

REDES SOCIAIS E PROTEÇÃO INFANTOJUVENIL: ANÁLISE DA RESPONSABILIDADE CIVIL DOS PROVEDORES DE INTERNET

**SOCIAL NETWORKS AND CHILD AND ADOLESCENT PROTECTION: AN
ANALYSIS OF THE CIVIL LIABILITY OF INTERNET SERVICE PROVIDERS**

Ciências Humanas • 30/10/2026

REGISTRO DOI: [10.70773/revistatopicos/793243169](https://doi.org/10.70773/revistatopicos/793243169)

Jovane Pereira¹

Lidimar Andrade Carvalho²

Vilma de Fátima Diniz de Sousa³

RESUMO

O artigo analisa a responsabilidade civil das redes sociais e dos provedores de internet diante da divulgação de conteúdos ilícitos envolvendo crianças e adolescentes no Brasil. O objetivo é compreender como os deveres de prevenção, resposta e reparação se relacionam à circulação, ao reenvio e à indexação de materiais ilegais em ambientes digitais. A pesquisa apresenta abordagem qualitativa, de natureza bibliográfica e documental, fundamentada na análise da legislação brasileira, de decisões judiciais, de documentos institucionais e da literatura especializada sobre Direito Digital e proteção infantojuvenil. A análise considera o Estatuto da Criança e do Adolescente, o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais, o Estatuto Digital da Criança e do Adolescente e sua regulamentação, além de mecanismos de denúncia, moderação, preservação de evidências e prevenção da recirculação de conteúdos ilícitos. Os resultados indicam que a proteção infantojuvenil no ambiente digital depende da adoção de medidas preventivas, mecanismos eficientes de resposta, governança de conteúdo, transparência e cooperação com autoridades competentes. Conclui-se que a responsabilização civil deve considerar as circunstâncias concretas de cada caso, especialmente a previsibilidade do risco, as medidas disponíveis e a atuação efetivamente adotada pelo provedor.

Palavras-chave: Direito Digital; Proteção Infanto-juvenil; ECA Digital; Redes Sociais; Responsabilidade Civil.

ABSTRACT

The article analyzes the civil liability of social networks and internet providers regarding the dissemination of illicit content involving children and adolescents in Brazil. The objective is to understand how the duties of prevention, response, and reparation relate to the

circulation, redistribution, and indexing of illegal materials in digital environments. The research adopts a qualitative approach based on bibliographic and documentary research, supported by the analysis of Brazilian legislation, judicial decisions, institutional documents, and specialized literature on Digital Law and child and adolescent protection. The analysis considers the Statute of the Child and Adolescent, the Brazilian Civil Rights Framework for the Internet, the General Data Protection Law, the Digital Statute of Children and Adolescents, and its regulation, as well as reporting mechanisms, content moderation, evidence preservation, and measures to prevent the recirculation of illicit content. The results indicate that child and adolescent protection in digital environments depends on preventive measures, effective response mechanisms, content governance, transparency, and cooperation with competent authorities. The study concludes that civil liability should consider the specific circumstances of each case, particularly the foreseeability of the risk, the available measures, and the actions effectively adopted by the provider.

Keywords: Digital Law; Child And Adolescent Protection; Digital Statute Of Children And Adolescents; Social Networks; Civil Liability.

1. INTRODUÇÃO

O avanço das tecnologias digitais transformou de maneira significativa as formas de comunicação, interação e circulação de informações na sociedade. As redes sociais, plataformas de compartilhamento e outros serviços disponíveis na internet passaram a fazer parte da rotina de diferentes grupos sociais, incluindo crianças e adolescentes. Esses espaços oferecem possibilidades de comunicação, aprendizagem e acesso a conteúdos diversos, mas também podem ser utilizados para práticas ilícitas que

atingem direitos fundamentais do público infantojuvenil. Entre essas situações estão a divulgação de material de abuso sexual infantil, o aliciamento de crianças e adolescentes no ambiente virtual, a extorsão e outras formas de violência mediadas pelas tecnologias digitais (Rodrigues; Melo, 2025).

A própria dinâmica da internet contribui para aumentar a complexidade desses casos. Um conteúdo publicado em uma plataforma pode ser copiado em poucos segundos, compartilhado por diferentes usuários e disponibilizado novamente em outros ambientes digitais. Mesmo após uma primeira retirada, novas cópias podem surgir, prolongando os efeitos da violação e dificultando o controle sobre a circulação do material. Sistemas de busca, mecanismos de recomendação e ferramentas automatizadas também podem ampliar a visibilidade de determinadas publicações. Diante disso, a atuação das plataformas deixa de ser apenas uma questão relacionada ao funcionamento técnico dos serviços e passa a envolver discussões jurídicas sobre prevenção, resposta, monitoramento e reparação dos danos provocados pela circulação de conteúdos ilícitos (Mendes, 2020; Santos, 2025).

A proteção de crianças e adolescentes no ambiente digital encontra fundamento no princípio da proteção integral e na prioridade absoluta estabelecidos pelo ordenamento jurídico brasileiro. O art. 227 da Constituição Federal determina que cabe à família, à sociedade e ao Estado assegurar à criança e ao adolescente seus direitos fundamentais, colocando-os a salvo de situações de negligência, exploração, violência e crueldade (Brasil, 1988). Essa proteção é complementada pelo Estatuto da Criança e do Adolescente e por outras normas relacionadas ao uso da internet e ao tratamento de dados pessoais. Juntas, essas disposições formam

uma base jurídica que precisa ser considerada diante dos riscos decorrentes da crescente utilização das plataformas digitais por esse público (Brasil, 1990; Brasil, 2014; Brasil, 2018).

