usuários comuns em situação digital comum. São pessoas em desenvolvimento expostas a serviços que coletam dados, recomendam conteúdo, organizam interações e monetizam atenção. A lei especial surge para traduzir a prioridade constitucional em deveres operacionais, aproximando proteção integral e governança tecnológica (BRASIL, 1988; UNITED NATIONS, 2021).

A classificação do ECA Digital como *lex specialis* deve ser compreendida com cuidado. A especialidade não significa revogação automática das normas gerais. Significa que, em conflitos envolvendo crianças e adolescentes no ambiente digital, a interpretação de Código Civil, CDC, LGPD e Marco Civil deve considerar deveres específicos de proteção infantojuvenil. A lei especial orienta o recorte do risco, o padrão de cuidado e a resposta esperada da plataforma (BRASIL, 2025a; MARQUES, 2012).

A *lex specialis* também organiza a relação entre proteção individual e coletiva. A mesma regra que protege uma vítima pode justificar medidas preventivas para grupos de menores. Quando a falha é sistêmica, a resposta individual não corrige o risco. O ECA Digital permite enxergar a plataforma como ambiente de proteção e não apenas como espaço de conflito entre duas partes.

A especialidade do ECA Digital deve alcançar também a interpretação dos deveres empresariais. O fornecedor que atua em ambiente provavelmente acessado por menores precisa incorporar essa realidade em sua governança. Não basta adaptar a resposta após judicialização; a especialidade impõe planejamento. Isso inclui mapear riscos, definir fluxos de atendimento e ajustar funcionalidades que possam impactar crianças e adolescentes.

O debate do STF reforça que a matéria exige precisão. Decisões sobre responsabilidade de plataformas possuem efeitos sistêmicos sobre remoção, moderação, inovação e participação digital. Por isso, a dissertação não propõe critério único para todos os conflitos. Propõe uma técnica decisória que separa conteúdo de terceiro, dever proativo, proteção de dados e risco arquitetônico.

A especialidade do ECA Digital deve ser aplicada sem ruptura. Ela acrescenta densidade à proteção de menores, mas deve respeitar devido processo, liberdade comunicativa e causalidade. A plataforma pode ser chamada a responder quando sua organização do serviço contribui para o dano, não quando apenas serve de local remoto para comportamento totalmente externo. A distinção entre intermediação e governança é, portanto, o eixo do capítulo.

A qualificação do ECA Digital como lei especial deve ser feita por matéria e finalidade. Sua especialidade decorre do foco em crianças e adolescentes e da disciplina de deveres próprios do ambiente digital. Isso não significa revogação global do Marco Civil, do CDC ou da LGPD. A norma especial prevalece quando regula de maneira específica o mesmo ponto ou quando acrescenta proteção compatível ao regime geral. Nos demais aspectos, permanece necessária a coordenação das fontes, preservando garantias e conceitos que não foram afastados (MARQUES, 2012; BRASIL, 2025a).

Um teste de especialidade pode seguir três perguntas: o serviço é abrangido pela lei? O dever discutido foi especificamente previsto ou densificado para proteção de menores? A aplicação do regime geral reduziria a eficácia dessa proteção? Se as respostas forem afirmativas, o ECA Digital deve orientar a solução. Se a controvérsia

envolver apenas remoção de conteúdo sem relação com dever especial, o Marco Civil continuará desempenhando função predominante. Esse método evita tanto a absorção completa de um diploma pelo outro quanto a fragmentação incoerente do sistema (FUNDAÇÃO GETULIO VARGAS, 2025; FRAZÃO, 2022).

A especialidade também repercute na interpretação do nexo e das excludentes. A presença de dever proativo pode tornar juridicamente relevante uma omissão que, no regime comum, seria insuficiente. Por outro lado, a plataforma continua autorizada a demonstrar impossibilidade técnica, fato exclusivo ou adoção de medidas adequadas. A lei especial não cria responsabilidade integral; ela altera o padrão esperado de cuidado diante de público vulnerável. A solução permanece condicionada à relação entre dever descumprido, risco protegido e dano verificado (BRASIL, 2025a; TEPEDINO; TERRA; GUEDES, 2024).

A análise do Marco Civil e da jurisprudência constitucional permite formular uma conclusão intermediária: o regime geral protege a liberdade de expressão e impede responsabilidade automática, mas não cria imunidade para condutas próprias das plataformas. Essa conclusão é decisiva para a presente pesquisa, pois conserva a função do art. 19 e, ao mesmo tempo, abre espaço para deveres especiais em contextos infantojuvenis.

A coordenação entre regime geral e tutela especial também se beneficia da reflexão sobre neutralidade da rede e desenvolvimento. Melo (2018) demonstra que escolhas regulatórias sobre infraestrutura e intermediação não são tecnicamente neutras: elas distribuem poder, custos e oportunidades de acesso. No contexto do ECA Digital, essa constatação recomenda cautela para que deveres de proteção não produzam bloqueios indiscriminados ou barreiras desproporcionais à participação. A especialidade deve incidir sobre riscos e funcionalidades identificáveis, preservando a abertura da rede e a capacidade de inovação compatível com os direitos de crianças e adolescentes (MELO, 2018).

A persistência da exclusão digital introduz outro limite ao desenho regulatório. A proteção de menores não pode pressupor acesso homogêneo, equipamentos equivalentes ou igual capacidade das famílias para acompanhar práticas *online*. Ao examinar pressões emergentes da regulação da internet no Brasil, Melo (2022) destaca a convivência entre expansão tecnológica e desigualdades estruturais. Esse quadro reforça que medidas de segurança devem ser acessíveis, compreensíveis e sensíveis a diferentes condições de conectividade. Uma política protetiva que

simplesmente expulse usuários vulneráveis ou transfira integralmente o controle às famílias pode ampliar a desigualdade que pretende enfrentar (MELO, 2022).

5 CRITÉRIOS DOGMÁTICOS PARA A RESPONSABILIZAÇÃO OBJETIVA DAS PLATAFORMAS

Estabelecido no capítulo anterior qual regime incide sobre o dano digital infantojuvenil, resta examinar como aplicá-lo. A pergunta muda de registro: não se trata mais de saber se o ECA Digital atrai deveres próprios para as plataformas, mas de determinar em que condições o descumprimento desses deveres autoriza a imputação. É nessa passagem que a especialidade encontra seu limite. A lei especial torna mais densos os deveres de proteção, porém não dispensa a demonstração de falha e de nexo causal, nem funciona como cláusula ilimitada de condenação. Em lugar de perguntar genericamente se a plataforma deveria ter protegido o usuário, o julgador precisa verificar qual dever concretamente incidia, se a medida omitida era proporcional ao risco e de que modo a omissão se relaciona com o dano. É essa verificação que o presente capítulo organiza.

O propósito da sistematização é converter a proposta em método de decisão. Em vez de partir da gravidade abstrata do dano ou do porte econômico da empresa, o intérprete reconstrói uma sequência: identifica o serviço; verifica a presença provável de menores; define a funcionalidade relevante e o dever aplicável; localiza a falha; delimita o dano; examina o nexo e aprecia as excludentes. A ordem não é rígida, mas reduz saltos argumentativos e explica por que situações aparentemente semelhantes podem receber soluções diferentes. O capítulo oferece, assim, uma linguagem comum para decisões judiciais, políticas internas e estratégias preventivas (TEPEDINO; TERRA; GUEDES, 2024).

A matriz também separa planos que, com frequência, são tratados como equivalentes. A obrigação de reparar pertence ao direito material; a distribuição do ônus da prova é técnica processual; a tutela inibitória busca evitar ou cessar o ilícito; e a sanção administrativa possui fundamento próprio. Uma mesma prática pode ativar mais de um plano, mas cada consequência exige pressupostos e motivação específicos. A distinção preserva a coerência do trabalho e evita que a responsabilidade civil se transforme em substituto genérico da regulação digital (BRASIL, 2015a; BRASIL, 1985).

A especialidade repercute, por fim, na leitura da prova. Quem oferece serviço de acesso provável por menores deve estar em condições de demonstrar como cumpriu deveres de segurança e resposta. A falta de documentação não prova,

isoladamente, a falha, mas pode adquirir relevância quando os registros decisivos permanecem sob controle exclusivo da empresa e a narrativa da vítima apresenta elementos concretos.

5.1 Pressupostos de incidência no microssistema do ECA Digital

A responsabilização objetiva das plataformas no microssistema do ECA Digital depende de cinco pressupostos cumulativos, enunciados a seguir e desenvolvidos, na sequência, um a um. O primeiro é bifocal e reúne serviço e sujeito: exige a presença de serviço digital direcionado a crianças e adolescentes ou provavelmente acessado por eles e, simultaneamente, a identificação da condição concreta do sujeito protegido, consideradas faixa etária, estágio de desenvolvimento, capacidades em evolução e eventuais vulnerabilidades agravadas. O segundo é a existência de dever proativo concretamente aplicável. O terceiro é o descumprimento ou cumprimento insuficiente desse dever, em situação relacionada ao risco que se concretizou no dano. O quarto é o dano juridicamente relevante. O quinto é o nexo entre a falha e o resultado. Sem essa sequência, a responsabilidade perde controle dogmático (BRASIL, 2025a; TEPEDINO; TERRA; GUEDES, 2024).

O primeiro pressuposto, acesso provável por menores, deve ser demonstrado por indícios objetivos. Métricas de uso, linguagem, conteúdo promovido, funcionalidades, publicidade e histórico de denúncias podem comprovar previsibilidade. A plataforma que explora dados para personalização não pode ignorar completamente o perfil de seus usuários. Esse ponto reforça a coerência entre capacidade econômica e dever de cuidado.

O acesso provável por menores não pode ser presumido de forma abstrata. Ele deve ser inferido a partir de elementos do serviço, como linguagem, *design*, audiência, conteúdo promovido, publicidade, funcionalidades, métricas internas e histórico de uso. Essa análise impede que a plataforma se afaste do regime especial apenas por declaração contratual, mas também evita aplicar deveres reforçados a serviços sem vínculo concreto com público infantojuvenil. Funcionando como porta de entrada do microssistema especial, o pressuposto não se satisfaz com o uso meramente excepcional do serviço por uma criança, nem se afasta quando a plataforma explora público juvenil, oferece funcionalidades atrativas ou dispõe de métricas internas que indicam esse acesso (ICO, 2022; EUROPEAN COMMISSION, 2025; COMITÊ GESTOR DA INTERNET NO BRASIL, 2026).

O primeiro pressuposto, contudo, não se esgota na verificação do acesso provável. Ele possui um segundo foco, dirigido não ao serviço, mas ao sujeito protegido. A criança e o adolescente não integram a análise apenas como condição de incidência do regime especial e como portadores do dano ao final examinado; sua condição concreta constitui critério autônomo de aferição. Isso significa apurar a faixa etária e o estágio de desenvolvimento, reconhecer que as capacidades evoluem progressivamente e que exigências e proteções devem acompanhar essa evolução, verificar vulnerabilidades agravadas demonstráveis no caso – deficiência, situação de acolhimento, exposição prévia, condição de saúde mental – e considerar o melhor interesse como critério de escolha entre as respostas juridicamente possíveis. (UNITED NATIONS, 2021; MACIEL, 2024a).

Esse segundo foco cumpre função dogmática precisa, e não meramente principiológica. Ele repercute sobre a intensidade do dever exigível, pois o que se espera de serviço provavelmente acessado por criança de tenra idade não coincide com o exigível diante de adolescente prestes a atingir a maioridade. Repercute sobre a aferição do defeito, uma vez que a segurança legitimamente esperada é sempre relativa ao público concretamente atingido, e não a um usuário abstrato. Repercute sobre as excludentes, porque não se pode reconhecer culpa exclusiva da vítima quando se exige discernimento que a etapa de desenvolvimento não comporta. E repercute sobre a escolha da tutela, que não pode ter por resultado padrão a exclusão da criança do ambiente digital, solução que converteria proteção em privação do direito de participar, informar-se e conviver. Com essa articulação, a matriz proposta deixa de ser mera avaliação de conformidade da arquitetura do serviço e passa a considerar a criança em sua dimensão humana, sem que a análise da conduta da plataforma seja substituída pela comoção diante da lesão (BRASIL, 1988; MACHADO, 2003; MORAES, 2003).

O segundo pressuposto é a identificação do dever concretamente aplicável. A responsabilidade não pode ser fundada em expressão genérica de proteção: termos como segurança, transparência e melhor interesse são importantes, mas precisam ser traduzidos em condutas verificáveis. É preciso indicar se a falha está em privacidade por padrão, aferição de idade, moderação, canal de denúncia, resposta a incidente, recomendação algorítmica, limitação de publicidade, avaliação de risco ou preservação de registros. Essa especificação torna controlável a imputação, permite que a plataforma saiba que conduta era esperada e é o que diferencia

responsabilização fundamentada de responsabilização retórica (FRAZÃO, 2021; TEPEDINO; TERRA; GUEDES, 2024).

Identificar o dever exige, ainda, indicar sua fonte e calibrar sua intensidade. A fonte pode estar na Lei nº 15.211/2025, na Lei Geral de Proteção de Dados, no Código de Defesa do Consumidor ou na boa-fé objetiva, e essa indicação importa porque define o âmbito de exigibilidade e os efeitos do descumprimento. A intensidade, por sua vez, não é uniforme: varia conforme a condição concreta do sujeito, apurada no primeiro pressuposto, e conforme a capacidade técnica e econômica do fornecedor. Exigir de aplicação de pequeno porte o mesmo padrão de detecção esperado de serviço com alcance global seria tão inadequado quanto dispensar este último de controles que sua própria escala torna viáveis. A proporcionalidade entre risco criado, meios disponíveis e público atingido é o critério que impede tanto a diluição do dever quanto sua conversão em obrigação impossível.

A identificação do serviço precede a identificação do dever. Uma rede social que recomenda vídeos, um jogo com compras internas e um aplicativo de mensagens não controlam as mesmas funcionalidades. O dever de limitar publicidade pode ser central no primeiro caso, enquanto mecanismos de contato, bloqueio ou proteção contra gasto podem assumir maior relevância nos demais. A classificação funcional evita copiar obrigações de um setor para outro e torna a responsabilidade proporcional à atividade efetivamente desenvolvida (SOUZA; LEMOS, 2016; LIVINGSTONE; STOILOVA; HOPWOOD, 2021).

O terceiro pressuposto, descumprimento, deve ser comparativo. Pergunta-se o que a plataforma fez, o que era razoavelmente esperado, quais meios estavam disponíveis e qual era a gravidade do risco. Essa comparação evita análise retrospectiva injusta, na qual toda lesão é vista como prova de falha. O direito deve exigir diligência possível, não perfeição.

O descumprimento deve ser verificável. A plataforma pode demonstrar políticas, relatórios, fluxos de atendimento, registros de resposta e medidas de mitigação. A ausência desses elementos, quando relevantes, pode pesar contra o fornecedor, mas não dispensa a análise do dano. O juiz deve reconstruir o que foi exigido, o que foi feito e o que deixou de ser adotado (BRASIL, 2015a; MULHOLLAND, 2009).

O descumprimento relevante é, ademais, aquele vinculado ao risco que veio a concretizar-se. O descumprimento formal de uma obrigação só terá relevância

indenizatória se estiver conectado ao dano sofrido. Se a falha não aumentou o risco, não impediu resposta possível ou não se relacionou com a lesão, a responsabilidade perde fundamento. A ideia defendida, portanto, não substitui causalidade por vulnerabilidade; ela qualifica a causalidade diante de assimetria informacional e risco organizado.

O quarto pressuposto, dano, exige seletividade. Nem toda experiência negativa em ambiente digital constitui lesão indenizável: frustração, desconforto ou desagrado diante de conteúdo não bastam. É preciso identificar o bem jurídico atingido – imagem, privacidade, dados pessoais, integridade psíquica, reputação, patrimônio ou desenvolvimento biopsicossocial – e demonstrar sua repercussão concreta sobre a esfera do lesado. Em matéria infantojuvenil, a aferição possui particularidade relevante: lesões de pequena monta para um adulto podem produzir efeitos persistentes sobre pessoa em formação, de modo que a condição concreta apurada no primeiro pressuposto repercute diretamente sobre a valoração do dano. A recíproca, contudo, também vale: a gravidade da lesão não supre a ausência de dever violado ou de nexo, sob pena de converter comoção em fundamento de condenação. Quando a pretensão for inibitória, basta a ameaça concreta e suficientemente determinada de ilícito, sem que a dispensa da consumação do dano signifique dispensa da demonstração de risco sério (BRASIL, 1990a; MORAES, 2003; ROSENVALD, 2017).