A partir desse cenário, a responsabilidade civil dos diferentes agentes que participam do funcionamento da internet passa a ocupar posição relevante no debate. Provedores de conexão, de aplicação e de hospedagem não desempenham as mesmas funções e, por isso, também não possuem idênticas possibilidades de atuação diante de um conteúdo ilícito. Enquanto os provedores de conexão estão ligados ao acesso e à transmissão dos dados, os provedores de aplicação podem administrar perfis, publicações, sistemas de armazenamento, mecanismos de interação e ferramentas de recomendação. Identificar essas diferenças é necessário para compreender quais deveres podem ser atribuídos a cada agente e em que situações uma eventual omissão pode contribuir para a continuidade ou o agravamento do dano (Lima, 2015).

Essa discussão ganhou novos contornos com as recentes mudanças no regime jurídico brasileiro voltado à proteção de crianças e adolescentes no ambiente digital. A Lei nº 15.211/2025, denominada Estatuto Digital da Criança e do Adolescente, juntamente com sua regulamentação pelo Decreto nº 12.880/2026, reforça uma perspectiva voltada à prevenção dos riscos e à segurança de usuários infantojuvenis. Nesse contexto, temas como verificação de idade, segurança desde a concepção, proteção de dados pessoais, transparência e mecanismos de denúncia passam a ter maior importância na definição dos deveres atribuídos às plataformas digitais (Santos, 2025; Brasil, 2026).

Mesmo diante desse avanço normativo, ainda existe uma questão que precisa ser analisada com maior precisão: **em que medida as redes sociais e os provedores de internet podem ser responsabilizados civilmente pela divulgação, permanência ou recirculação de conteúdos ilícitos envolvendo crianças e adolescentes?**

A resposta não depende somente da constatação de que determinado material ilegal esteve disponível na plataforma. Também é necessário observar quando o provedor tomou conhecimento do fato, quais recursos técnicos estavam ao seu alcance, quais medidas preventivas haviam sido adotadas e se houve demora ou omissão após uma denúncia ou outra forma de ciência da ilicitude. Ao mesmo tempo, essa análise precisa considerar a proteção integral da criança e do adolescente sem desconsiderar direitos fundamentais como liberdade de expressão, privacidade e proteção de dados pessoais (Cavaliere Filho, 2020; Diniz, 2021).

A relevância do estudo está relacionada justamente a esse ponto. A circulação de conteúdos ilícitos em ambientes digitais possui características que dificultam a interrupção dos danos, especialmente quando o material é reproduzido, compartilhado ou disponibilizado novamente por diferentes usuários. No caso de crianças e adolescentes, os efeitos da exposição podem permanecer mesmo depois da retirada de uma publicação específica. Por essa razão, compreender os deveres de prevenção e resposta atribuídos aos provedores pode contribuir para o desenvolvimento do debate jurídico e, ao mesmo tempo, para a construção de mecanismos de proteção mais eficientes.

Nesse sentido, o presente estudo tem como objetivo analisar a responsabilidade civil das redes sociais e dos provedores de internet diante da divulgação de conteúdos ilícitos envolvendo crianças e adolescentes no Brasil, considerando os deveres de prevenção, resposta e reparação previstos no ordenamento jurídico. De forma específica, busca-se compreender as diferenças entre os principais tipos de provedores, examinar o marco normativo relacionado à proteção infantojuvenil no ambiente digital e identificar critérios que auxiliem na avaliação de situações envolvendo eventual omissão, culpa, nexo causal e dever de reparação.

Para o desenvolvimento da pesquisa, foi adotada uma abordagem qualitativa, de caráter bibliográfico e documental, com análise de legislação, doutrina, decisões judiciais e documentos institucionais relacionados à responsabilidade civil dos provedores e à proteção de crianças e adolescentes na internet. A investigação procura aproximar os fundamentos jurídicos das situações que ocorrem no ambiente digital, permitindo examinar os limites e as possibilidades de responsabilização dos diferentes agentes envolvidos.

O estudo parte da compreensão de que a proteção de crianças e adolescentes no ambiente digital não se resume à existência de normas jurídicas. É necessário que os deveres previstos nessas normas sejam acompanhados de mecanismos capazes de prevenir violações, identificar situações de risco e oferecer respostas adequadas quando o dano ocorrer. Ao analisar a responsabilidade civil das redes sociais e dos provedores de internet, a pesquisa busca contribuir para uma compreensão mais precisa dos deveres desses agentes e para o fortalecimento de medidas destinadas a reduzir a exposição e a continuidade dos danos provocados pela circulação de conteúdos ilícitos envolvendo crianças e adolescentes.

2. FUNDAMENTAÇÃO TEÓRICA OU REVISÃO DA LITERATURA

2.1. Fundamentos da Responsabilidade Civil no Ambiente das Plataformas

A circulação de conteúdos sexuais ilícitos envolvendo crianças e adolescentes no ambiente digital produz consequências que podem se prolongar mesmo depois da publicação inicial. Isso ocorre porque o material pode ser copiado, armazenado e compartilhado diversas vezes, fazendo com que a violação se reproduza em diferentes espaços e alcance novos usuários. A continuidade da circulação amplia a exposição da vítima e dificulta a interrupção dos efeitos do dano. Nesse cenário, a responsabilidade civil assume uma função relevante, pois permite discutir os deveres de prevenção, resposta e reparação atribuídos aos agentes que disponibilizam ou administram serviços utilizados para publicação, armazenamento e compartilhamento de informações. Essa discussão deve ser conduzida em conjunto com a proteção integral e a prioridade atribuídas às crianças e aos adolescentes, sem afastar as garantias relacionadas ao devido processo e à transparência (Brasil, 2023).

A análise da responsabilidade dos provedores exige, inicialmente, a compreensão das diferentes funções exercidas na estrutura da internet. Os provedores de aplicação administram serviços nos quais os usuários podem criar perfis, publicar conteúdos, realizar comentários, trocar mensagens ou receber recomendações. Os serviços de hospedagem, por sua vez, estão relacionados ao armazenamento de arquivos e informações, enquanto os provedores de conexão oferecem a infraestrutura necessária para o acesso e a transmissão dos dados. Essa divisão não possui apenas importância técnica. Ela também interfere na análise jurídica, uma vez que o

grau de controle sobre determinado conteúdo e a possibilidade concreta de intervenção variam conforme a atividade desempenhada pelo provedor (Lima, 2015).

Quanto maior for a proximidade do agente em relação ao conteúdo e aos mecanismos que permitem sua circulação, maior tende a ser sua capacidade de identificar situações de risco e adotar medidas de resposta. Uma rede social, por exemplo, dispõe de recursos próprios para receber denúncias, administrar publicações, suspender contas e controlar determinadas formas de compartilhamento. Já um provedor responsável pela conexão não exerce o mesmo nível de controle sobre aquilo que os usuários publicam. Essa diferença precisa ser considerada quando se examina uma possível omissão, pois não seria adequado atribuir obrigações idênticas a agentes que ocupam posições distintas na cadeia de funcionamento da internet (Lima, 2015).

No caso de conteúdos relacionados à exploração sexual de crianças e adolescentes, a análise assume uma gravidade ainda maior. Trata-se de material cuja própria natureza está associada à violação de direitos fundamentais desse público, o que exige uma resposta compatível com a dimensão do dano produzido. A permanência de um arquivo em circulação pode favorecer novas cópias, downloads e compartilhamentos, mantendo a situação lesiva mesmo após o primeiro episódio de divulgação. Por isso, a atuação dos provedores não deve ser analisada somente a partir do momento em que o conteúdo foi originalmente publicado, mas também considerando as providências adotadas depois que a situação chegou ao seu conhecimento (Brasil, 2024).

A ciência da existência do conteúdo ilícito constitui, nesse contexto, um elemento importante para a avaliação da conduta do provedor. Essa ciência pode ocorrer por meio de uma denúncia apresentada por usuário ou representante da vítima, de uma determinação emitida por autoridade competente ou, ainda, de mecanismos internos utilizados pela própria plataforma para identificar possíveis violações. Uma vez conhecida a situação, torna-se necessário avaliar quais providências foram adotadas, em quanto tempo ocorreram e se foram suficientes para interromper a continuidade da circulação. O registro das decisões e dos procedimentos empregados também possui relevância, pois permite verificar posteriormente como o caso foi tratado e quais critérios orientaram a atuação da empresa (Brasil, 2014).

A responsabilidade civil, entretanto, não pode ser definida apenas pela existência de um conteúdo ilícito em determinada plataforma. É necessário observar as circunstâncias concretas do caso. Entre os elementos que podem ser considerados estão a previsibilidade do risco, a existência de medidas razoáveis para sua redução, o cumprimento das políticas de segurança anunciadas pelo próprio serviço e a ocorrência de falhas semelhantes que permaneceram sem correção. Quando uma empresa possui conhecimento de determinado risco e, ainda assim, deixa de adotar providências que estavam ao seu alcance, a discussão sobre culpa e nexo causal ganha maior consistência. A repetição de falhas também pode demonstrar que o problema não decorre de um episódio isolado, mas de uma deficiência na estrutura de prevenção e resposta da plataforma (Frazão, 2022).

As tecnologias utilizadas para identificação e moderação de conteúdos também passaram a integrar essa discussão. Sistemas

automatizados podem auxiliar na identificação de padrões, na triagem de denúncias e na localização de arquivos previamente identificados por meio de mecanismos de hash. Esses recursos aumentam a capacidade de resposta das plataformas, principalmente diante do grande volume de informações processadas diariamente. Entretanto, a automação não elimina a possibilidade de erros. Falsos positivos e falsos negativos podem ocorrer, tornando necessária a adoção de procedimentos de revisão humana em situações que apresentem maior complexidade ou potencial de dano.

A utilização desses mecanismos deve estar acompanhada de procedimentos que permitam compreender como as decisões foram tomadas. Registros de auditoria, mecanismos de revisão e informações sobre as providências adotadas contribuem para a transparência das plataformas e permitem avaliar a efetividade de suas políticas de proteção. Relatórios com dados agregados sobre denúncias, medidas de remoção, tempo de resposta e decisões posteriormente revistas também podem fornecer elementos para o acompanhamento das práticas adotadas pelas empresas. Nesse sentido, a transparência não representa apenas uma ferramenta de prestação de informações, mas também um instrumento para identificar falhas e aperfeiçoar os mecanismos de proteção existentes (SaferNet Brasil, 2024).