O quinto pressuposto, nexo, é o mais delicado. Ele deve ligar a falha ao dano sem exigir prova impossível da vítima nem aceitar presunções ilimitadas. A resposta está em presunções relativas, exibição de documentos, inferências e avaliação de plausibilidade. A causalidade precisa ser suficientemente demonstrada para legitimar a imputação.

O nexo causal é o elemento de fechamento. A plataforma só responde quando a falha em dever proativo contribuiu de modo relevante para a criação, ampliação ou manutenção do dano. Esse nexo pode ser demonstrado diretamente ou inferido de forma relativa em razão da opacidade e da posse de informações pelo fornecedor. A inferência, porém, deve ser fundamentada em indícios concretos.

Por fim, a incidência do microssistema exige compatibilização com o Marco Civil da Internet e com a LGPD. O ECA Digital não revoga o regime geral, mas acrescenta uma camada protetiva quando há menores envolvidos. A responsabilidade

objetiva aqui sustentada nasce dessa coordenação: proteção integral, atividade de risco, dever proativo e controle técnico da plataforma.

A organização dos pressupostos tem função prática. Ela permite ao julgador examinar o caso por etapas e impede decisões baseadas apenas em repulsa ao dano. Primeiro se identificam o serviço, seu público provável e a condição concreta do sujeito protegido. Depois se verifica qual dever proativo existia. Em seguida se examina se houve falha, dano e nexo. Essa sequência torna a proteção mais forte porque reduz arbitrariedade.

Os pressupostos também têm função defensiva. Eles protegem plataformas contra imputações genéricas, pois exigem descrição da funcionalidade, do dever e do nexo. Uma plataforma que demonstrar ausência de acesso provável, adoção de medidas adequadas ou fato externo exclusivo poderá afastar a responsabilidade. A qualificação do regime, portanto, aumenta rigor analítico para ambos os lados.

O microssistema não exige que todos os deveres apareçam em todos os casos. Um dano por publicidade comportamental pode envolver informação, consentimento, perfilamento e exploração comercial. Um caso de exposição íntima pode envolver denúncia, preservação de prova e resposta emergencial. Um caso de recomendação nociva pode exigir análise de curadoria e redução de alcance. Cada cenário seleciona deveres diferentes, e a responsabilidade depende da ligação entre o dever violado e o resultado.

A aplicação dos pressupostos pode ser ilustrada por hipótese de recomendação autolesiva. Primeiro, confirma-se que adolescentes eram usuários previsíveis do serviço. Segundo, identifica-se o dever de mitigação de conteúdo sensível e de manutenção de canal de denúncia. Terceiro, apura-se a existência de alerta ou padrão reconhecível. Quarto, verifica-se o dano. Por fim, reconstrói-se em que medida a recomendação ou a omissão contribuiu para o resultado.

Outra hipótese envolve publicidade comportamental. O serviço pode ser acessado por menores, coletar dados e direcionar anúncios com base em comportamento. O dever concreto pode ser limitar segmentação, informar adequadamente ou bloquear certos produtos. A falha será avaliada conforme previsibilidade, controle e dano. Esses exemplos demonstram que os pressupostos funcionam em casos diversos, sem depender apenas de remoção de conteúdo.

A aplicação cumulativa dos pressupostos facilita a expansão para casos futuros. Novas plataformas, novas formas de inteligência artificial e novos modelos de

interação poderão surgir, mas o método permanece útil: identificar público, dever, falha, dano e nexo. Essa adaptabilidade é importante em direito digital, no qual a lei não consegue prever antecipadamente cada funcionalidade.

Os pressupostos devem ser utilizados também para rejeitar pedidos mal formulados. Se a parte não identifica o serviço, a funcionalidade, o dever e o nexo, a demanda tende a permanecer genérica. A proteção de menores não autoriza condenação por indignação. O modelo proposto é exigente justamente porque busca permitir responsabilização forte nos casos adequados e afastá-la quando faltar base técnica ou jurídica.

5.2 Descumprimento de dever proativo e presunção de causalidade

O descumprimento de dever proativo ocorre quando a plataforma deixa de adotar providência juridicamente exigível de prevenção, segurança, transparência ou resposta diante de risco previsível a crianças e adolescentes. A falha pode estar na concepção do serviço, na operação cotidiana ou na reação a um incidente. O enquadramento temporal é relevante porque uma configuração insegura por padrão, uma recomendação nociva e uma denúncia ignorada representam condutas distintas e exigem provas diferentes (BRASIL, 2025a; FRAZÃO, 2021).

A presunção de causalidade, nesse contexto, não substitui a demonstração do fato lesivo nem autoriza imputação baseada apenas na condição de menor da vítima. Sua função é enfrentar situações em que a parte autora apresenta indícios objetivos de conexão com o serviço, mas os elementos capazes de confirmar ou afastar a cadeia técnica permanecem sob domínio exclusivo da empresa. Trata-se de presunção relativa, estruturada para equilibrar acesso à prova e preservar o contraditório (MULHOLLAND, 2009; BRASIL, 2015a).

Convém distinguir presunção de causalidade e presunção de defeito. A primeira permite inferir contribuição causal a partir de fatos conhecidos e da indisponibilidade injustificada de dados técnicos. A segunda diz respeito à inadequação do serviço em relação à segurança legitimamente esperada. Ambas podem dialogar em um mesmo caso, mas a decisão deve declarar qual inferência está sendo utilizada, quais fatos a sustentam e de que modo a plataforma poderá produzir prova em sentido contrário.

O ponto de partida probatório é sempre um fato-base verificável. Protocolos de denúncia, sequência de recomendações, histórico de exposição, identificação de anúncio, alteração de alcance, configuração pública de perfil ou ausência de resposta

podem cumprir essa função. Alegações genéricas de que “o algoritmo causou o dano” são insuficientes. A inferência somente se legitima quando a irregularidade apontada guarda correspondência com o tipo de lesão que o dever pretendia evitar (TEPEDINO; TERRA; GUEDES, 2024).

A correspondência entre dever e risco funciona como limite material. Se a plataforma deixa de restringir contato de desconhecidos e ocorre abordagem abusiva, existe proximidade entre a salvaguarda omitida e o dano. Em contrapartida, falha contratual sem relação com a exposição alegada não autoriza presunção causal. Esse teste evita que qualquer desconformidade administrativa seja convertida em fundamento autônomo de indenização.

A assimetria informacional explica a necessidade de cooperação probatória. Crianças, adolescentes e responsáveis conseguem documentar o resultado externo do incidente, mas raramente têm acesso a métricas de recomendação, registros de moderação, critérios de segmentação, testes de segurança ou fluxos internos de resposta. Quando esses dados são relevantes e permanecem exclusivamente com a plataforma, o art. 373, § 1º, do CPC permite distribuir o encargo conforme a possibilidade real de produção da prova (BRASIL, 2015a).

Essa distribuição não inverte automaticamente todos os encargos. A parte autora continua responsável por individualizar a vítima, a funcionalidade discutida, o dano, o período de exposição e os indícios de participação do serviço. À plataforma caberá esclarecer os aspectos internos que não poderiam ser demonstrados externamente. A divisão deve ser definida em decisão fundamentada, com indicação dos documentos esperados e prazo razoável para apresentação.

A proteção de segredos empresariais não elimina o dever de colaboração. Relatórios de impacto, parâmetros gerais de classificação, trilhas de auditoria, *logs* relacionados ao perfil afetado e registros de providências podem ser apresentados sob sigilo processual ou com anonimização. O objetivo não é abrir integralmente o código-fonte, mas permitir explicação suficiente sobre o papel da funcionalidade no episódio concreto.

A omissão documental pode adquirir valor indiciário quando a empresa deveria conservar registros mínimos e não apresenta justificativa plausível para sua ausência. A inexistência de protocolos, histórico de moderação ou documentação de decisão não produz responsabilidade automática; contudo, enfraquece a alegação de

diligência quando o fornecedor controla a infraestrutura e afirma ter seguido procedimentos que não consegue demonstrar.

O nexo digital costuma ser multifatorial. Conteúdo de terceiro, compartilhamentos, mecanismos de recomendação, falha de privacidade, demora de resposta e vulnerabilidades pessoais podem atuar conjuntamente. A análise não precisa eleger uma causa única, mas deve identificar se a conduta da plataforma criou, ampliou ou conservou parcela juridicamente relevante do risco. O fato de outros agentes participarem do evento não elimina, por si só, a contribuição empresarial (SCHREIBER, 2015).

A dimensão temporal auxilia a reconstrução causal. Antes do incidente, examinam-se avaliação de risco, privacidade por padrão, controles etários e desenho da funcionalidade. Durante a exposição, observam-se recomendação, impulsionamento, segmentação e disponibilidade de canais de denúncia. Depois da ciência, avaliam-se tempo de resposta, preservação de evidências, comunicação à família e correção de falhas recorrentes. Cada momento pode gerar consequência própria.

Em caso de recomendação reiterada de conteúdo autolesivo, por exemplo, a parte autora pode apresentar histórico de visualização, capturas de tela e tentativas de interrupção. A plataforma terá melhores condições de esclarecer por que o conteúdo foi repetido, quais classificadores eram utilizados, se havia mecanismos de redução e que providências foram tomadas após os sinais de risco. A presunção somente se mantém se a documentação faltar ou confirmar contribuição relevante do sistema.

Na exposição íntima de adolescente, a sequência probatória é distinta. A existência do material, a notificação identificável e o período de permanência formam o núcleo externo. *Logs* de recebimento, priorização da denúncia, medidas de indisponibilização e prevenção de republicação integram a esfera empresarial. O nexo poderá abranger tanto a permanência injustificada quanto a ampliação posterior, sem atribuir à plataforma a autoria originária do conteúdo.

Em publicidade comportamental dirigida a criança, o foco recai sobre perfilamento, critérios de segmentação, identificação da natureza comercial e controles de faixa etária. A vítima não precisa reconstruir toda a cadeia de dados, mas deve indicar o anúncio, a exposição e a relação com o serviço. A empresa poderá

afastar a inferência demonstrando que não houve direcionamento etário, que adotou bloqueios adequados ou que a distribuição ocorreu por fator externo imprevisível.

A prova em contrário permanece essencial. A plataforma pode demonstrar que respondeu tempestivamente, que a recomendação alegada não ocorreu, que o conteúdo não foi impulsionado, que o risco era tecnicamente imprevisível ou que o dano decorreu de fato exclusivo de terceiro. A presunção organiza a incerteza; não antecipa a condenação nem impede o reconhecimento de excludentes.

A intensidade da inferência deve acompanhar a robustez do conjunto fático. Uma denúncia específica ignorada, somada a exposição persistente e ausência de registros, sustenta presunção mais forte do que narrativa sem data, conteúdo ou funcionalidade identificável. O julgador precisa explicitar esse grau de convencimento para permitir controle recursal e evitar que a técnica se transforme em fórmula abstrata.

A inconsistência entre política declarada e prática observada também pode demonstrar falha. Se a plataforma anuncia prioridade para denúncias envolvendo menores, mas não apresenta fluxo, prazo ou registro compatível, a confiança criada por sua própria comunicação passa a integrar a avaliação. A boa-fé objetiva exige coerência entre promessa de segurança e operação efetiva do serviço.

A atuação administrativa da ANPD pode densificar padrões de governança, aferição etária, transparência e proteção de dados, mas não autoriza responsabilidade civil retroativa. O fato deve ser examinado segundo as normas e o conhecimento técnico disponíveis no momento da conduta. Orientações posteriores podem auxiliar a interpretação, desde que não sejam convertidas em dever inexistente à época.

Na prática, a aplicação da presunção relativa pode seguir uma sequência controlável: identificação do dano e da funcionalidade; apresentação de indícios mínimos; delimitação do dever proativo; especificação dos documentos sob controle da plataforma; oportunidade de exibição e explicação; avaliação de eventual omissão; e exame final do nexo, das excludentes e da extensão da contribuição causal. Essa ordem reduz decisões intuitivas e torna transparente a passagem do fato conhecido ao fato técnico inferido.

A consequência processual deve guardar relação com a informação ausente. A falta de *log* de denúncia pode influenciar a análise da ciência e do tempo de resposta, mas não prova automaticamente que o conteúdo foi recomendado. A ausência de dados de segmentação pode pesar na publicidade, sem resolver por si

só o dano psicológico alegado. A inferência deve permanecer limitada ao ponto que a prova empresarial poderia esclarecer.

A utilidade da presunção depende também de salvaguardas processuais. O fato-base precisa ser delimitado, a informação requerida deve guardar relação com a controvérsia e a plataforma deve ter oportunidade efetiva de exibir registros ou justificar sua indisponibilidade. Sem esses limites, a técnica deixaria de corrigir assimetria probatória e passaria a funcionar como atalho para condenação.

Antes do exame das excludentes, é necessário precisar como preservação de evidências, porte do serviço, não exibição documental e perícia funcional interferem na reconstrução causal. Esses elementos não criam responsabilidade autônoma, mas definem a qualidade da prova disponível e o alcance legítimo das inferências judiciais.

A preservação de evidências precisa ser proporcional ao risco e delimitada no tempo. Em incidentes que envolvam exposição íntima, publicidade direcionada ou recomendação potencialmente lesiva, a plataforma deve conservar os registros necessários para reconstruir o evento sem acumular dados indefinidamente. A ordem judicial pode especificar período, categorias de informação e medidas de sigilo, conciliando direito à prova, minimização e proteção da própria vítima (BRASIL, 2018; ROSA; PIN, 2022).

O porte e a função do serviço influenciam a extensão do dever probatório. Uma plataforma de grande escala, que opera sistemas sofisticados de personalização, possui capacidade superior para registrar decisões e explicar critérios de distribuição. Serviços menores não estão dispensados de diligência, mas o grau de documentação exigível deve observar tecnologia disponível, volume de usuários e intensidade do risco. A proporcionalidade impede que a colaboração se transforme em obrigação impossível e evita que a escala seja utilizada como justificativa para opacidade.

A consequência da não exibição deve ser definida com precisão. O juiz pode considerar verdadeira a existência de ciência, recomendação ou falha de resposta apenas quando o documento requerido era pertinente, estava sob controle da empresa e sua ausência não foi justificada. A sanção não deve alcançar fatos que o registro não teria capacidade de provar. Esse cuidado aproxima a presunção de uma técnica racional de inferência, e não de punição processual genérica.

A separação entre teoria e aplicação também precisa ser preservada. O tópico 3.6 fundamentou a admissibilidade das presunções e da distribuição dinâmica; neste momento, o objetivo é converter essas categorias em procedimento decisório. A

utilidade da construção está em permitir que as partes saibam, desde o início, quais fatos mínimos devem apresentar, quais informações podem ser exigidas e em que condições a inferência será mantida ou afastada.

A delimitação do fato-base deve anteceder qualquer ordem ampla de exibição. Em demanda sobre recomendação nociva, por exemplo, a parte autora pode indicar perfil, período, conteúdo, sequência de exposição e efeitos observados; a plataforma, por sua vez, deve esclarecer os sinais de recomendação, as medidas de redução de alcance, os registros de denúncia e os testes de segurança pertinentes. Esse método evita pedidos genéricos sobre todo o sistema e permite que a prova se concentre na funcionalidade que teria contribuído para o dano. A proporcionalidade probatória protege a vítima sem transformar o processo em devassa tecnológica (BRASIL, 2015a; MULHOLLAND, 2009).

A preservação de registros deve observar finalidade e limite temporal. *Logs*, métricas e decisões de moderação não precisam ser conservados indefinidamente, mas sua eliminação após ciência de incidente relevante pode comprometer a reconstrução causal. Uma vez comunicada a controvérsia, a plataforma deve adotar protocolo de retenção compatível com o risco, preservando o material necessário e segregando dados de terceiros. Essa cautela aproxima proteção de dados e direito à prova, pois reduz exposição excessiva ao mesmo tempo que impede desaparecimento da informação indispensável ao contraditório (BRASIL, 2018; SARLET et al., 2021).

A não apresentação injustificada de documentos submetidos ao controle exclusivo do fornecedor pode produzir consequência probatória adversa, mas essa consequência exige decisão fundamentada. O julgador deve indicar qual registro era pertinente, por que estava disponível, de que modo foi solicitado e qual inferência decorre da omissão. A ausência de um dado secundário não autoriza presumir toda a cadeia causal; já a supressão de histórico de denúncias ou de métricas diretamente relacionadas ao evento pode reforçar a narrativa construída por outros indícios. A técnica deve ser calibrada ao valor informativo do elemento não exibido (BRASIL, 2015a; MULHOLLAND, 2009).

A perícia, quando necessária, deve privilegiar explicações funcionais e resultados reproduzíveis. Em vez de exigir acesso irrestrito a código-fonte ou segredo industrial, o perito pode examinar documentação de produto, parâmetros de teste, amostras de recomendação, registros de alcance e procedimentos internos de

mitigação. A empresa conserva o direito de proteger conhecimento competitivo, mas não pode invocar sigilo para impedir todo controle sobre a segurança do serviço. O processo deve combinar acesso restrito, anonimização e quesitos específicos, de modo que a prova seja tecnicamente suficiente e juridicamente proporcional (BRASIL, 2015a; SARLET et al., 2021). Com esses parâmetros, o descumprimento do dever proativo e a presunção causal permanecem categorias distintas: a primeira identifica a falha objetiva; a segunda disciplina a inferência sobre a contribuição do serviço. O tópico seguinte examina os fatos capazes de romper ou limitar essa imputação.

5.3 Excludentes admissíveis e limites da imputação

As excludentes são indispensáveis para impedir que a responsabilidade objetiva se converta em garantia universal contra todo dano ocorrido na internet. A prioridade conferida à infância intensifica o padrão de proteção, mas não elimina nexo causal, possibilidade de defesa ou necessidade de individualizar a contribuição do fornecedor. Fato exclusivo de terceiro, culpa exclusiva da vítima, caso fortuito externo, inexistência de dano e ausência de relação causal podem afastar ou limitar a imputação (CAVALIERI FILHO, 2024; TEPEDINO; TERRA; GUEDES, 2024).

A avaliação precisa respeitar uma ordem lógica. Primeiro, identifica-se o dever aplicável e a conduta atribuída à plataforma. Em seguida, apura-se se a falha contribuiu para o resultado. Somente então se examina se um evento externo rompeu integralmente a cadeia ou se houve concorrência causal. Invocar a excludente antes de esclarecer o dever pode ocultar omissão própria sob a simples afirmação de que o conteúdo foi criado por terceiro.

O fato exclusivo de terceiro ocorre quando a atuação externa absorve integralmente a produção do dano e não mantém vínculo relevante com risco próprio do serviço. A origem do conteúdo em usuário, por si só, não basta. Se a plataforma apenas hospedou material imprevisível, cumpriu o regime de resposta e não participou de sua amplificação, o autor externo poderá ser responsável único. Se houve recomendação, impulsionamento ou inércia qualificada, a exclusividade deixa de existir (BRASIL, 2014a; FRAZÃO, 2022).

A exclusividade exige prova positiva. A empresa deve apresentar registros capazes de demonstrar que não recomendou, monetizou ou ampliou o conteúdo, que possuía mecanismos compatíveis com o risco e que reagiu em tempo adequado após

receber sinal específico. Alegações genéricas de neutralidade técnica não substituem a reconstrução da funcionalidade discutida.

Considere-se publicação ofensiva inserida por usuário em comunidade de alcance restrito, removida logo após notificação precisa. Se não houver evidência de recomendação, publicidade ou falha anterior de segurança, o fato de terceiro poderá romper o nexo em relação à plataforma. A solução muda quando o mesmo material é promovido pelo sistema, permanece após denúncias reiteradas ou circula por rede automatizada detectável.

A culpa exclusiva da vítima deve ser aplicada com especial cautela em matéria infantojuvenil. Crianças pequenas possuem capacidade limitada para compreender persistência de dados, estratégias persuasivas e consequências de exposição pública. Em adolescentes, a autonomia progressiva pode influenciar o caso, mas não equivale automaticamente à plena capacidade de um adulto nem afasta o efeito de desenho manipulativo, informação insuficiente ou proteção etária inadequada (BRASIL, 1990a; UNITED NATIONS, 2021).

Para que a conduta da vítima rompa integralmente o nexo, deve ser determinante, consciente no grau compatível com sua idade e desvinculada de falha própria do serviço. A mera aceitação de termos de uso, a manutenção de perfil ou a interação com funcionalidade projetada para estimular permanência não bastam. É necessário demonstrar que o resultado não foi favorecido por arquitetura persuasiva, ausência de advertência ou resposta deficiente.

Em muitos casos, a figura mais adequada será a concorrência causal. O adolescente pode ter participado de interação arriscada, enquanto a plataforma falhou em limitar contato de desconhecidos ou ignorou denúncia grave. A contribuição do usuário pode repercutir na extensão da reparação, mas não elimina a parcela de risco criada ou ampliada pela empresa. A decisão deve explicar a participação de cada fator e evitar culpabilização automática da vítima.

A conduta dos responsáveis também pode ser considerada, desde que não seja utilizada para transferir à família deveres inerentes à organização do serviço. Mediação e acompanhamento são relevantes, porém não substituem privacidade por padrão, canais acessíveis, controles de publicidade e resposta a incidentes. Eventual omissão familiar somente terá efeito causal quando demonstrada de forma concreta e proporcional.

A invocação da conduta familiar exige, contudo, precisão dogmática. O art. 932, inciso I, do Código Civil, combinado com o art. 933, imputa aos pais responsabilidade independente de culpa pelos atos dos filhos menores que estiverem sob sua autoridade e companhia. Essa norma, porém, rege hipótese diversa da examinada nesta dissertação: ela disciplina a responsabilidade dos pais por danos causados pelo filho a terceiro, e não a situação em que o próprio filho é a vítima. Quando a criança ou o adolescente figura como lesado, o comportamento dos responsáveis não se enquadra no art. 932; ele apenas poderá ser examinado como fato de terceiro concorrente, na moldura do art. 14, § 3º, inciso II, do Código de Defesa do Consumidor, que somente admite exclusão quando a culpa de terceiro for exclusiva (BRASIL, 1990b; BRASIL, 2002).

Os deveres de vigilância, criação e educação previstos no art. 1.634 do Código Civil e no art. 22 do Estatuto da Criança e do Adolescente são deveres dirigidos à proteção do filho, e não posições jurídicas oponíveis pelo fornecedor em seu próprio benefício. Reconhecer o contrário produziria resultado incompatível com a proteção integral: a criança seria duplamente prejudicada, primeiro pela falha do serviço e depois pela omissão de quem deveria protegê-la. Por essa razão, a eventual negligência dos responsáveis não deve ser transposta automaticamente para a esfera da vítima como culpa concorrente redutora da indenização a que ela própria faz jus (BRASIL, 1990a; BRASIL, 2002).

Por outro lado, o caso fortuito externo pressupõe evento imprevisível, inevitável e estranho ao risco ordinário da atividade. Ataque excepcional que supera medidas de segurança adequadas pode romper o nexo; vulnerabilidade conhecida, falha recorrente de sistema ou ausência de atualização tendem a integrar o risco interno. A simples classificação do incidente como “falha técnica” ou “ataque cibernético” não resolve a controvérsia (SCHREIBER, 2015; FARIAS; ROSENVALD; BRAGA NETTO, 2023).

A previsibilidade deve ser aferida segundo porte, natureza do serviço, público provável e conhecimento técnico disponível no momento do fato. Plataformas de grande escala não podem tratar contato abusivo, exposição de imagens, exploração publicitária ou tentativas de automação como acontecimentos absolutamente inesperados. Em contrapartida, não se deve exigir ferramenta inexistente ou solução experimental que ainda não constituía padrão razoável de diligência.

A inevitabilidade também precisa ser demonstrada. Não basta afirmar que nenhum sistema é totalmente seguro. A empresa deve indicar avaliações realizadas, controles implementados, alertas recebidos, tempo de reação e motivo pelo qual medidas proporcionais não poderiam impedir ou reduzir o dano. A excludente será mais convincente quando acompanhada de documentação contemporânea ao incidente.

O limite temporal pode fracionar a responsabilidade. A plataforma talvez não pudesse impedir a primeira publicação, mas poderia ter reduzido alcance, bloqueado republicações ou preservado prova após ciência qualificada. Nesse caso, o fato de terceiro pode excluir imputação pelo início do evento e não pelo agravamento posterior. A decisão deve separar origem, manutenção e amplificação da lesão.

A inexistência de dano também integra os limites da imputação. Violação administrativa, falha documental ou descumprimento abstrato de política não produz automaticamente dever de indenizar. A tutela inibitória pode ser cabível diante de risco comprovado, mas a reparação pecuniária exige lesão juridicamente relevante. Essa distinção preserva a função preventiva sem banalizar o dano civil.

A ausência de nexo pode ser reconhecida quando a funcionalidade apontada não participou da exposição ou quando os registros demonstram que o evento ocorreu fora do ambiente controlado pela plataforma. A coincidência temporal não basta. É necessário examinar se a conduta empresarial foi condição relevante para criação, ampliação ou conservação do risco.

As excludentes podem produzir afastamento total ou redução proporcional. Em causalidade concorrente, o juiz deverá avaliar a intensidade da recomendação, a persistência do conteúdo, a reação da empresa, a participação do terceiro e a conduta da vítima. A repartição não deve ser intuitiva; precisa apoiar-se em elementos concretos e em justificativa sobre o peso atribuído a cada contribuição.

Em ações coletivas, a defesa por fato individual de usuário não afasta, por si só, discussão sobre política sistêmica. Configuração pública por padrão, ausência estrutural de canal de denúncia ou publicidade dirigida a menores podem atingir grupo indeterminado independentemente de comportamentos pessoais. A plataforma poderá contestar a existência do padrão, a adequação da medida requerida e a conexão entre a política e o risco coletivo.

Limites técnicos e direitos fundamentais também condicionam a imputação. Não se pode exigir vigilância integral de mensagens privadas, filtragem indiscriminada

ou medida incompatível com proteção de dados. A plataforma, porém, deve explicar por que determinada providência seria desproporcional e quais alternativas menos invasivas foram consideradas. Complexidade tecnológica não constitui excludente autônoma.

A prova das excludentes recai, em regra, sobre quem as invoca, especialmente quando os elementos estão sob controle empresarial. *Logs* de resposta, relatórios de segurança, registros de recomendação, auditorias e documentação de incidentes podem demonstrar diligência, exterioridade ou ruptura do nexo. A ausência injustificada desses elementos reduz a força da defesa sem gerar condenação automática.

Um ataque coordenado por contas externas ilustra a gradação possível. Se a plataforma detecta rapidamente o padrão, interrompe a rede, preserva dados e comunica autoridades, a atuação diligente pode afastar ou limitar responsabilidade. Se os sinais eram recorrentes, as denúncias foram ignoradas e a ferramenta continuou impulsionando o material, o comportamento externo não será causa exclusiva.

Em compras internas realizadas por criança, a análise deve considerar configuração do serviço, clareza das informações, autenticação, mecanismos de confirmação e atuação dos responsáveis. A conduta familiar pode concorrer, mas a plataforma não poderá invocar culpa exclusiva se o desenho explora impulsividade ou dificulta reconhecer o caráter oneroso da operação. A solução depende da interação entre proteção do consumidor e autonomia progressiva.

Além das excludentes clássicas, a análise precisa considerar situações que apenas limitam a imputação ou modificam a extensão da reparação. Consentimento formal, cumprimento de ordem válida, impossibilidade de evitar integralmente o resultado, atuação posterior da plataforma e autonomia progressiva do adolescente não produzem efeitos uniformes. Cada fator deve ser relacionado ao dever discutido e à parcela do dano que efetivamente poderia ser evitada.

Esses fatores podem ser organizados por uma matriz decisória: qual dever incidia; que conduta própria foi atribuída ao serviço; como essa conduta se relacionou ao dano; o evento externo rompeu ou apenas concorreu para o nexo; que discernimento era concretamente exigível da criança ou do adolescente envolvido, consideradas idade e etapa de desenvolvimento; e que documentação sustenta a

defesa. A resposta fundamentada a essas perguntas permite aplicar excludentes e causas de redução sem transformar categorias tradicionais em fórmulas automáticas.

A distinção entre ruptura do nexo, concorrência causal e mitigação posterior também repercute na escolha da tutela. Uma excludente que afaste indenização pelo evento inicial não impede, necessariamente, ordem de preservação de dados ou correção de risco futuro, desde que presentes os requisitos próprios. Da mesma forma, a responsabilidade por agravamento posterior não autoriza atribuir à plataforma todo o prejuízo originariamente causado por terceiro.

O consentimento formal não opera como excludente ampla quando o serviço é utilizado por menores. A concordância com termos extensos ou a autorização genérica de responsáveis não legitima prática incompatível com melhor interesse, transparência ou segurança. O consentimento poderá integrar a análise apenas quando for válido para a finalidade discutida, informado em linguagem adequada e livre de desenho que induza a escolha. Mesmo nessas condições, não exonera o fornecedor de deveres legais indisponíveis (BRASIL, 2018; FERNANDES; TEFFÉ; BRANCO, 2024).

Ordens de autoridades e medidas emergenciais também precisam ser consideradas. A plataforma que atua em cumprimento de determinação válida, dentro de seus limites, pode afastar imputação por efeitos inerentes à execução da ordem. A defesa perde força se houver excesso, demora injustificada ou aplicação a conteúdo diverso. A documentação da origem, do alcance e do momento da providência é essencial para distinguir cumprimento regular de falha autônoma.

Em situações de risco imediato, a impossibilidade de eliminar completamente o dano não afasta o dever de mitigação. Mesmo quando terceiro já iniciou a circulação, a empresa pode reduzir alcance, bloquear contas coordenadas, preservar provas e orientar a vítima. A excludente somente alcança a parcela inevitável do resultado; não cobre agravamento decorrente de omissão posterior. Essa distinção impede que a inevitabilidade inicial se transforme em licença para inércia.

A fundamentação deve indicar o efeito concreto de cada excludente. Reconhecer fato exclusivo implica afastar o nexo; admitir concorrência exige justificar eventual redução; identificar fortuito externo demanda demonstrar exterioridade e inevitabilidade. Sem essa explicitação, categorias distintas produzem o mesmo resultado de forma intuitiva. A precisão reforça previsibilidade e permite comparar decisões em casos semelhantes.

A causalidade concorrente exige solução distinta da exclusão total. Se o autor do conteúdo, a plataforma e eventualmente os responsáveis contribuíram em graus diferentes, a decisão deve explicitar a participação de cada agente. A responsabilidade objetiva não impede essa individualização; ao contrário, pressupõe que o risco próprio do serviço seja separado de fatores externos. A redução proporcional da reparação pode ser adequada quando a conduta alheia agravou o resultado sem romper integralmente o nexo, evitando tanto a transferência completa do dano à vítima quanto a imputação de consequências estranhas à atividade empresarial (TEPEDINO; TERRA; GUEDES, 2024; CAVALIERI FILHO, 2024).

A autonomia progressiva do adolescente também não pode ser convertida em excludente automática. O grau de compreensão, a idade, a informação disponibilizada e o desenho da interface influenciam a avaliação da conduta. Uma escolha feita após aviso claro e adequado difere de comportamento induzido por recompensa, pressão social, ocultação de risco ou recomendação persistente. A análise deve reconhecer capacidade crescente sem ignorar que o próprio serviço pode explorar impulsividade e busca de pertencimento. A culpa exclusiva somente se sustenta quando a decisão da vítima é livre, informada e determinante para o dano (BRASIL, 1990a; MACIEL, 2024a).

Em incidentes de segurança, a distinção entre fortuito interno e externo depende da relação com o risco ordinário do serviço. Ataques comuns, falhas conhecidas, credenciais comprometidas por mecanismos previsíveis e exploração de vulnerabilidade não corrigida integram a esfera empresarial. Situação diferente pode ocorrer diante de técnica inédita, inevitável mesmo com controles atualizados e sem qualquer contribuição do fornecedor. A plataforma que invoca exterioridade deve demonstrar governança anterior ao evento, resposta tempestiva e medidas de contenção, porque a simples sofisticação do ataque não basta para romper o nexo (BRASIL, 2018; CAVALIERI FILHO, 2024).