Outro aspecto relacionado ao dever de cuidado está na prevenção da reincidência. A retirada de determinado arquivo não impede, por si só, que o mesmo material volte a ser disponibilizado. Em ambientes digitais caracterizados pela facilidade de reprodução, a adoção de mecanismos capazes de reconhecer conteúdos anteriormente identificados pode reduzir a ocorrência de novos

compartilhamentos. Bases de hash, sistemas internos de bloqueio, cooperação com canais especializados de denúncia e integração entre diferentes mecanismos de proteção podem contribuir para limitar a recirculação desses materiais. Essas medidas precisam ser acompanhadas por treinamento das equipes responsáveis pela moderação, avaliação periódica dos procedimentos e mecanismos de auditoria que permitam verificar seu funcionamento (CGI.br, 2024).

A proteção das evidências também ocupa espaço importante nesse processo. Quando um conteúdo ilícito é identificado, a retirada não deve significar necessariamente a perda dos elementos que podem auxiliar uma investigação. Informações técnicas relacionadas ao arquivo, aos registros de acesso e às circunstâncias de sua disponibilização podem ser relevantes para a atuação das autoridades competentes. Essa preservação, entretanto, precisa observar as normas de segurança da informação e de proteção de dados pessoais, restringindo o acesso às informações necessárias e registrando as operações realizadas sobre os dados (CGI.br, 2024).

Os provedores de conexão ocupam uma posição diferente nesse sistema. Como não administram diretamente as publicações realizadas pelos usuários, sua atuação não se confunde com aquela exercida pelos provedores de aplicação ou de hospedagem. Ainda assim, podem possuir obrigações relacionadas à guarda e ao fornecimento de registros, desde que observados os requisitos legais aplicáveis. A cooperação entre os diferentes agentes pode contribuir para a identificação de responsáveis pela prática ilícita, mas deve ocorrer dentro dos limites estabelecidos pela legislação, evitando a exposição desnecessária de informações pessoais e preservando a integridade dos registros utilizados na investigação (Brasil, 2018).

A partir dessa perspectiva, a responsabilidade civil no ambiente das plataformas não deve ser compreendida apenas como uma consequência posterior à ocorrência do dano. Ela também envolve a análise das medidas adotadas para reduzir riscos previsíveis e impedir que uma violação conhecida continue produzindo efeitos. A existência de canais específicos de denúncia, procedimentos de resposta rápida, mecanismos de identificação de conteúdos reincidentes, revisão humana em situações sensíveis, preservação adequada das evidências e comunicação com as autoridades são elementos que podem ser considerados na avaliação da diligência do provedor (Brasil, 2023).

Desse modo, a discussão sobre responsabilidade civil das plataformas digitais exige uma análise que considere tanto a posição ocupada por cada provedor quanto sua capacidade concreta de prevenir, identificar e interromper situações de violação. No caso de conteúdos ilícitos envolvendo crianças e adolescentes, essa análise assume especial importância em razão da possibilidade de reprodução contínua do material e da extensão dos danos provocados. A responsabilidade não decorre simplesmente da presença de um conteúdo em determinado serviço, mas deve ser examinada a partir das circunstâncias do caso, do conhecimento do provedor, das medidas disponíveis e da conduta adotada diante do risco ou da violação já identificada.

2.2. Marco Normativo e Deveres de Cuidado em Casos de CSAM

A proteção de crianças e adolescentes diante de conteúdos de natureza sexual no ambiente digital encontra fundamento em um conjunto de normas que reconhecem a condição peculiar de desenvolvimento desse público e estabelecem uma proteção

jurídica diferenciada. O Estatuto da Criança e do Adolescente constitui uma das principais bases desse sistema ao assegurar a proteção integral e a prioridade absoluta dos direitos infantojuvenis. Quando a circulação de material de abuso sexual infantil é identificada, a resposta jurídica precisa considerar a gravidade da violação e a possibilidade de continuidade do dano por meio de novas cópias e compartilhamentos. Nesse sentido, medidas relacionadas à retirada do conteúdo, à preservação de elementos necessários à investigação e à cooperação com as autoridades passam a integrar a discussão sobre a proteção das vítimas (Brasil, 2024).

No ambiente digital, essa proteção se relaciona diretamente com as regras estabelecidas pelo Marco Civil da Internet. A Lei nº 12.965/2014 definiu princípios, garantias, direitos e deveres para o uso da internet no Brasil e estabeleceu parâmetros para a atuação dos diferentes agentes que participam desse ambiente. A responsabilização dos provedores, especialmente diante de conteúdos produzidos por terceiros, deve ser analisada considerando as circunstâncias previstas na legislação e a forma pela qual o agente toma conhecimento da situação. Ao mesmo tempo, o Marco Civil procura preservar direitos como a liberdade de expressão e a privacidade, o que exige equilíbrio entre a retirada de conteúdos ilícitos e a adoção de procedimentos que permitam verificar e documentar as decisões tomadas (Brasil, 2014).

Nos casos envolvendo crianças e adolescentes, contudo, a análise não pode ignorar a prioridade atribuída à proteção desse público. A presença de um conteúdo ilícito e a possibilidade de sua rápida reprodução tornam o tempo de resposta um elemento relevante. Uma demora injustificada pode permitir novos compartilhamentos

e aumentar a exposição da vítima. Por essa razão, a atuação do provedor deve ser examinada não apenas pela existência de mecanismos formais de denúncia, mas também pela capacidade de responder de maneira adequada depois de tomar conhecimento de uma situação concreta.

Outro marco relevante é a Lei nº 13.718/2018, que promoveu alterações no tratamento jurídico de crimes contra a dignidade sexual e ampliou a proteção diante de determinadas condutas praticadas no ambiente físico e digital. A divulgação não autorizada de imagens de conteúdo sexual representa uma forma de violação que pode adquirir proporções ainda maiores quando ocorre pela internet, devido à facilidade de reprodução e compartilhamento. No caso de crianças e adolescentes, essa preocupação se soma às disposições específicas de proteção previstas no Estatuto da Criança e do Adolescente. A articulação entre essas normas contribui para delimitar o caráter ilícito das condutas e para reforçar a necessidade de medidas capazes de interromper sua continuidade (Brasil, 2018).

A responsabilidade dos provedores também está relacionada à forma como as empresas estruturam seus mecanismos internos de prevenção e resposta. A existência de políticas públicas de proteção, regras de uso e procedimentos de moderação permite estabelecer parâmetros para avaliar a atuação de determinada plataforma diante de um risco conhecido. Registros sobre denúncias, decisões de remoção, preservação de evidências e encaminhamentos realizados podem contribuir para verificar se os procedimentos previstos foram efetivamente cumpridos. A documentação dessas etapas também favorece a transparência e permite uma análise posterior da conduta adotada pela empresa. A bibliografia selecionada pelo Supremo Tribunal Federal sobre a

responsabilização civil de provedores destaca justamente a relevância de aspectos como previsibilidade dos riscos, deveres de cuidado e observância das regras aplicáveis ao serviço (Brasil, 2023).

A prevenção também passou a ocupar espaço importante no debate sobre proteção de crianças e adolescentes na internet. Ferramentas de correspondência por hash podem auxiliar na identificação de arquivos previamente reconhecidos como ilícitos, enquanto mecanismos automatizados de classificação permitem realizar uma primeira triagem diante do grande volume de conteúdos processados pelas plataformas. Essas tecnologias podem reduzir o tempo necessário para identificar situações de risco, mas não afastam a necessidade de supervisão adequada. Em casos que envolvam dúvidas ou decisões de maior complexidade, a revisão humana pode contribuir para reduzir erros e assegurar que as medidas adotadas sejam compatíveis com a situação analisada. Ao mesmo tempo, o tratamento das informações precisa respeitar princípios relacionados à privacidade, à segurança e à minimização de dados (Frazão, 2022).

A diferenciação entre os tipos de provedores permanece necessária para compreender como esses deveres são distribuídos. Os provedores de aplicação, por administrarem serviços nos quais ocorre publicação, interação e circulação de conteúdos, possuem instrumentos específicos para receber denúncias e intervir sobre determinadas atividades. Os serviços de hospedagem estão diretamente relacionados ao armazenamento das informações, enquanto os provedores de conexão desempenham função ligada ao acesso e à transmissão dos dados. As possibilidades de intervenção, nesse sentido, não são iguais. A posição ocupada por cada agente na estrutura da internet precisa ser considerada

quando se avalia sua capacidade de prevenção, resposta e colaboração com investigações (Lima, 2015).

Os mecanismos de denúncia representam outro componente desse sistema de proteção. Canais específicos para situações envolvendo crianças e adolescentes podem facilitar a comunicação da violação e reduzir obstáculos para que vítimas, familiares, representantes ou outras pessoas legitimadas comuniquem a existência do conteúdo. Quando esses canais estão articulados com organizações especializadas, autoridades públicas e entidades da sociedade civil, torna-se possível ampliar a capacidade de identificação e encaminhamento dos casos. A atuação de organizações voltadas à proteção de crianças e adolescentes no ambiente digital também demonstra a importância da cooperação entre empresas, Estado e sociedade civil na prevenção e no enfrentamento dessas violações (SaferNet Brasil, 2024).

A necessidade de medidas preventivas ganha maior importância diante da ampla presença de crianças e adolescentes no ambiente digital. Pesquisas sobre o uso da internet por esse público indicam que a participação em plataformas digitais ocorre cada vez mais cedo e em diferentes contextos de interação. Esse cenário exige que a proteção não seja pensada somente depois da ocorrência de uma violação. Educação para o uso seguro da internet, mecanismos adequados de identificação etária, recursos de denúncia acessíveis e medidas de segurança incorporadas ao próprio desenvolvimento das plataformas são estratégias que podem contribuir para reduzir a exposição a riscos. A adoção dessas medidas deve ser acompanhada por avaliações periódicas, indicadores de desempenho e procedimentos de auditoria que permitam verificar sua efetividade (CGI.br, 2024).

Os deveres de cuidado atribuídos aos provedores não se limitam à retirada de um conteúdo depois que o dano já ocorreu. A atuação preventiva, a existência de mecanismos de identificação, a resposta às denúncias, a preservação das evidências e a cooperação com as autoridades fazem parte de uma estrutura mais ampla de proteção. O modo como essas medidas são organizadas pode ser considerado na análise da diligência do provedor, principalmente quando existem riscos previsíveis e recursos técnicos disponíveis para reduzi-los.