A conduta posterior ao dano influencia a extensão da reparação, embora nem sempre elimine a responsabilidade pelo evento já consumado. Remoção rápida, bloqueio de novas cópias, comunicação à família, preservação de evidências e oferta de canal especializado podem reduzir consequências e demonstrar diligência superveniente. Em sentido oposto, demora, perda de registros ou resposta padronizada diante de risco grave podem ampliar o dano. A decisão deve distinguir a causa inicial do agravamento posterior, atribuindo a cada fase os efeitos jurídicos

correspondentes e evitando que uma providência tardia apague falha anterior (ROSENVALD, 2017; FRAZÃO, 2021). Consideradas em conjunto, as excludentes preservam a justiça da imputação: afastam responsabilidade quando o risco é verdadeiramente externo, reduzem-na quando há concausas e mantêm a obrigação quando a arquitetura ou a resposta empresarial contribuiu de modo relevante. Com esses limites bem definidos, passa-se à escolha das tutelas adequadas.

5.4 Tutela inibitória, tutela coletiva e distribuição dinâmica do ônus da prova

A tutela inibitória é especialmente importante em danos digitais infantojuvenis porque a reparação posterior pode ser insuficiente. Exposição de imagem, contato abusivo, recomendação nociva ou publicidade exploratória podem gerar efeitos antes mesmo da formação de um processo indenizatório. Por isso, a tutela civil deve admitir medidas voltadas a impedir a repetição do dano, reduzir o alcance do risco e exigir ajustes proporcionais no serviço (BRASIL, 1985; BRASIL, 1990a).

A tutela coletiva ganha relevância quando o risco decorre de padrão sistêmico da plataforma. Falhas recorrentes de denúncia, ausência de privacidade por padrão, publicidade comportamental dirigida a menores ou recomendação de conteúdos inadequados podem atingir grupo indeterminado de crianças e adolescentes. Nesses casos, a solução individual não enfrenta a fonte do risco, razão pela qual medidas coletivas podem ser mais adequadas para corrigir a arquitetura do serviço (BRASIL, 1990b; ROSENVALD, 2017).

A distribuição dinâmica do ônus da prova complementa essas tutelas. Em litígios digitais, documentos decisivos frequentemente estão sob controle do fornecedor: *logs*, métricas de alcance, histórico de moderação, critérios de bloqueio, relatórios de risco e registros de denúncia. Exigir que a vítima prove integralmente elementos inacessíveis pode inviabilizar a proteção. A redistribuição deve ser fundamentada na assimetria concreta e na relevância da informação para o caso (BRASIL, 2015a; MULHOLLAND, 2009).

Essa técnica não dispensa a vítima de apresentar narrativa mínima. É necessário indicar o dano, o contexto, o serviço utilizado, a tentativa de denúncia ou o elemento que sugere falha da plataforma. A partir dessa base, pode-se exigir que o fornecedor apresente registros e justificativas compatíveis com seu dever de documentação. A tutela se torna equilibrada quando combina plausibilidade inicial e colaboração técnica do fornecedor.

Medidas inibitórias e coletivas devem ser proporcionais. O julgador deve evitar ordens vagas, impossíveis ou excessivamente invasivas. Obrigações de fazer podem envolver revisão de canal de denúncia, preservação de logs, transparência sobre resposta, limitação de publicidade, ajuste de privacidade ou relatório de risco, desde que vinculadas ao problema identificado. A intervenção judicial deve corrigir o risco sem substituir integralmente a gestão do serviço.

A proteção de dados também limita a produção de prova. A plataforma não pode usar o processo como justificativa para coleta indiscriminada ou exposição indevida de informações de menores. A prova deve respeitar minimização, necessidade, sigilo e proteção da criança. Esse cuidado mostra que a efetividade da tutela civil deve caminhar junto com a própria proteção que a dissertação busca defender (BRASIL, 2018; DONEDA, 2020).

Esses fundamentos permitem passar da enumeração das tutelas para sua operacionalização processual. A escolha entre providência individual, coletiva, inibitória ou probatória depende da origem do risco, do alcance da falha e da informação disponível. O ponto central é construir ordem executável, capaz de corrigir o problema identificado sem transferir ao Judiciário a administração cotidiana da plataforma.

A tutela coletiva é adequada quando a causa do dano está em política ou funcionalidade comum a uma pluralidade de usuários. Configuração pública por padrão, ausência de avaliação de risco, publicidade infantil ou canal de denúncia estruturalmente ineficaz não são corrigidos pela soma de indenizações individuais. A demanda coletiva permite discutir a arquitetura do serviço e formular obrigação uniforme, preservando as pretensões pessoais relativas aos danos já sofridos (BRASIL, 1985; BRASIL, 1990b).

A tutela inibitória exige probabilidade de ilícito e risco concreto de continuidade ou repetição. Não pressupõe que todos os danos já tenham ocorrido, pois sua função é impedir que a ameaça se realize ou se prolongue. Em ambiente digital, podem justificar a medida a persistência de recomendações nocivas, a circulação de publicidade proibida ou a manutenção de configuração insegura, desde que o pedido identifique a prática e a providência necessária.

A distribuição dinâmica do ônus da prova deve ser decidida de forma fundamentada e relacionada a fatos específicos. O juiz precisa indicar quais informações estão sob domínio da plataforma, por que são relevantes e quais

elementos mínimos já foram apresentados pela parte autora. Essa técnica não transfere genericamente toda a prova ao réu; ela corrige assimetria concreta relativa a *logs*, métricas, histórico de moderação, segmentação e resposta (BRASIL, 2015a; MULHOLLAND, 2009).

Um protocolo probatório pode organizar a produção documental em etapas. Primeiro, preservam-se dados para evitar perda ou alteração. Depois, delimitam-se período, perfil, conteúdo e funcionalidade. Em seguida, a plataforma apresenta registros técnicos e políticas aplicáveis, enquanto eventual perícia verifica consistência e causalidade. A sequência reduz pedidos excessivamente amplos e torna mais transparente o vínculo entre a prova requerida e o dever discutido.

Segredo comercial e proteção de dados não autorizam recusa absoluta à produção de prova. Informações sensíveis podem ser submetidas a segredo de justiça, anonimização, acesso restrito a peritos ou apresentação agregada. O desenho processual deve proteger terceiros e a segurança do sistema sem impedir o controle jurisdicional. A confidencialidade funciona como limite à forma de acesso, não como imunidade material da plataforma.

A urgência da tutela deve ser calibrada pela gravidade e pela reversibilidade. Exposição sexual de menor, aliciamento, desafio perigoso ou recomendação autolesiva podem exigir resposta imediata. Já controvérsias dependentes de ponderação complexa podem demandar contraditório prévio. A fundamentação precisa explicar por que a demora aumenta o dano e por que a medida escolhida é menos restritiva do que alternativas disponíveis.

Ordens estruturais devem definir resultado, prazo e indicadores de cumprimento, sem impor solução tecnológica única. O Judiciário pode exigir canal acessível, privacidade protetiva, revisão de fluxo publicitário ou avaliação de risco, deixando à empresa a escolha técnica compatível. Esse modelo preserva capacidade de inovação e evita que a decisão se torne obsoleta ou converta o magistrado em gestor do serviço.

Planos de conformidade podem ser exigidos quando a correção depende de várias providências coordenadas. O documento deve identificar responsáveis, cronograma, recursos, critérios de priorização e forma de comunicação aos usuários. Sua apresentação não encerra o controle: é necessário demonstrar implementação e efetividade. Políticas meramente declaratórias não bastam quando incidentes semelhantes continuam ocorrendo.

O acompanhamento do cumprimento pode utilizar relatórios periódicos, auditoria independente e amostragem de casos. A fiscalização deve ser temporária, proporcional e vinculada à obrigação determinada. Auditorias não precisam revelar código-fonte ou dados pessoais indiscriminadamente; podem avaliar processos, testes, taxas de resposta e documentação. O objetivo é verificar resultado, e não substituir permanentemente a governança interna.

A multa coercitiva deve guardar relação com capacidade econômica, gravidade do risco e resistência ao cumprimento. Valor irrisório perde função; valor desproporcional pode estimular bloqueios excessivos e afetar expressão legítima. A decisão deve prever momento de incidência, forma de comprovação e possibilidade de revisão. Astreintes são instrumento de efetividade, não indenização antecipada nem sanção automática.

A coisa julgada coletiva precisa ser compatibilizada com pretensões individuais. A correção da arquitetura pode beneficiar todo o grupo, enquanto indenizações pessoais dependem da demonstração de dano e nexo em cada caso. A decisão deve distinguir obrigação estrutural, reparação coletiva e direitos individuais homogêneos, evitando dupla reparação e preservando acesso das vítimas à tutela específica.

A perícia técnica pode ser essencial quando a controvérsia envolve recomendação, segmentação ou aferição etária. O objeto pericial deve ser formulado em linguagem funcional: quais objetivos orientavam o sistema, que sinais eram considerados, quais salvaguardas existiam e como o perfil afetado foi tratado. Perguntas genéricas sobre o algoritmo produzem respostas pouco úteis e ampliam custos sem esclarecer a cadeia causal.

A participação de especialistas em infância, proteção de dados e usabilidade pode melhorar a adequação da medida. Risco digital infantojuvenil não é apenas problema de engenharia; envolve compreensão, autonomia progressiva e efeitos sobre desenvolvimento. Pareceres técnicos devem auxiliar a tradução desses fatores em requisitos verificáveis, sem substituir a decisão jurídica sobre dever, ilicitude e proporcionalidade.

A escuta de crianças e adolescentes pode ser relevante em ações coletivas, desde que realizada de maneira segura e adequada à idade. Pesquisas de usabilidade, consultas protegidas e contribuições de entidades representativas ajudam a identificar dificuldades de denúncia, compreensão e controle. Essa

participação não transfere aos menores a responsabilidade pela solução; serve para evitar que medidas sejam formuladas exclusivamente a partir da perspectiva adulta.

A coordenação institucional evita ordens incompatíveis. ANPD, Ministério Público, órgãos de defesa do consumidor e sistema de garantia de direitos podem atuar sobre aspectos distintos da mesma prática. O processo coletivo deve considerar decisões e procedimentos já existentes, promovendo cooperação sem diluir responsabilidades. A multiplicidade de autoridades não pode produzir nem duplicidade sancionatória nem vazio de proteção.

A preservação de evidências deve ser determinada assim que houver risco de desaparecimento dos dados. *Logs*, histórico de denúncia, parâmetros de campanha e registros de moderação podem ser apagados por rotinas automáticas. A ordem precisa indicar escopo e duração, respeitando necessidade e minimização. Preservar não significa entregar imediatamente todo o conteúdo, mas impedir que a prova deixe de existir antes da análise judicial.

A destruição injustificada ou a não apresentação de registros relevantes pode produzir consequências processuais. O juiz deve examinar se havia dever de conservação, se a ordem era clara e se a perda impediu a reconstrução dos fatos. A consequência pode envolver presunção relativa, redistribuição do ônus ou valoração desfavorável da conduta, sempre com oportunidade de explicação e sem converter qualquer ausência documental em confissão.

Em prova algorítmica, transparência útil é mais importante que transparência meramente formal. Relatórios genéricos sobre princípios do sistema não esclarecem o tratamento do perfil afetado. Devem ser priorizados histórico de recomendações, categorias aplicadas, testes de segurança e medidas de redução de alcance. A exposição pode ocorrer em ambiente controlado, preservando propriedade intelectual e segurança.

A proporcionalidade exige comparar alternativas. Antes de ordenar remoção ampla, pode ser suficiente limitar recomendação, desativar segmentação ou restringir publicidade. Antes de exigir identificação documental de todos os usuários, podem existir mecanismos menos invasivos de estimativa etária ou configuração protetiva. A decisão deve justificar por que a providência escolhida protege o menor com o menor sacrifício necessário a outros direitos.

Serviços de mensageria privada demandam soluções próprias. A tutela não pode impor leitura generalizada de comunicações criptografadas. Medidas possíveis

incluem bloqueio facilitado, denúncia pelo destinatário, restrição de contato desconhecido, preservação de metadados nas hipóteses legais e resposta a contas abusivas. O dever deve respeitar a arquitetura do serviço e o sigilo comunicacional.

Tutela inibitória e reparação coletiva cumprem funções diferentes. A primeira interrompe ou previne a prática; a segunda compensa lesão transindividual e reconhece a gravidade social do comportamento. Nem toda falha estrutural produz automaticamente dano moral coletivo. É necessário demonstrar violação relevante a valores compartilhados e extensão que ultrapasse desconfortos individuais.

Medidas estruturais devem prever revisão periódica. Tecnologias, riscos e formas de abuso mudam rapidamente, de modo que obrigações muito rígidas podem perder utilidade. Cláusulas de reavaliação permitem adaptar prazos e indicadores mediante fundamentação, sem reabrir o mérito indevidamente. A flexibilidade deve ser controlada e transparente, não delegação irrestrita à plataforma.

O porte e a função do serviço influenciam a extensão da obrigação. Grandes plataformas possuem escala, dados e capacidade técnica superiores, enquanto aplicações menores podem cumprir o mesmo objetivo por procedimentos mais simples. A proporcionalidade não reduz a proteção do menor; ajusta o meio exigido à capacidade de intervenção e evita que a tutela se converta em barreira injustificada à entrada.

A dimensão transnacional das plataformas pode exigir cooperação para execução e obtenção de prova. A presença de representante no país, a localização dos dados e a cadeia contratual devem ser identificadas desde o início. A complexidade societária não pode impedir cumprimento de ordem brasileira quando o serviço atua no mercado nacional, mas a medida deve respeitar competência, tratados e limites de alcance territorial.

Protocolos de emergência são justificáveis para riscos de elevada gravidade, como exploração sexual, ameaça concreta ou incentivo à automutilação. Eles devem definir critérios de acionamento, revisão humana, preservação de evidências e comunicação com autoridades competentes. A urgência não elimina controles; exige procedimentos previamente desenhados para que a resposta rápida seja também auditável e proporcional.

A integração entre tutela inibitória, ação coletiva e prova dinâmica transforma a responsabilidade civil em mecanismo de prevenção, correção e reparação. O modelo é legítimo quando parte de risco identificado, delimita a informação necessária e

produz ordem executável. Dessa forma, o processo enfrenta falhas de governança sem instaurar vigilância geral, responsabilidade integral ou microgestão judicial da tecnologia.

5.5 Danos individuais, coletivos e danos ao desenvolvimento biopsicossocial

Os danos digitais infantojuvenis podem assumir dimensão individual, coletiva e relacionada ao desenvolvimento biopsicossocial. Essas categorias não devem ser tratadas como rótulos acumuláveis de forma automática. A classificação serve para identificar o bem jurídico atingido, a extensão da lesão, os legitimados e a tutela adequada. A decisão precisa evitar tanto a banalização de desconfortos cotidianos quanto a invisibilização de efeitos que não possuem expressão patrimonial imediata.

O dano individual alcança direitos da personalidade, patrimônio e autonomia informativa de uma vítima determinada. Exposição de imagem, ofensa à honra, divulgação de dados, contato abusivo, fraude e publicidade exploratória podem produzir consequências distintas. A análise deve considerar idade, contexto familiar e escolar, alcance, duração, possibilidade de replicação, tentativas de interrupção e resposta oferecida pela plataforma (MORAES, 2003; MACIEL, 2024a).

A violação de imagem íntima possui gravidade própria porque a circulação digital pode escapar ao controle da vítima mesmo depois da indisponibilização inicial. Protocolos de denúncia, registros de compartilhamento, tempo de resposta e medidas contra republicação auxiliam a dimensionar o dano. A reparação pecuniária pode ser acompanhada de remoção, desindexação quando cabível, preservação de prova e proteção do sigilo processual.

Nos danos à privacidade e aos dados pessoais, a lesão não se limita a prejuízo econômico. Perfilamento indevido, inferência de vulnerabilidades, exposição de localização ou compartilhamento sem base adequada podem reduzir o controle da criança sobre sua identidade digital. A gravidade dependerá da sensibilidade dos dados, da finalidade, do número de destinatários, da permanência e do risco de reutilização (BRASIL, 2018; DONEDA, 2020).

Dano material exige demonstração de perda efetiva, despesa ou frustração economicamente mensurável. Gastos com tratamento, mudança de escola, proteção de contas ou recuperação de dados podem ser relevantes quando vinculados ao incidente. A reparação não deve incluir valores hipotéticos sem base, mas pode

abranger custos razoavelmente necessários para conter ou remediar consequência previsível.

O dano moral individual não depende sempre de diagnóstico clínico. Violações objetivas de honra, imagem, intimidade ou autodeterminação podem ser reconhecidas a partir da própria gravidade do fato. Quando a alegação envolve repercussões complexas sobre saúde mental ou desenvolvimento, avaliações especializadas, relatos escolares e contexto familiar ajudam a demonstrar intensidade e duração sem transformar a perícia em requisito universal.

A resposta posterior da plataforma interfere na extensão da lesão. Remoção rápida, comunicação clara, preservação de evidências e prevenção de republicação podem reduzir agravamento. Demora, perda de registros, resposta padronizada ou continuidade da recomendação podem ampliar o dano. A conduta posterior não apaga a falha original, mas integra a quantificação e a escolha das medidas reparatórias.

O dano coletivo não corresponde à soma aritmética de lesões individuais. Ele surge quando prática sistêmica viola valor transindividual ou expõe grupo indeterminado de crianças e adolescentes a padrão incompatível de segurança. Perfilamento em massa, publicidade comportamental infantil, ausência de privacidade por padrão ou canal de denúncia estruturalmente ineficaz podem justificar tutela coletiva, ainda que nem todas as vítimas sejam identificadas. Não se trata de somar danos individuais, mas de reconhecer lesão autônoma ao padrão social de segurança, cuja reparação deve vincular-se à gravidade, à duração, ao alcance e ao benefício obtido com a prática (BRASIL, 1985; BRASIL, 1990b; ROSENVALD, 2017).

A prova do dano coletivo pode combinar documentos institucionais, pesquisas, reclamações convergentes, auditorias, políticas de *design* e dados de alcance. Não é necessário identificar cada vítima quando o objeto é a própria prática empresarial. Ainda assim, a decisão deve demonstrar relevância social da violação e evitar presumir dano coletivo a partir de irregularidade isolada sem capacidade de afetar o grupo.

A reparação coletiva deve guardar relação com a natureza transindividual do interesse. Obrigações de fazer, alteração de configuração, melhoria de canais, relatórios de transparência e destinação de valores a fundos legalmente previstos podem ser mais adequados do que simples multiplicação de indenizações. É necessário evitar duplicidade entre condenação coletiva e reparações individuais pelo mesmo prejuízo.

O dano ao desenvolvimento biopsicossocial exige definição rigorosa. Ele se refere a impactos comprováveis sobre formação identitária, saúde, relações sociais, escolarização, autonomia e participação, e não a qualquer sofrimento associado ao uso da internet. A expressão somente acrescenta valor analítico quando o texto identifica a dimensão afetada, a duração, a intensidade e a conexão com a prática digital.

Exposição prolongada a assédio, recomendação autolesiva, pressão estética ou contato predatório pode repercutir em autoestima, sono, convivência, rendimento escolar e confiança social. Esses efeitos são avaliados a partir do conjunto do caso. Laudos psicológicos ou médicos podem ser necessários em situações complexas, mas não substituem a prova da funcionalidade, do período de exposição e da contribuição da plataforma (UNICEF, 2025).

A causalidade biopsicossocial raramente é exclusiva. Condições pessoais, ambiente familiar, escola, terceiros e arquitetura do serviço podem interagir. O julgador deve evitar tanto atribuir todo sofrimento à plataforma quanto negar contribuição relevante porque existem outros fatores. A análise de concausas permite reconhecer parcela de influência sem formular conclusões clínicas que o processo não sustenta.

Danos cumulativos merecem atenção específica. Uma recomendação isolada pode não explicar o resultado, enquanto a repetição, o estreitamento progressivo do conteúdo e a ausência de mecanismos de interrupção podem formar cadeia lesiva. A prova deve reconstruir frequência, duração, mudanças de comportamento e sinais oferecidos ao serviço. A temporalidade ajuda a distinguir coincidência de contribuição causal.

Danos futuros são reparáveis quando apresentam probabilidade concreta, e não mera especulação. Vazamento de dados de menores pode ampliar risco de fraude, perseguição ou discriminação posterior. Em certas hipóteses, custeio de monitoramento, reforço de segurança ou medidas preventivas será mais adequado do que indenização baseada em receio abstrato. A possibilidade futura não autoriza reparação fundada em conjectura: exige elementos clínicos, sociais ou contextuais que demonstrem risco concreto. Em situações de evolução incerta, o acompanhamento periódico, o custeio de tratamento e a revisão posterior da tutela tendem a ser mais adequados do que estimativa definitiva e antecipada de todas as consequências (UNICEF, 2025; AZEVEDO; TORRES, 2023).

A voz da criança ou do adolescente precisa ser considerada conforme idade e maturidade. A reparação pode envolver retirada de conteúdo, anonimização, pedido de desculpas, apoio ou restrição de contato, e a preferência da vítima pode influenciar a escolha. A escuta deve ocorrer de forma protegida, evitando exposição processual que agrave o dano e respeitando sigilo e melhor interesse.

Medidas não pecuniárias são particularmente relevantes. Retificação, indisponibilização, desindexação, correção de perfil, retirada de perfis falsos, bloqueio de contato, comunicação a responsáveis, preservação de sigilo, suporte especializado e revisão de mecanismos de recomendação podem produzir resultado mais útil do que valor monetário isolado, sem que disso decorra obrigação impossível ou dever de vigilância geral. A ordem deve indicar objeto, prazo e critério de cumprimento para não se tornar comando genérico ou impossível.

A quantificação do dano individual deve ser fundamentada em fatores verificáveis: gravidade do direito violado, idade, alcance, duração, repetição, finalidade econômica, resposta do fornecedor e possibilidade de recuperação. Tabelas rígidas podem ignorar a singularidade do caso; valores sem parâmetros favorecem arbitrariedade. A função compensatória deve conviver com prevenção e proporcionalidade, e a fundamentação precisa explicar por que aqueles elementos justificam a medida adotada, permitindo controle recursal e reduzindo disparidades entre casos semelhantes (MORAES, 2003; ROSENVALD, 2017).

Esses fatores, contudo, só se tornam operacionais quando ancorados em regra de medida e em método de arbitramento. A regra de medida está no art. 944, caput, do Código Civil: a indenização mede-se pela extensão do dano, comando reforçado, na relação de consumo, pelo princípio da reparação integral do art. 6º, inciso VI, do Código de Defesa do Consumidor. Daí decorrem dois limites simétricos: o valor não pode ficar aquém da repercussão efetivamente demonstrada, nem convertê-la em fonte de enriquecimento sem causa. A redução equitativa autorizada pelo parágrafo único do art. 944, por representar exceção à reparação integral, comporta interpretação restritiva, e sua incidência nas hipóteses de responsabilidade objetiva permanece controvertida na doutrina, razão pela qual seu emprego exige fundamentação específica e não deve ser mobilizado como atenuação genérica em favor do fornecedor (BRASIL, 1990b; BRASIL, 2002; CONSELHO DA JUSTIÇA FEDERAL, 2012).

Quanto ao método, o arbitramento do dano extrapatrimonial pode valer-se do critério bifásico consolidado pela jurisprudência do Superior Tribunal de Justiça. Na primeira fase, fixa-se valor básico de referência a partir de precedentes que examinaram o mesmo interesse jurídico lesado, o que assegura tratamento isonômico entre casos semelhantes. Na segunda, esse valor é ajustado às circunstâncias concretas, considerada a extensão do dano, a intensidade da lesão, a repercussão sobre a vítima e a conduta das partes. A transposição do método para os danos digitais infantojuvenis exige apenas que o interesse jurídico lesado seja corretamente identificado na primeira fase – imagem íntima, dados pessoais, honra, autodeterminação informativa ou desenvolvimento –, pois é essa identificação que define o conjunto de precedentes comparáveis. Na segunda fase incidem os fatores próprios do ambiente digital: alcance da difusão, persistência do conteúdo, reiteração após ciência qualificada, grau de amplificação algorítmica e tempestividade da resposta institucional (BRASIL, 2011; MORAES, 2003).

Resta a questão da função dissuasória. O direito brasileiro não acolhe a indenização punitiva (*punitive damages*) como categoria autônoma e a condenação não pode ser arbitrada como sanção desvinculada da extensão do dano. Isso não significa, porém, que o efeito preventivo seja juridicamente indiferente. Em danos produzidos em escala, nos quais a prática lesiva gera proveito econômico mensurável, uma reparação sistematicamente inferior ao benefício obtido converte a indenização em custo operacional previsível e neutraliza a função preventiva da responsabilidade civil. A solução compatível com o ordenamento não está em majorar o dano individual além de sua extensão, mas em mobilizar os instrumentos próprios da tutela transindividual: o dano moral coletivo, com destinação a fundo legalmente previsto, e as obrigações de fazer com metas verificáveis, que atuam sobre a causa estrutural da lesão em vez de apenas compensar seus efeitos (ROSENVALD, 2017; BRASIL, 1985).

É com esses parâmetros que se opera a última etapa da matriz decisória proposta ao final deste trabalho. A escolha de tutela proporcional ao risco e à lesão não é juízo discricionário: pressupõe identificar o interesse lesado, verificar sua extensão, situar o caso entre precedentes comparáveis, ajustar o valor às circunstâncias verificadas e justificar a preferência entre providências específicas e reparação pecuniária, que no âmbito infantojuvenil frequentemente recai sobre as primeiras.

Na publicidade comportamental dirigida a crianças, o dano pode envolver exploração da inexperiência, tratamento indevido de dados e indução ao consumo. Nem toda visualização gera reparação individual; é preciso demonstrar exposição, prática abusiva e repercussão. Em escala, entretanto, política sistemática de segmentação pode fundamentar tutela coletiva mesmo quando o prejuízo de cada usuário é de difícil individualização (BRASIL, 1990b; BRASIL, 2014b).

Em caso de recomendação reiterada de conteúdo autolesivo, a tutela deve distinguir o material originário, a amplificação algorítmica e o efeito sobre a vítima. Histórico de recomendações, tentativas de interrupção, resposta a denúncias e avaliação especializada podem demonstrar contribuição relevante. A reparação deve evitar afirmar causalidade médica total e concentrar-se na parcela de risco comprovadamente ampliada pelo serviço.

No perfilamento massivo de menores, o interesse coletivo decorre da política de tratamento e da exposição comum a riscos. A adequação da base legal, a minimização, a transparência e a finalidade são elementos centrais. A solução pode exigir cessação da prática, exclusão ou segregação de dados, auditoria e comunicação, além de indenização quando houver lesão transindividual relevante (BRASIL, 2018).

A legitimação coletiva permite enfrentar falhas que dificilmente seriam discutidas em milhares de ações individuais. Ministério Público, entidades e demais legitimados podem buscar correção estrutural, desde que a causa de pedir identifique política comum e risco compartilhado. A tutela não deve transformar incidente isolado em obrigação geral, nem exigir monitoramento indiscriminado sem base normativa.

A prevenção integra a resposta aos danos sem confundir risco e lesão consumada. Diante de probabilidade concreta de repetição, tutela inibitória pode ser concedida antes que novas vítimas apareçam. Para indenização, entretanto, permanecem necessários os pressupostos próprios. A distinção evita usar linguagem de dano para justificar toda medida preventiva e mantém clareza dogmática.

A prova pode combinar elementos digitais e extradigitais. Capturas de tela, protocolos, *logs*, dados de alcance e políticas internas demonstram a dinâmica *online*; relatórios escolares, atendimentos, testemunhos e avaliações especializadas ajudam a revelar repercussões. O conjunto deve ser analisado de forma integrada, pois nenhum documento isolado costuma explicar toda a experiência da vítima.

Uma matriz de avaliação pode organizar o julgamento: situar a condição do lesado quanto à idade e ao estágio de desenvolvimento; identificar o direito atingido; classificar a dimensão individual ou coletiva; verificar eventual repercussão sobre desenvolvimento; reconstruir duração, alcance e resposta; examinar causalidade e concausas; prevenir duplicidade; e escolher tutela pecuniária, específica ou estrutural. A sequência torna explícito por que determinado dano foi reconhecido e como a medida corresponde à lesão.

A prevenção de duplicidade exige mapear o objeto de cada condenação. O dano moral coletivo responde à lesão transindividual; a indenização individual compensa repercussões pessoais; o dano ao desenvolvimento somente deve ser reconhecido de forma autônoma quando houver dimensão específica comprovada. A mesma circunstância não pode ser remunerada repetidamente sob nomes distintos. A decisão deve explicar a função de cada parcela e sua relação com as medidas específicas concedidas.

A proteção de crianças e adolescentes exige sensibilidade sem abandono dos critérios jurídicos. Reconhecer a peculiaridade dos danos digitais não significa presumir sofrimento máximo, assim como exigir prova não autoriza ignorar lesões à identidade e à autonomia que não aparecem em balanços econômicos. A imputação objetiva encontra equilíbrio quando descreve o dano com precisão e vincula a reparação à contribuição efetiva da plataforma. Encerrada essa diferenciação, o direito comparado pode ser utilizado como apoio para concretizar prevenção e governança, sem importar automaticamente categorias indenizatórias estrangeiras.

5.6 Parâmetros comparados como apoio interpretativo

O direito comparado é utilizado nesta dissertação como instrumento de contraste e aprendizado institucional, não como fonte autônoma de obrigação civil no Brasil. A comparação permite observar como outros sistemas transformaram princípios de proteção da infância em deveres técnicos verificáveis. Sua utilidade está em testar a viabilidade de medidas como proteção por desenho, avaliação de risco, transparência algorítmica e resposta estruturada, sempre submetendo essas experiências à Constituição, ao ECA, ao CDC, à LGPD, ao Marco Civil e ao ECA Digital.

O *Age Appropriate Design Code*, elaborado pela autoridade britânica de proteção de dados, organiza padrões de desenho apropriado à idade. Entre seus

eixos estão melhor interesse da criança, minimização de dados, configurações de privacidade elevadas por padrão, limitação de geolocalização e redução de técnicas persuasivas. O documento demonstra que proteção infantil pode ser incorporada à fase de desenvolvimento do produto, em vez de depender exclusivamente de denúncias posteriores (ICO, 2022).

A principal contribuição do código britânico para o direito brasileiro é metodológica. Ele exige que o fornecedor identifique previamente como crianças provavelmente utilizarão o serviço e avalie impactos sobre privacidade e desenvolvimento. Essa lógica pode auxiliar a interpretar os deveres do ECA Digital, sobretudo quando a plataforma dispõe de dados que revelam presença significativa de menores. A importação literal, contudo, seria inadequada porque competências regulatórias e bases legais diferem entre os países.

Em uma plataforma de vídeos, por exemplo, o princípio de privacidade por padrão pode justificar conta infantil sem localização pública e com compartilhamento restrito. Em jogo conectado, pode exigir limitação de comunicação com desconhecidos e aviso claro sobre compras. Em rede social, pode recomendar desativação inicial de personalização sensível. Esses exemplos mostram que o dever de cuidado varia conforme funcionalidade e risco, não podendo ser reduzido a verificação etária única.

O *Digital Services Act* da União Europeia adota abordagem sistêmica para serviços intermediários, com obrigações graduadas segundo porte e função. Plataformas de grande escala devem avaliar riscos, adotar medidas de mitigação, oferecer transparência sobre publicidade e sistemas de recomendação e submeter determinados procedimentos a auditoria. O modelo reconhece que escala e arquitetura alteram a capacidade de produzir impactos sociais, o que se aproxima da análise de risco organizado desenvolvida nesta pesquisa (UNIÃO EUROPEIA, 2022).