A aplicação dessas normas ao ambiente digital exige, assim, uma análise conjunta entre proteção jurídica e capacidade efetiva de atuação. Prazos de resposta, critérios de prioridade, mecanismos de bloqueio de reenvios, preservação adequada das evidências e comunicação com os envolvidos são aspectos que podem contribuir para tornar mais efetiva a proteção de crianças e adolescentes. Mais do que estabelecer obrigações abstratas, o marco normativo fornece parâmetros para avaliar a conduta dos agentes diante de situações concretas. Quando esses parâmetros são relacionados à posição ocupada pelo provedor, ao conhecimento da violação e às medidas disponíveis, torna-se possível aprofundar a discussão sobre eventual omissão e responsabilidade civil pela continuidade do dano (Brasil, 2014).

2.3. Procedimentos de Notificação, Prova e Cooperação para Retirada e Staydown

A notificação de conteúdos ilícitos envolvendo crianças e adolescentes representa um dos principais momentos para a atuação dos provedores de internet. A partir da ciência sobre determinada violação, torna-se possível avaliar o conteúdo, adotar

medidas de contenção e preservar informações que possam contribuir para a investigação. Nos casos de material de abuso sexual infantil, essa resposta assume especial importância, pois a permanência do conteúdo pode favorecer novas cópias e ampliar a exposição da vítima. Por essa razão, os procedimentos de atendimento devem estar estruturados de modo a permitir uma resposta rápida, documentada e compatível com o princípio da proteção integral (Brasil, 2024).

O processo começa com a possibilidade de comunicação da situação à plataforma. Para isso, os serviços digitais precisam disponibilizar canais que sejam acessíveis e suficientemente claros para que o usuário consiga informar a existência do conteúdo. Dados como o endereço da publicação ou outras informações que permitam sua localização podem facilitar a análise da denúncia. Depois de recebida a comunicação, o registro da ocorrência permite acompanhar as providências adotadas e verificar o tempo transcorrido entre a ciência do fato e a resposta do provedor. Essa documentação possui importância jurídica, especialmente porque a notificação pode constituir elemento relevante para a análise da conduta adotada diante de um conteúdo produzido por terceiros (Brasil, 2014).

A partir da denúncia, a avaliação do caso envolve diferentes providências que podem ocorrer de forma articulada. A primeira está relacionada à contenção do conteúdo identificado, evitando que ele permaneça disponível enquanto a situação é analisada. Paralelamente, pode ser necessário verificar a existência de outras cópias dentro do mesmo serviço. Há ainda a preservação de informações relevantes para eventual investigação. Essas três dimensões, contenção, identificação de possíveis réplicas e

preservação da prova, são importantes porque a simples retirada de uma publicação não impede, por si só, a continuidade dos efeitos da violação (Ministério Público do Paraná, 2018).

A preservação das evidências exige critérios específicos. Informações como identificadores da publicação, data e horário, registros técnicos disponíveis e determinados metadados podem contribuir para reconstruir as circunstâncias em que o conteúdo foi disponibilizado. O cálculo do hash do arquivo também pode ser utilizado como recurso técnico para identificar posteriormente o mesmo material ou versões correspondentes, sem que seja necessário manter sua circulação. Nesse processo, o acesso às informações preservadas deve ser restrito e documentado, especialmente quando envolver dados pessoais ou elementos que possam integrar uma investigação oficial. A preocupação com a rastreabilidade das providências adotadas está relacionada à necessidade de conferir maior segurança e confiabilidade à utilização dessas informações (Brasil, 2023).

A prevenção de novos compartilhamentos está relacionada ao conceito de staydown, utilizado para designar mecanismos destinados a impedir ou reduzir a recirculação de conteúdos que já foram identificados e removidos. Nesse modelo, a retirada da publicação original representa apenas uma etapa da resposta. A partir da identificação técnica do arquivo, recursos como o hash podem auxiliar na localização de novas tentativas de disponibilização do mesmo material. Essa estratégia é especialmente relevante em situações nas quais a repetição do conteúdo constitui parte importante da continuidade do dano.

A utilização de sistemas automatizados pode ampliar a capacidade das plataformas de localizar possíveis cópias. Classificadores e ferramentas de correspondência podem analisar grandes volumes de informações em períodos reduzidos, contribuindo para a identificação inicial de conteúdos potencialmente ilícitos. Entretanto, esses mecanismos não estão livres de falhas. Uma decisão baseada exclusivamente em processos automatizados pode produzir erros, especialmente em situações que exigem análise contextual. A revisão humana, nesse sentido, permanece relevante para os casos que apresentam dúvida ou maior complexidade, juntamente com procedimentos de contestação e mecanismos de transparência sobre as decisões tomadas (Frazão, 2022).

A cooperação entre plataformas, autoridades públicas e organizações especializadas também possui papel relevante no enfrentamento da circulação de conteúdos ilícitos. Canais de denúncia mantidos por entidades especializadas podem facilitar o encaminhamento das ocorrências e ampliar a capacidade de identificação de materiais que circulam em diferentes serviços. A atuação conjunta permite compartilhar informações dentro dos limites legais, reduzir a repetição de esforços e oferecer encaminhamento adequado às situações que envolvem vítimas. No Brasil, a atuação da SaferNet na recepção de denúncias relacionadas a violações de direitos no ambiente digital demonstra a importância desses mecanismos de articulação entre sociedade civil e instituições responsáveis pela proteção dos usuários (SaferNet Brasil, 2024).