No campo da infância, o DSA impede práticas publicitárias baseadas em perfilamento de menores em determinadas condições e exige atenção a riscos de saúde, segurança e direitos fundamentais. Sua contribuição para o Brasil está em demonstrar que transparência e avaliação periódica podem ser obrigações estruturais, não favores voluntários. O ECA Digital pode ser interpretado de forma compatível com essa racionalidade, respeitadas as diferenças entre o modelo europeu e o sistema brasileiro.

A comparação com o DSA também esclarece o papel da proporcionalidade. Uma pequena aplicação de caráter local não pode receber exatamente o mesmo conjunto de exigências de uma rede social global. O tamanho, a base de usuários, o modelo de negócio e a capacidade técnica influenciam a diligência esperada. Esse critério evita que deveres de proteção se convertam em barreiras desnecessárias à inovação, sem permitir que grandes plataformas invoquem complexidade como justificativa para omissão.

O *Online Safety Act* do Reino Unido concentra-se em deveres de segurança, avaliação de risco e tratamento de conteúdos prejudiciais, com atenção especial a crianças. O regime busca exigir que serviços compreendam riscos previsíveis e organizem sistemas de governança, denúncia e mitigação. Sua importância para esta dissertação está em reforçar a distinção entre moderação de conteúdo específico e segurança do sistema: a primeira reage a ocorrências; a segunda examina como o serviço favorece repetição, contato ou amplificação (UNITED KINGDOM, 2023).

O modelo britânico não deve ser convertido em obrigação de vigilância total. A experiência mostra, ao contrário, a necessidade de delimitar categorias de serviço e de dano, definir responsabilidades internas e produzir avaliações documentadas. Para o ECA Digital, essa lição sugere que políticas genéricas são insuficientes. A plataforma deve relacionar riscos identificados a medidas concretas, responsáveis definidos e indicadores de efetividade.

O Comentário Geral nº 25 do Comitê dos Direitos da Criança oferece perspectiva centrada em direitos. O documento afirma que o ambiente digital pode ampliar participação, educação e expressão, mas também produzir discriminação, exploração e invasão de privacidade. Recomenda que Estados e empresas considerem o melhor interesse, a evolução das capacidades e a inclusão digital. Diferentemente de regimes essencialmente regulatórios, o comentário conecta segurança e autonomia, evitando que proteção resulte em exclusão de crianças da vida digital (UNITED NATIONS, 2021).

Essa abordagem é relevante para aferição etária. Medidas de verificação podem reduzir acesso a riscos, mas também coletar dados adicionais, excluir usuários sem documentos ou comprometer anonimato. A solução deve equilibrar precisão, minimização e proporcionalidade. Sistemas de estimativa, declaração assistida, controle parental e verificação documental possuem diferentes custos e riscos. O padrão adequado depende da gravidade do conteúdo e da finalidade do serviço.

A síntese comparativa revela quatro convergências. A primeira é a passagem da reação para a prevenção. A segunda é a proteção por padrão. A terceira é a necessidade de avaliar risco conforme serviço, público e escala. A quarta é a documentação da diligência. Esses elementos podem auxiliar a densificar deveres brasileiros sem criar responsabilidade por simples semelhança com norma estrangeira.

Há, contudo, diferenças relevantes. O DSA possui arquitetura de supervisão europeia e categorias próprias de plataformas. O *Online Safety Act* atribui competências específicas ao regulador britânico. O código de desenho está ligado à legislação de proteção de dados do Reino Unido. O Comentário Geral nº 25 não possui a mesma força de lei nacional. O uso acadêmico responsável deve explicitar essas diferenças e evitar citação comparada como argumento de autoridade isolado.

A compatibilidade com o direito brasileiro deve ser testada por três filtros. O primeiro é normativo: existe base na Constituição, no ECA, na LGPD, no CDC, no Marco Civil ou no ECA Digital? O segundo é institucional: qual autoridade pode exigir ou fiscalizar a medida? O terceiro é proporcional: a obrigação é adequada ao risco e à capacidade do serviço? Somente depois desses filtros o parâmetro estrangeiro pode orientar interpretação ou decisão.

Um caso hipotético ilustra a aplicação. Uma plataforma de vídeos usada por adolescentes recomenda sequências de conteúdo autolesivo. O DSA sugere avaliação de risco sistêmico; o código britânico recomenda desenho apropriado à idade; o *Online Safety Act* destaca dever de segurança; o Comentário Geral nº 25 exige proteção do desenvolvimento. No Brasil, a decisão deve ser fundamentada no art. 227, da Constituição Federal, no ECA, no ECA Digital e nos deveres de segurança, usando a comparação para demonstrar viabilidade técnica das medidas.

Outro cenário envolve aplicativo de mensagens com criptografia e risco de aliciamento. A proteção comparada não autoriza quebrar indiscriminadamente o sigilo. Pode, porém, orientar medidas de segurança de conta, bloqueio facilitado, alertas de contato desconhecido, controle parental voluntário e canais de denúncia. A proporcionalidade impede que segurança da criança seja invocada para eliminar direitos de todos os usuários.

A comparação também contribui para a prova. Relatórios de avaliação de risco, auditorias, registros de design e indicadores de moderação podem demonstrar diligência ou revelar falhas. Quando a plataforma afirma ter adotado proteção por

padrão, deve apresentar documentação compatível. O julgador não precisa conhecer o código do algoritmo, mas pode exigir explicação funcional sobre objetivos, sinais considerados, testes e medidas de mitigação.

A comparação entre os modelos examinados indica que os parâmetros comparados confirmam que deveres proativos são tecnicamente possíveis e juridicamente controláveis. Eles não substituem as fontes brasileiras nem autorizam transposição automática. Sua função é ampliar o repertório interpretativo, oferecer exemplos de governança e mostrar que proteção infantojuvenil pode ser incorporada à arquitetura do serviço. A responsabilidade civil permanece dependente do direito nacional, do dever violado, do dano e do nexo causal.

Confirmam-se, assim, as três funções anunciadas na introdução para o recurso ao direito comparado. Em sua função interpretativa, os parâmetros estrangeiros esclarecem o sentido de categorias que o ECA Digital deles recebeu, como o desenho apropriado à idade e o critério de acesso provável. Em sua função de concretização, fornecem repertório para traduzir deveres proativos abertos em rotinas verificáveis. E em sua função dogmática, ao evidenciar que plataformas transnacionais já operam tais medidas, reforçam a previsibilidade do risco e a exigibilidade do dever – precisamente os elementos que sustentam a responsabilidade objetiva por violação de deveres proativos defendida nesta dissertação.

A comparação entre os modelos estrangeiros revela formas distintas de fiscalização. Na União Europeia, o DSA combina supervisão pública, relatórios e sanções; no Reino Unido, a segurança *online* é acompanhada por autoridade especializada; e o código de desenho apropriado à idade deriva da regulação de dados. No Brasil, a implementação já está em curso sob coordenação da Agência Nacional de Proteção de Dados, em articulação com órgãos de defesa da criança, Ministério Público, Judiciário e entidades de consumo. Essa multiplicidade institucional exige protocolos claros para evitar lacunas, sobreposição de ordens e duplicidade sancionatória (BRASIL, 2026a; BRASIL, 2026b).

A efetividade dos parâmetros comparados deve ser avaliada por resultados, não apenas por existência formal de políticas. Relatórios podem indicar tempo de resposta, reincidência, alcance de conteúdos e uso de recursos. Indicadores precisam ser interpretados com contexto, pois redução de denúncias pode refletir melhoria ou dificuldade de acesso ao canal. Auditorias independentes ajudam a validar informações sem expor segredos desnecessários.

A participação de crianças e adolescentes na elaboração de medidas é recomendável. Pesquisas, testes de usabilidade e consultas podem revelar riscos ignorados por adultos. Essa participação deve ser segura, informada e adequada à idade, sem transformar menores em responsáveis pela solução. O melhor interesse ganha concretude quando experiências reais influenciam desenho e avaliação.

Por fim, a experiência comparada confirma que a proteção digital não é estado definitivo. Tecnologias, práticas comerciais e formas de abuso mudam rapidamente. Deveres precisam ser revisados, mas a revisão deve ocorrer dentro de bases legais e com transparência. A adaptabilidade não autoriza decisões arbitrárias; exige processos de governança capazes de aprender com incidentes e justificar mudanças.

6 CONCLUSÃO

A questão que orientou a pesquisa foi apurar em que medida os deveres proativos estabelecidos ou reforçados pelo ECA Digital permitem sustentar a responsabilidade civil objetiva das plataformas por danos sofridos por crianças e adolescentes. A resposta é afirmativa, mas depende de condições verificáveis. A imputação objetiva pode ocorrer quando a plataforma organiza atividade de risco, está submetida a dever concreto de prevenção ou resposta, descumpre esse dever e contribui causalmente para dano juridicamente relevante. A condição de pessoa em desenvolvimento eleva o padrão de cuidado; não elimina, contudo, os requisitos da responsabilidade.

A análise exigiu afastar duas simplificações. De um lado, a plataforma não pode ser descrita como espaço neutro em todas as situações, pois define arquitetura, visibilidade, recomendação, publicidade, tratamento de dados e canais de denúncia. De outro, não se torna garantidora universal de qualquer comportamento praticado por usuários. A qualificação depende da função efetivamente exercida no evento: hospedar, recomendar, impulsionar, comercializar distribuição ou responder a um risco já identificado são condutas juridicamente distintas.

O ECA Digital atua como especialização protetiva dentro de um sistema normativo mais amplo. Sua incidência deve ser coordenada com o art. 227 da Constituição, o Estatuto da Criança e do Adolescente, o Código Civil, o Código de Defesa do Consumidor, a LGPD e o Marco Civil da Internet. Essa coordenação preserva a coerência do sistema: a lei especial não revoga integralmente os regimes anteriores, mas também não pode ser neutralizada por uma aplicação abstrata das normas gerais.

A proteção integral mostrou-se, simultaneamente, fundamento constitucional e critério de interpretação. Ela impõe consideração prioritária do melhor interesse, da evolução das capacidades e da vulnerabilidade inerente ao desenvolvimento. No ambiente digital, essa vulnerabilidade é intensificada pela opacidade dos sistemas de recomendação, pela exploração econômica da atenção e pela persistência dos registros. A consequência não é excluir menores da vida *online*, mas compatibilizar participação, autonomia progressiva e segurança.

Os riscos examinados não decorrem apenas do conteúdo publicado por terceiros. Interfaces persuasivas, configurações públicas por padrão, publicidade

pouco identificável, perfilamento, recomendação reiterada e canais de denúncia inacessíveis podem produzir ou ampliar danos. Por isso, a avaliação jurídica deve percorrer o ciclo do serviço, ingresso do usuário, coleta de dados, distribuição de conteúdo, detecção do risco, resposta e preservação de evidências e localizar a etapa que estava sob controle do fornecedor.

O modelo econômico exerce função probatória e normativa, sem gerar responsabilidade automática. A monetização da atenção pode revelar previsibilidade e capacidade de intervenção, sobretudo quando a empresa reconhece a presença de menores e utiliza dados para personalizar experiências. Anúncios e impulsionamentos pagos justificam escrutínio mais rigoroso porque envolvem participação comercial na distribuição. Ainda assim, a condenação depende de ilicitude, contribuição causal e ausência de diligência suficiente.

O dever geral de cuidado foi tratado como conjunto de obrigações concretas, e não como cláusula retórica. Avaliação de risco, proteção por desenho, privacidade por padrão, informação adequada, moderação proporcional, resposta tempestiva, controle de publicidade e documentação podem integrar esse conjunto. A intensidade do dever varia conforme a natureza do serviço, o público previsível, a escala e a gravidade do risco, o que impede a transposição automática das exigências dirigidas a redes globais para aplicações de pequena dimensão.

A aferição de idade evidencia a necessidade de proporcionalidade. A autodeclaração isolada pode ser facilmente contornada, mas mecanismos invasivos de identificação também criam riscos à privacidade e à inclusão. A solução deve combinar gravidade do conteúdo, precisão necessária, minimização de dados e alternativas menos restritivas. A falha ganha relevância civil quando a plataforma conhece a presença provável de menores e deixa de adotar medida compatível com o risco do serviço.

No plano civil-constitucional, a teoria do risco oferece fundamento para a responsabilidade objetiva apenas quando o risco é específico da atividade organizada. Não basta afirmar que a *internet* é perigosa. É necessário demonstrar de que modo recomendação, publicidade, tratamento de dados ou falha de resposta alteraram a probabilidade ou a extensão da lesão. A objetivação afasta a investigação da culpa psicológica, mas preserva dever, dano, nexo e excludentes.

A função social da responsabilidade civil manifesta-se nas dimensões reparatória e preventiva. A indenização permanece indispensável quando o dano já

se consumou, mas não responde, sozinha, à velocidade e à replicabilidade dos ambientes digitais. Tutelas inibitórias, obrigações de fazer, preservação de registros e medidas estruturais podem interromper ou evitar a repetição da lesão. A providência escolhida, porém, deve ser executável e proporcional, sem converter o processo em administração permanente da plataforma.

A hipervulnerabilidade digital repercute diretamente sobre a prova. Crianças, adolescentes e famílias raramente têm acesso a métricas de recomendação, histórico de moderação ou registros publicitários, enquanto a plataforma concentra os dados capazes de explicar a cadeia causal. A distribuição dinâmica do ônus e as presunções relativas podem reduzir essa assimetria, desde que a parte autora apresente indícios concretos e que o fornecedor possa demonstrar diligência ou causa externa.

A causalidade digital é, em regra, multifatorial. O dano pode envolver o autor do conteúdo, usuários que o replicam, mecanismos de recomendação, anúncios, demora de resposta e vulnerabilidades pessoais. O direito não precisa eleger uma causa única, mas deve individualizar contribuições juridicamente relevantes. A presunção de causalidade somente se justifica quando a prova decisiva está sob controle do réu e os fatos apontam conexão plausível entre a falha e o resultado.

A revisão do Marco Civil pelo Supremo Tribunal Federal alterou o ponto de partida jurisprudencial. O julgamento conjunto concluído em 2025 reconheceu a inconstitucionalidade parcial e progressiva do art. 19 e definiu parâmetros distintos segundo a natureza do conteúdo, a ciência do provedor, o ato próprio e a falha sistêmica. Em junho de 2026, os embargos aperfeiçoaram a tese e fixaram prazo de 60 dias para implementação das medidas estruturais. O resultado consolida um regime mais complexo, sem transformar toda controvérsia em hipótese de remoção extrajudicial automática (BRASIL, 2025b; BRASIL, 2025c; BRASIL, 2026c).

No regime resultante dos Temas 987 e 533, anúncios, impulsionamentos pagos e redes artificiais recebem tratamento mais rigoroso por revelarem participação econômica ou técnica na amplificação. A presunção de responsabilidade continua relativa e pode ser afastada mediante prova de diligência e resposta tempestiva. Em danos contra menores, a disciplina reforça controles sobre segmentação, aprovação publicitária e circulação coordenada, sem dispensar a demonstração da ilicitude, do dano e da contribuição causal.

A causa de pedir define o alcance da especialidade. Se a controvérsia envolve apenas conteúdo de terceiro e ausência de remoção, o regime constitucional do Marco

Civil desempenha papel central. Se envolve desenho inseguro, recomendação, publicidade, dados ou descumprimento de dever proativo, a análise recai sobre comportamento próprio da plataforma. Essa distinção impede que a lei especial seja utilizada como atalho para qualquer condenação.

As excludentes permanecem compatíveis com o modelo proposto. Culpa exclusiva da vítima, fato exclusivo de terceiro, força maior e inevitabilidade técnica podem romper o nexo quando efetivamente demonstrados. Nos casos envolvendo crianças, a culpa exclusiva exige cautela adicional, consideradas a idade, a capacidade de compreensão e a influência do design. A participação do usuário não exclui a responsabilidade quando a arquitetura contribuiu de forma relevante para o dano.

Os danos digitais podem assumir dimensão individual, coletiva ou relacionada ao desenvolvimento biopsicossocial. Exposição de imagem, violação de privacidade e assédio atingem direitos pessoais; práticas sistemáticas de publicidade ou perfilamento podem lesar grupos; recomendações nocivas podem repercutir sobre saúde e desenvolvimento. A reparação deve corresponder à natureza da lesão e evitar duplicidade, enquanto a tutela coletiva se mostra particularmente adequada quando a falha decorre de política geral do serviço.