A proteção da vítima também deve ser considerada durante esse processo. A pessoa que realiza uma denúncia precisa encontrar informações claras sobre o recebimento da comunicação e, quando

possível, sobre o encaminhamento dado à situação. Em casos envolvendo crianças e adolescentes, a preocupação não deve estar limitada à retirada do conteúdo. A resposta institucional precisa evitar novas exposições, reduzir a circulação do material e orientar os envolvidos sobre os canais disponíveis para buscar auxílio. Essa perspectiva aproxima os procedimentos técnicos da finalidade maior de proteção dos direitos infantojuvenis.

As medidas de prevenção também podem ser incorporadas ao próprio desenvolvimento das plataformas. Recursos de denúncia acessíveis, mecanismos de identificação de idade, alertas educativos e ferramentas que dificultem determinadas formas de compartilhamento podem atuar antes que a violação alcance maiores proporções. A adoção dessas salvaguardas ganha importância diante da presença significativa de crianças e adolescentes na internet e da variedade de ambientes digitais utilizados por esse público. Estudos sobre o uso da rede por crianças e adolescentes reforçam a necessidade de considerar segurança e proteção como elementos presentes no próprio desenho dos serviços (CGI.br, 2024).

A distribuição dos deveres também depende da função exercida por cada tipo de provedor. As plataformas que administram perfis, feeds, comentários e sistemas de recomendação possuem instrumentos diretamente relacionados à publicação e à circulação dos conteúdos. Os serviços de hospedagem, por sua vez, possuem atuação vinculada ao armazenamento das informações. Já os provedores de conexão não exercem controle editorial sobre aquilo que é publicado pelos usuários, embora possam possuir registros relevantes para investigações e estejam sujeitos às obrigações legais correspondentes. A diferenciação dessas funções permite analisar a

capacidade concreta de intervenção de cada agente e evita que responsabilidades sejam atribuídas de maneira uniforme a estruturas que desempenham atividades distintas (Lima, 2015).

Outro aspecto importante é a transparência sobre os resultados das medidas adotadas. Relatórios periódicos podem apresentar informações agregadas sobre denúncias recebidas, conteúdos removidos, tempo de resposta, identificação de novas cópias e participação de mecanismos de revisão humana. Esses dados ajudam a compreender como as políticas de proteção estão funcionando e permitem comparar resultados ao longo do tempo. Para que tenham utilidade, entretanto, os indicadores precisam ser acompanhados de informações sobre os critérios utilizados para sua elaboração, possibilitando uma avaliação mais consistente das práticas adotadas pelos provedores (Brasil, 2014).

A notificação, a preservação da prova e a prevenção da recirculação, quando articuladas, formam um conjunto de medidas que ultrapassa a simples retirada de uma publicação. O objetivo é interromper a circulação do conteúdo, preservar os elementos necessários à investigação e reduzir a possibilidade de que a mesma violação volte a ocorrer. Em situações envolvendo crianças e adolescentes, essa estrutura precisa ser orientada pela proteção integral e pela necessidade de reduzir a continuidade do dano. A forma como o provedor responde depois de tomar conhecimento da situação pode, nesse sentido, fornecer elementos importantes para a análise de sua diligência e para a discussão sobre eventual responsabilidade civil (Brasil, 2014; Brasil, 2024).

2.4. Reparação de Danos, Tutela Inibitória e Parâmetros de Diligência

A reparação civil nos casos envolvendo conteúdos sexuais ilícitos relacionados a crianças e adolescentes apresenta uma particularidade importante: os efeitos da violação podem continuar mesmo depois da publicação original. Cada nova cópia, compartilhamento ou disponibilização do material pode ampliar a exposição da vítima e prolongar as consequências do dano. Por essa razão, a reparação não deve ser compreendida somente como pagamento de indenização. Dependendo das circunstâncias, também podem ser necessárias medidas destinadas a interromper a circulação do conteúdo e impedir que novas ocorrências produzam efeitos semelhantes. Nesse contexto, a responsabilidade civil pode envolver tanto a compensação pelos danos já produzidos quanto medidas voltadas à sua contenção e prevenção (Frazão, 2022).

A tutela inibitória possui importância justamente por atuar diante da possibilidade de continuidade ou repetição da lesão. Em situações nas quais determinado conteúdo permanece disponível ou existe risco concreto de novos compartilhamentos, medidas direcionadas à interrupção da conduta podem assumir papel relevante. A remoção do material, o bloqueio de novas formas de disponibilização e outras obrigações de fazer ou não fazer podem ser determinadas de acordo com as circunstâncias do caso.

O Marco Civil da Internet oferece parâmetros relevantes para a análise da atuação dos provedores e das condições em que sua responsabilidade pode ser discutida. A ciência sobre determinado conteúdo, os procedimentos adotados após a comunicação e o cumprimento das determinações aplicáveis constituem elementos que podem ser considerados na avaliação da conduta do agente. A existência de registros também possui importância probatória.

Protocolos de denúncia, informações sobre as providências adotadas e documentação relacionada ao cumprimento de decisões permitem reconstruir a sequência dos acontecimentos e verificar se houve atuação adequada ou demora injustificada (Brasil, 2014).