Os parâmetros comparados confirmam a viabilidade de técnicas como proteção por desenho, avaliação de risco e transparência, mas não foram tratados como direito diretamente aplicável. *Age Appropriate Design Code, DSA, Online Safety Act* e Comentário Geral nº 25 fornecem experiências úteis para concretizar deveres brasileiros. Sua utilização depende, em cada caso, de compatibilidade normativa, competência institucional e proporcionalidade.

Como síntese, propõe-se uma matriz decisória em seis etapas. Primeiro, identificam-se conjuntamente o serviço e o sujeito: de um lado, o tipo de serviço e a presença provável de crianças e adolescentes; de outro, a condição concreta desse sujeito – faixa etária, estágio de desenvolvimento e capacidades em evolução, vulnerabilidades agravadas verificáveis e melhor interesse aplicável ao caso –, que gradua a intensidade do dever exigível nas etapas seguintes e delimita a tutela adequada na etapa final. Em seguida, define-se a conduta relevante – hospedagem, recomendação, publicidade, tratamento de dados ou resposta institucional – e determina-se o dever aplicável. Depois, verificam-se o descumprimento e sua contribuição causal; examinam-se o dano, as excludentes e a prova disponível; e, por

fim, escolhe-se tutela proporcional ao risco e à lesão. A sequência torna a imputação controlável e reduz decisões fundadas apenas na gravidade abstrata do caso.

Convém explicitar o sentido da primeira etapa. Ela é deliberadamente bifocal porque a matriz, sendo instrumento de imputação, precisa examinar a conduta da plataforma sem por isso reduzir a criança a variável do cálculo de risco alheio. O serviço define o campo de deveres possíveis; o sujeito, em sua condição concreta, define a intensidade com que esses deveres são exigíveis e o modo como a tutela deve ser desenhada. A criança não é, portanto, apenas pressuposto de incidência e portadora de dano: é critério de graduação que atravessa as demais etapas e impede que a proteção integral seja convertida em simples auditoria de conformidade técnica.

Do ponto de vista empresarial, a proteção precisa ser demonstrável. Responsáveis internos, avaliações periódicas, registro de denúncias, critérios de escalonamento, controles de publicidade, testes de recomendação e comunicação adequada às famílias integram uma governança minimamente verificável. A documentação não atende apenas ao interesse defensivo da empresa; permite auditoria, aprendizagem institucional e prevenção. Em atividades de alto risco, a ausência injustificada de registros pode constituir indício relevante.

Para o Poder Judiciário, o desafio central está em formular ordens executáveis. A decisão deve indicar o conteúdo ou a funcionalidade atingida, o público, o prazo e a providência esperada. Comandos genéricos de eliminação de todo risco tendem a ser inexequíveis ou desproporcionais; por outro lado, a retirada de um único endereço pode ser insuficiente diante de redes de contas, mecanismos de recomendação ou políticas publicitárias. A tutela deve corresponder à arquitetura concreta do dano.

No plano administrativo, parte relevante da regulamentação já foi estabelecida pelo Decreto nº 12.880/2026, enquanto a Agência Nacional de Proteção de Dados conduz orientações e atos complementares sobre temas como aferição etária, transparência e fiscalização. Esses parâmetros podem reduzir incertezas e esclarecer o conteúdo objetivo dos deveres. A atuação administrativa não substitui a responsabilidade civil, mas contribui para prevenir litígios e avaliar a diligência quando segurança e tratamento de dados se sobrepõem (BRASIL, 2026a; BRASIL, 2026b).

A hipótese central foi confirmada sob condições. Os deveres proativos do ECA Digital podem fundamentar responsabilidade civil objetiva quando se vinculam ao risco da atividade e a falha própria da plataforma. Não é necessário provar intenção ou negligência psicológica, mas permanece indispensável demonstrar o descumprimento

de uma obrigação objetiva e sua contribuição para o dano. A proteção prioritária torna o padrão mais exigente; não dissolve os limites dogmáticos.

As hipóteses secundárias também se confirmaram, e igualmente sob condições. Quanto à primeira, o exame do Marco Civil da Internet e dos Temas 987 e 533 demonstrou que o art. 19 conserva função relevante nas pretensões fundadas exclusivamente em conteúdo de terceiro, mas não esgota as situações de dano digital infantojuvenil: quando a lesão decorre de arquitetura, recomendação, publicidade, tratamento de dados ou falha de resposta, o regime especial do ECA Digital incide em diálogo com o regime geral, sem revogá-lo. Quanto à segunda, verificou-se que a hipervulnerabilidade repercute diretamente sobre a prova: a distribuição dinâmica do ônus, a exibição de documentos e a presunção relativa de causalidade mostraram-se instrumentos adequados de reequilíbrio, desde que ancorados em indícios concretos de falha, sob pena de se converterem em presunção abstrata de responsabilidade. A condicionalidade de ambas as confirmações é o que preserva a coerência do modelo: sem a primeira, a imputação careceria de fronteira normativa; sem a segunda, teria fronteira, mas não teria realização prática.

O modelo resultante combina prevenção, reparação e controle. Ele recusa tanto a neutralidade absoluta das plataformas quanto sua responsabilização universal. Ao exigir a identificação do dever, do risco, da falha, do dano e do nexo, permite proteger crianças e adolescentes sem sacrificar liberdade de expressão, inovação e segurança jurídica. A distribuição de responsabilidades acompanha, assim, a capacidade de prevenção e a contribuição de cada agente para o risco.

A aplicação da matriz dependerá do amadurecimento jurisprudencial e da implementação regulatória já iniciada. Casos concretos ainda precisarão definir o alcance de expressões como acesso provável, a proporcionalidade dos mecanismos de aferição etária e os meios adequados de demonstrar diligência. A pesquisa não encerra essas questões; oferece critérios para reduzir arbitrariedade e tornar comparáveis decisões proferidas em contextos tecnológicos distintos.

A proteção infantojuvenil requer cooperação sem diluição de responsabilidades. Família, escola, Estado e empresas desempenham funções distintas e não respondem de modo uniforme. A plataforma responde pela arquitetura e pela governança do serviço; responsáveis orientam e acompanham; o Estado regula, fiscaliza e assegura tutela; e a sociedade participa da formação de uma cultura digital compatível com os direitos de crianças e adolescentes.

Pesquisas posteriores poderão examinar empiricamente a efetividade das medidas, as diferenças entre faixas etárias e os impactos sobre grupos em maior vulnerabilidade. Também será necessário acompanhar os atos regulatórios complementares da ANPD e a evolução jurisprudencial dos Temas 987 e 533. Estudos interdisciplinares sobre saúde mental, *design* e comportamento podem enriquecer a análise, desde que não substituam a identificação jurídica do dever e da causalidade.

A principal contribuição da dissertação é demonstrar que proteção prioritária e limites de responsabilidade não são incompatíveis. Critérios rigorosos fortalecem a tutela ao permitir o reconhecimento de falhas relevantes e o afastamento de imputações indevidas. A responsabilidade objetiva aqui defendida procura esse equilíbrio: exige diligência proporcional ao poder exercido pelas plataformas e preserva segurança jurídica ao condicionar a reparação a elementos demonstráveis.

Resta indagar, por fim, se o ECA Digital é suficiente para tutelar os interesses de crianças e adolescentes ou se ainda falta algo para completá-lo. Em sua arquitetura normativa, a lei representa avanço expressivo: substitui a lógica meramente reativa por deveres proativos de prevenção, segurança e transparência, incorpora a proteção desde a concepção e articula-se de modo coerente com a Constituição, o Estatuto da Criança e do Adolescente, o Código Civil, o Código de Defesa do Consumidor, a LGPD e o Marco Civil da Internet. Nesse plano, o diploma oferece base sólida e, em larga medida, adequada para responsabilizar plataformas por falhas próprias.

A suficiência, contudo, não se mede apenas pela qualidade do texto legal. Uma lei protetiva bem concebida não protege por si só: sua eficácia depende de implementação regulatória, de capacidade fiscalizatória e de amadurecimento jurisprudencial capaz de converter princípios abstratos em deveres verificáveis. Enquanto esses fatores não se consolidarem, o potencial protetivo permanecerá, em parte, promessa normativa.

Persistem, ademais, lacunas e tensões que a legislação, isoladamente, não resolve. No plano técnico-normativo, ainda faltam parâmetros claros que conciliem a aferição de idade com a minimização de dados exigida pela LGPD, evitando que a proteção de um direito fundamental se faça à custa de outro. No plano processual, a assimetria probatória entre famílias e plataformas reclama a consolidação de instrumentos como a distribuição dinâmica do ônus da prova e o acesso a registros internos, sob pena de o direito material não encontrar realização prática. No plano

institucional, a efetividade dependerá de recursos e expertise da autoridade administrativa e de mecanismos aptos a alcançar fornecedores sediados no exterior.

Por fim, nenhuma norma substitui a educação digital, a mediação familiar e a atuação da escola, dimensões que escapam ao alcance da responsabilidade civil. A resposta, portanto, é matizada: o ECA Digital é condição necessária e bem construída, mas não autossuficiente. Sua adequação plena dependerá menos de novas leis do que da implementação séria dos deveres que já instituiu e da articulação com medidas educativas, regulatórias e processuais que lhe deem concretude.

Essa constatação reforça, no plano conclusivo, o que se sustentou ao longo do trabalho: o ECA Digital inova pouco quanto ao regime de imputação e muito quanto aos seus pressupostos. Ao converter em deveres típicos aquilo que antes se extraía de cláusulas gerais, ele torna o risco normativamente previsível, a falha verificável e a decisão controlável. A responsabilidade civil que daí resulta não é nova em espécie, mas é substancialmente mais exigível do que aquela que o sistema anterior permitia mobilizar.

O ECA Digital inaugura uma etapa de maior densidade jurídica na proteção de crianças e adolescentes em ambientes digitais. Seu potencial dependerá de interpretação capaz de converter princípios em deveres concretos, sem prometer risco zero. Quando a plataforma conhece o público, controla mecanismos relevantes e deixa de adotar medidas proporcionais, a responsabilidade civil pode cumprir funções preventiva, reparatória e social. Quando demonstra diligência compatível e o dano resulta de causa externa inevitável, as excludentes preservam a justiça da imputação.

REFERÊNCIAS

ALMEIDA, Juliana Evangelista de; PENAFORTE, Gabriella Mundim. Marco Civil da Internet (Lei n. 12.965/14) e os desafios contemporâneos à responsabilidade civil dos provedores na era das *fake news*. **Revista de Ciências do Estado**, Belo Horizonte, 2025. Disponível em: https://periodicos.ufmg.br/index.php/revice/article/view/e54425/e54425. Acesso em: 23 jun. 2026.

AZEVEDO, Fernando Costa de; TORRES, Julia Fátima Gonçalves. A hipervulnerabilidade digital situacional de crianças, adolescentes e do núcleo familiar no jogo eletrônico Fortnite. **Civilistica.com**, Rio de Janeiro, a. 12, n. 3, p. 1-26, 2023. Disponível em: https://civilistica.emnuvens.com.br/redc/article/download/927/1082. Acesso em: 05 jul. 2026.

BALKIN, Jack M. Free speech in the algorithmic society: big data, private governance, and new school speech regulation. **U.C. Davis Law Review**, Davis, v. 51, p. 1149-1210, 2018. Disponível em: https://lawreview.law.ucdavis.edu/issues/51/3/Essays/51-3_Balkin.pdf. Acesso em: 28 jun. 2026.

BENJAMIN, Antonio Herman V.; MARQUES, Claudia Lima; BESSA, Leonardo Roscoe. **Manual de direito do consumidor**. 10. ed. São Paulo: Revista dos Tribunais, 2022.

BIBLIOTECAS ALFA EDUCAÇÃO. **Manual de normalização para apresentação de trabalhos acadêmicos conforme a ABNT**. São Paulo: Alfa Educação UNIALFA/FADISP, 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. **Enunciado CD/ANPD nº 1, de 22 de maio de 2023**. Dispõe sobre tratamento de dados pessoais de crianças e adolescentes. Brasília, DF: ANPD, 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/enunciado-cd/anpd-n-1-de-22-de-maio-de-2023-485306934. Acesso em: 10 jul. 2026.

BRASIL. Autoridade Nacional de Proteção de Dados. **Estudo preliminar**: hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes. Brasília, DF: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf. Acesso em: 22 jun. 2026.

BRASIL. Conselho Nacional dos Direitos da Criança e do Adolescente. **Resolução nº 163, de 13 de março de 2014**. Dispõe sobre a abusividade do direcionamento de publicidade e de comunicação mercadológica à criança e ao adolescente. Brasília, DF: CONANDA, 2014b. Disponível em: https://www.gov.br/mdh/pt-br/acesso-a-informacao/participacao-social/conselho-nacional-dos-direitos-da-crianca-e-do-adolescente-conanda/resolucoes/resolucao-163-_publicidade-infantil.pdf. Acesso em: 02 jul. 2026.

BRASIL. Conselho Nacional dos Direitos da Criança e do Adolescente. **Resolução nº 245, de 5 de abril de 2024**. Dispõe sobre os direitos das crianças e adolescentes em ambiente digital. Brasília, DF: CONANDA, 2024. Disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/48630. Acesso em: 29 jun. 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: 08 jul. 2026.

BRASIL. **Decreto nº 12.622, de 17 de setembro de 2025**. Regulamenta a Lei nº 15.211, de 17 de setembro de 2025, para designar a Agência Nacional de Proteção de Dados como autoridade administrativa autônoma de proteção de crianças e adolescentes em ambientes digitais. Brasília, DF: Presidência da República, 2025d. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12622.htm. Acesso em: 20 jun. 2026.

BRASIL. **Decreto nº 12.880, de 18 de março de 2026**. Regulamenta a Lei nº 15.211, de 17 de setembro de 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, 2026a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12880.htm. Acesso em: 07 jul. 2026.

BRASIL. **Decreto nº 99.710, de 21 de novembro de 1990**. Promulga a Convenção sobre os Direitos da Criança. Brasília, DF: Presidência da República, 1990c. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d99710.htm. Acesso em: 01 jul. 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/l10406compilada.htm. Acesso em: 26 jun. 2026.

BRASIL. **Lei nº 10.741, de 1º de outubro de 2003**. Dispõe sobre o Estatuto da Pessoa Idosa e dá outras providências. Brasília, DF: Presidência da República, 2003. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2003/l10.741.htm. Acesso em: 17 jul. 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, 2014a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 24 jun. 2026.

BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. Brasília, DF: Presidência da República, 2015a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 11 jul. 2026.

BRASIL. **Lei nº 13.146, de 6 de julho de 2015**. Institui a Lei Brasileira de Inclusão da Pessoa com Deficiência (Estatuto da Pessoa com Deficiência). Brasília, DF:

Presidência da República, 2015b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13146.htm. Acesso em: 17 jul. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 06 jul. 2026.

BRASIL. **Lei nº 15.211, de 17 de setembro de 2025**. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais. Brasília, DF: Presidência da República, 2025a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm. Acesso em: 04 jul. 2026.

BRASIL. **Lei nº 15.352, de 25 de fevereiro de 2026**. Transforma cargos no âmbito do Poder Executivo federal; altera a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), para dispor sobre a Agência Nacional de Proteção de Dados (ANPD), a Lei nº 10.871, de 20 de maio de 2004, para criar a Carreira de Regulação e Fiscalização de Proteção de Dados, a Lei nº 15.211, de 17 de setembro de 2025 (Estatuto Digital da Criança e do Adolescente), para dispor sobre o início da vigência da referida Lei; altera as Leis nºs 9.008, de 21 de março de 1995, 11.890, de 24 de dezembro de 2008, 13.326, de 29 de julho de 2016, 13.848, de 25 de junho de 2019, e 14.600, de 19 de junho de 2023; revoga a Medida Provisória nº 1.319, de 17 de setembro de 2025; e dá outras providências. Brasília, DF: Presidência da República, 2026b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/L15352.htm. Acesso em: 25 jun. 2026.

BRASIL. **Lei nº 7.347, de 24 de julho de 1985**. Disciplina a ação civil pública de responsabilidade por danos causados ao meio ambiente, ao consumidor e a outros interesses difusos e coletivos. Brasília, DF: Presidência da República, 1985. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm. Acesso em: 09 jul. 2026.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, 1990a. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 21 jun. 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/l8078compilado.htm. Acesso em: 27 jun. 2026.

BRASIL. Ministério da Justiça e Segurança Pública. **Relatório do Comitê de Denúncia**: crimes digitais contra crianças e adolescentes. Brasília, DF: MJSP, 2025e. Disponível em: https://www.gov.br/mj/pt-br/assuntos/arquivos-imprensa/sedigi/relatorio_comite_denuncia.pdf. Acesso em: 30 jun. 2026.

BRASIL. Secretaria de Comunicação Social da Presidência da República. **Crianças, adolescentes e telas**: guia sobre usos de dispositivos digitais. Brasília, DF:

SECOM, 2025f. Disponível em: https://www.gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia/guia-de-telas_sobre-usos-de-dispositivos-digitais_versaoweb.pdf. Acesso em: 03 jul. 2026.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.152.541/RS**. Relator: Ministro Paulo de Tarso Sanseverino. Brasília, DF: STJ, 2011. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200901570760&dt_publicacao=21/09/2011. Acesso em: 21 ago. 2026.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.783.269/MG**. Relator: Ministro Antonio Carlos Ferreira. Brasília, DF: STJ, 2021. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?dt=20220218&formato=PDF&nreg=201702627555&seq=2128573&tipo=0. Acesso em: 10 jul. 2026.

BRASIL. Supremo Tribunal Federal. **Tema 533 da repercussão geral: RE 1.057.258/MG**. Brasília, DF: STF, 2025c. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?classeProcesso=RE&incidente=5217273&numeroProcesso=1057258&numeroTema=533. Acesso em: 20 jun. 2026.

BRASIL. Supremo Tribunal Federal. **Tema 987 da repercussão geral: RE 1.037.396/SP**. Brasília, DF: STF, 2025b. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/tema.asp?num=987. Acesso em: 08 jul. 2026.

BRASIL. Supremo Tribunal Federal. **Plataformas terão 60 dias para implementar medidas estruturais, decide STF**. Brasília, DF: STF, 17 jun. 2026c. Disponível em: https://noticias.stf.jus.br/postsnoticias/plataformas-terao-60-dias-para-implementar-medidas-estruturais-decide-stf/. Acesso em: 05 jul. 2026.

CASTRO, Carla Frade de Paula. Responsabilidade civil de provedores de aplicações de internet por infrações de terceiros a direitos autorais. **Revista de Informação Legislativa**, Brasília, DF, a. 60, n. 237, p. 141-171, jan./mar. 2023. Disponível em: https://www12.senado.leg.br/ril/edicoes/60/237/ril_v60_n237_p141.pdf. Acesso em: 29 jun. 2026.

CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 16. ed. Barueri: Atlas, 2024.

COHEN, Julie E. **Between truth and power**: the legal constructions of informational capitalism. Oxford: Oxford University Press, 2019.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil**: TIC Kids Online Brasil 2024. São Paulo: CGI.br, 2025. Disponível em: https://cetic.br/media/docs/publicacoes/2/20250512154312/tic_kids_online_2024_livro_eletronico.pdf. Acesso em: 11 jul. 2026.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil**: TIC Kids Online Brasil 2025. São Paulo: CGI.br, 2026. Disponível em: https://cetic.br/media/docs/publicacoes/2/pt-

br/20260317181039/tic_kids_online_2025_livro_eletronico.pdf.pdf. Acesso em: 03 jul. 2026.

CONSELHO DA JUSTIÇA FEDERAL. **Jornadas de direito civil I, III, IV e V**: enunciados aprovados. Coordenador científico Ministro Ruy Rosado de Aguiar Júnior. Brasília, DF: CJF, 2012.

COUTO E SILVA, Clóvis V. do. **A obrigação como processo**. Rio de Janeiro: FGV, 2006.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

EUROPEAN COMMISSION. **Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065**. Brussels: European Commission, 2025. Disponível em: https://eur-lex.europa.eu/eli/C/2025/5519/oj/eng. Acesso em: 25 jun. 2026.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson; BRAGA NETTO, Felipe Peixoto. **Novo tratado de responsabilidade civil**. 4. ed. São Paulo: Atlas, 2023.

FERNANDES, Elora; TEFFÉ, Chiara de; BRANCO, Sérgio (coord.). **Privacidade e proteção de dados de crianças e adolescentes**. 2. ed. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2024. Disponível em: https://itsrio.org/wp-content/uploads/2016/12/Livro-Privacidade-Protecao_REV-ITS_converted.pdf. Acesso em: 06 jul. 2026.

FERNANDES, Márcia Santana. O Estatuto Digital da Criança e do Adolescente, Lei 15.211/2025: contraste com o Livro de Direito Civil Digital do PL 04/2025. In: MARTINS-COSTA, Judith; MARTINS, Fábio; CRAVEIRO, Mariana Conti; XAVIER, Rafael Branco (org.). **Boletim IDiP-IEC**, [S. l.], v. LXXIX, 14 jan. 2026. Disponível em: https://canalarbitragem.com.br/boletim-idip-iec/vol-4-no-1-jan-2026-o-estatuto-digital-da-crianca-e-do-adolescente-lei-5-211-2025-contraste-com-o-livro-de-direito-civil-digital-do-pl04-2025/. Acesso em: 17 jul. 2026.

FRAZÃO, Ana. **Dever geral de cuidado das plataformas diante de crianças e adolescentes**. São Paulo: Instituto Alana; Criança e Consumo, 2021. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2021/11/dever-geral-de-cuidado-das-plataformas.pdf. Acesso em: 27 jun. 2026.

FRAZÃO, Ana. **Responsabilidade civil de provedores de aplicações por conteúdos de terceiros**: o art. 19 do Marco Civil não é nem pode ser a única referência normativa para o assunto. Brasília, DF: Ana Frazão, 2022. Disponível em: https://www.professoraanafrazao.com.br/files/publicacoes/2022-02-24-Responsabilidade_civil_de_provedores_de_aplicacoes_por_conteudos_de_terceiros_O_art_19_do_Marco_Civil_nao_e_nem_pode_ser_a_unica_referencia_normativa_para_o_assunto.pdf. Acesso em: 02 jul. 2026.

FUNDAÇÃO GETULIO VARGAS. **Cartilha explicativa**: ECA Digital: Lei nº 15.211/2025. Rio de Janeiro: FGV Direito Rio, 2025. Disponível em: https://direitorio.fgv.br/publicacao/eca-digital-lei-no-152112025. Acesso em: 28 jun. 2026.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 7. ed. Barueri: Atlas, 2022.

GILLESPIE, Tarleton. **Custodians of the internet**: platforms, content moderation, and the hidden decisions that shape social media. New Haven: Yale University Press, 2018.

GONÇALVES, Ana Paula; LARA, Célia Regina; SILVA, Rafael Fernandes da. A proteção de crianças e adolescentes no ambiente digital: Lei nº 15.211/2025. **Contribuciones a las Ciencias Sociales**, [S. l.], v. 19, n. 3, p. e23994, 2026. DOI: 10.55905/revconv.19n.3-057. Disponível em: https://ojs.revistacontribuciones.com/ojs/index.php/clcs/article/view/23994. Acesso em: 17 jul. 2026.

GUSTIN, Miracy Barbosa de Sousa; DIAS, Maria Tereza Fonseca; NICÁCIO, Camila Silva. **(Re)pensando a pesquisa jurídica**: teoria e prática. 5. ed. São Paulo: Almedina, 2020.

HIRONAKA, Giselda Maria Fernandes Novaes. **Responsabilidade pressuposta**. Belo Horizonte: Del Rey, 2005.

INFORMATION COMMISSIONER'S OFFICE (ICO). **Age appropriate design**: a code of practice for online services. Wilmslow: ICO, 2022. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/. Acesso em: 23 jun. 2026.

INSTITUTO ALANA. **Como o ECA Digital virou o jogo da proteção online de crianças e adolescentes**. São Paulo: Instituto Alana, 2026. Disponível em: https://alana.org.br/wp-content/uploads/2026/03/eca-digital-protecao-online-criancas-adolescentes-livro-digital.pdf. Acesso em: 09 jul. 2026.

ISHIDA, Válter Kenji. **Estatuto da Criança e do Adolescente**: doutrina e jurisprudência. 24. ed. São Paulo: Juspodivm, 2024.

LIVINGSTONE, Sonia; STOILOVA, Mariya; HOPWOOD, Katie. **The 4Cs**: classifying online risk to children. Hamburg: Leibniz Institute for the Social Sciences, 2021. Disponível em: https://www.ssoar.info/ssoar/bitstream/handle/document/71817/ssoar-2021-livingstone_et_al-The_4Cs_Classifying_Online_Risk.pdf. Acesso em: 21 jun. 2026.

LOPES, Maria Clara Bomfim Braz Ferreira; NOVAIS, Thyara Gonçalves. Lei 15.211/2025 (ECA Digital) e a atuação jurídica com base ao Estatuto da Criança e do Adolescente. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S. l.], v. 12, n. 5, p. 1-18, 2026. DOI: 10.51891/rease.v12i5.27008. Disponível em: https://periodicorease.pro.br/rease/article/view/27008. Acesso em: 17 jul. 2026.

MACHADO, Martha de Toledo. **A proteção constitucional de crianças e adolescentes e os direitos humanos**. Barueri: Manole, 2003.

MACIEL, Kátia Regina Ferreira Lobo Andrade (coord.). **Curso de direito da criança e do adolescente**: aspectos teóricos e práticos. 16. ed. São Paulo: SaraivaJur, 2024a.

MACIEL, Rafael. (In)constitucionalidade do artigo 19 do Marco Civil da Internet à luz do constitucionalismo digital. **SSRN**, 2024b. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4955566. Acesso em: 20 jun. 2026.

MARQUES, Claudia Lima. **Diálogo das fontes**: do conflito à coordenação de normas do direito brasileiro. São Paulo: Revista dos Tribunais, 2012.

MARQUES, Claudia Lima; BENJAMIN, Antonio Herman V.; MIRAGEM, Bruno. **Comentários ao Código de Defesa do Consumidor**. 7. ed. São Paulo: Revista dos Tribunais, 2020.

MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2. ed. São Paulo: Saraiva Educação, 2018.

MEDEIROS, Juliana. **Responsabilidade civil dos provedores de aplicações de internet**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2020. Disponível em: https://itsrio.org/wp-content/uploads/2020/10/Responsabilidade-civil-dos-provedores-de-aplica%C3%A7%C3%B5es-de-internet_Juliana_Medeiros.pdf. Acesso em: 05 jul. 2026.

MELO, Lílian Manoela Monteiro Cintra de. Enduring issues of digital exclusion, emerging pressures of internet regulation in Brazil. **Suprema**: Revista de Estudos Constitucionais, Brasília, DF, v. 2, n. 1, p. 287-326, 2022. Disponível em: https://suprema.stf.jus.br/index.php/suprema/article/download/156/61. Acesso em: 01 jul. 2026.

MELO, Lílian Manoela Monteiro Cintra de. **Regulação da internet e desenvolvimento**: a disputa da neutralidade da rede. 2018. Tese (Doutorado em Direito) - Universidade de São Paulo, São Paulo, 2018. Disponível em: https://teses.usp.br/teses/disponiveis/2/2132/tde-13112020-005158/. Acesso em: 10 jul. 2026.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 120, p. 555-587, nov./dez. 2018.

MIRAGEM, Bruno. Novo paradigma tecnológico, mercado de consumo digital e o direito do consumidor. **Revista de Direito do Consumidor**, São Paulo, v. 125, set./out. 2019. Disponível em: https://brunomiragem.com.br/wp-content/uploads/2020/06/003-novo-paradigma-tecnologico-e-consumo.pdf. Acesso em: 26 jun. 2026.

MORAES, Maria Celina Bodin de. **Danos à pessoa humana**: uma leitura civil-constitucional dos danos morais. Rio de Janeiro: Renovar, 2003.

MULHOLLAND, Caitlin Sampaio. **A responsabilidade civil por presunção de causalidade**. Rio de Janeiro: GZ Editora, 2009.

NUCCI, Guilherme de Souza. **Estatuto da Criança e do Adolescente comentado**. 6. ed. Rio de Janeiro: Forense, 2024.

OECD. **Children in the digital environment**: revised typology of risks. Paris: OECD Publishing, 2021. Disponível em: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/01/children-in-the-digital-environment_9d454872/9b8f222e-en.pdf. Acesso em: 24 jun. 2026.

PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

PEREIRA, Fabio Queiroz; LARA, Mariana Alves. A responsabilidade civil dos provedores de aplicação por conteúdo envolvendo crianças e adolescentes: análise do REsp n. 1.783.269/MG. **Civilistica.com**, Rio de Janeiro, a. 11, n. 3, p. 1-14, 2022. Disponível em: https://civilistica.emnuvens.com.br/redc/article/download/832/678/1867. Acesso em: 11 jul. 2026.

ROSA, Conrado Paulino da; PIN, Luiza Rodrigues. A proteção de dados pessoais de crianças e adolescentes: um debate sobre o direito à privacidade a partir da obra 1984 de George Orwell. **Revista Brasileira de Direito Civil**, Belo Horizonte, v. 31, n. 4, p. 333-351, out./dez. 2022. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/download/862/582. Acesso em: 22 jun. 2026.

ROSENVALD, Nelson. **As funções da responsabilidade civil**: a reparação e a pena civil. 3. ed. São Paulo: Saraiva, 2017.

ROSSATO, Luciano Alves; LÉPORE, Paulo Eduardo; CUNHA, Rogério Sanches. **Estatuto da Criança e do Adolescente comentado**: artigo por artigo. 15. ed. São Paulo: SaraivaJur, 2024.

SAFERNET BRASIL. **Indicadores**: denúncias SaferNet 2025. São Paulo: SaferNet Brasil, 2025. Disponível em: https://arquivos.safernet.org.br/pdfs/INDICADORES-DenunciasSaferNet2025.pdf. Acesso em: 28 jun. 2026.

SARLET, Ingo Wolfgang; MENDES, Laura Schertel; DONEDA, Danilo; RODRIGUES JUNIOR, Otavio Luiz (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil**: da erosão dos filtros da reparação à diluição dos danos. 6. ed. São Paulo: Atlas, 2015.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco Civil da Internet**: construção e aplicação. Juiz de Fora: Editar, 2016. Disponível em: https://itsrio.org/wp-content/uploads/2017/02/marco_civil_construcao_aplicacao.pdf. Acesso em: 25 jun. 2026.

TEFFÉ, Chiara Spadaccini de. A responsabilidade civil do provedor de aplicações de internet pelos danos decorrentes do conteúdo gerado por terceiros, de acordo com o Marco Civil da Internet. **Revista Fórum de Direito Civil**, Belo Horizonte, 2015. Disponível em: https://editoraforum.com.br/wp-content/uploads/2015/12/A-responsabilidade-civil-do-provedor-de-aplicacoes-de-internet.pdf. Acesso em: 09 jul. 2026.

TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do direito civil**: responsabilidade civil. 5. ed. Rio de Janeiro: Forense, 2024. v. 4.

UNICEF. **Childhood in a digital world**. Florence: UNICEF Innocenti, 2025. Disponível em: https://www.unicef.org/innocenti/media/11296/file/UNICEF-Innocenti-Childhood-in-a-digital-world-report-2025.pdf. Acesso em: 27 jun. 2026.

UNICEF. **Growing up in a connected world**. Florence: UNICEF Office of Research - Innocenti, 2019. Disponível em: https://www.unicef.org/innocenti/media/7006/file/GKO-Summary-Report-2019.pdf. Acesso em: 20 jun. 2026.

UNITED KINGDOM. **Online Safety Act 2023**. London: The Stationery Office, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50/pdfs/ukpga_20230050_en.pdf. Acesso em: 02 jul. 2026.

UNITED NATIONS. Committee on the Rights of the Child. **General comment No. 25 (2021) on children's rights in relation to the digital environment**. Geneva: OHCHR, 2021. Disponível em: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation. Acesso em: 29 jun. 2026.

UNIÃO EUROPEIA. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). **Official Journal of the European Union**, Luxembourg, L 277, 27 out. 2022. Disponível em: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng. Acesso em: 01 jul. 2026.

ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. New York: PublicAffairs, 2019.