A prioridade atribuída à proteção de crianças e adolescentes reforça a necessidade de respostas compatíveis com a gravidade dessas situações. O Estatuto da Criança e do Adolescente estabelece a proteção integral como princípio orientador e determina prioridade absoluta à efetivação dos direitos desse público. Quando a situação envolve material de abuso sexual infantil, a necessidade de interromper a circulação deve ser analisada em conjunto com a preservação dos elementos necessários à investigação. A retirada do conteúdo e a preservação adequada das evidências, nesse sentido, não são medidas necessariamente incompatíveis. É possível buscar a interrupção da exposição pública sem comprometer as informações que possam ser relevantes para a responsabilização dos envolvidos (Brasil, 2024).

A extensão do dano também precisa ser considerada na análise da reparação. Quando o conteúdo permanece disponível por determinado período ou circula por diferentes serviços, os efeitos da exposição podem se acumular. A quantidade de cópias, a duração da disponibilidade e a capacidade do provedor de interromper a recirculação são aspectos que podem auxiliar na compreensão das consequências provocadas pela violação. Da mesma forma, a existência de mecanismos preventivos, como sistemas de identificação por hash, ferramentas de denúncia e procedimentos de revisão, pode contribuir para avaliar quais medidas estavam disponíveis ao agente e como foram utilizadas diante da situação concreta (Brasil, 2023).

A análise da responsabilidade também exige diferenciar o conteúdo produzido por terceiros de uma eventual falha no cumprimento de deveres próprios do provedor. Um agente que apenas oferece infraestrutura de conexão não possui as mesmas possibilidades de intervenção que uma plataforma responsável por administrar perfis, publicações, mecanismos de recomendação e ferramentas de compartilhamento. Essa distinção influencia a avaliação da conduta, pois a capacidade concreta de prevenir ou interromper determinada situação varia conforme a função desempenhada. A doutrina sobre responsabilidade dos provedores antes e depois do Marco Civil contribui para compreender essas diferenças e para estabelecer parâmetros mais adequados à análise de cada caso (Lima, 2015).

A tutela inibitória pode adquirir maior efetividade quando acompanhada de mecanismos capazes de reduzir a reincidência. O uso de identificadores digitais, como hashes, permite reconhecer arquivos previamente identificados e pode dificultar novas tentativas de disponibilização. Sistemas automatizados também podem auxiliar na triagem de grandes quantidades de conteúdo, embora sua utilização exija cautela diante da possibilidade de erros. Em situações mais sensíveis, a revisão humana contribui para conferir maior segurança às decisões. Indicadores como tempo de resposta, quantidade de conteúdos bloqueados e taxa de reversão podem, ainda, fornecer elementos para avaliar o funcionamento dessas medidas ao longo do tempo (Frazão, 2022).

A cooperação com órgãos especializados e organizações que atuam na proteção de crianças e adolescentes complementa esse sistema. Canais específicos de denúncia e equipes capacitadas podem facilitar o encaminhamento das ocorrências, enquanto a articulação com autoridades permite que informações relevantes sejam

utilizadas em investigações dentro dos limites legais. A preservação da cadeia de custódia também merece atenção, principalmente quando os registros digitais poderão ser utilizados como elementos probatórios. A documentação sobre coleta, armazenamento e acesso às informações contribui para preservar sua integridade e, simultaneamente, reduzir o tratamento desnecessário de dados pessoais (Ministério Público do Paraná, 2018).

Os parâmetros de diligência também podem ser relacionados ao próprio desenvolvimento dos produtos e serviços digitais. A presença crescente de crianças e adolescentes na internet amplia a necessidade de considerar os riscos associados ao uso dessas plataformas desde a fase de planejamento. Recursos de verificação de idade, mecanismos que dificultem determinadas formas de envio de arquivos, ferramentas de denúncia e ações de educação digital podem integrar estratégias preventivas. A análise de dados sobre os hábitos e riscos relacionados ao uso da internet por esse público fornece elementos para compreender a dimensão do problema e para avaliar a necessidade de aperfeiçoamento das medidas de proteção (CGI.br, 2024).

A diligência do provedor, nesse sentido, não pode ser avaliada por um único indicador. É necessário observar o conjunto de medidas disponíveis, a natureza do serviço, os riscos envolvidos, o conhecimento sobre a situação e a resposta efetivamente oferecida. Também importa verificar se os mecanismos anunciados pela própria plataforma funcionam na prática. Uma política de proteção somente produz efeitos concretos quando existe estrutura para sua aplicação, acompanhamento dos resultados e correção das falhas identificadas.

A reparação civil, quando analisada sob essa perspectiva, ultrapassa a ideia de compensação financeira. Ela pode envolver medidas destinadas a interromper a continuidade da violação, reduzir a possibilidade de recirculação e corrigir falhas que favoreçam novos episódios. A tutela inibitória e os parâmetros de diligência assumem, assim, uma função complementar: enquanto a primeira busca impedir a continuidade ou repetição da lesão, os segundos auxiliam na avaliação da conduta adotada pelo provedor diante dos riscos existentes e das medidas que estavam ao seu alcance. No caso de conteúdos ilícitos envolvendo crianças e adolescentes, essa análise deve permanecer vinculada à proteção integral e à necessidade de reduzir, tanto quanto possível, a continuidade dos danos produzidos no ambiente digital.

2.5. Governança de Conteúdo, Transparência e Desenho de Produto Orientados à Proteção

A governança de conteúdo constitui uma dimensão importante da proteção de crianças e adolescentes no ambiente digital, especialmente quando se trata de situações envolvendo materiais de natureza sexual. Mais do que estabelecer regras de utilização, a governança envolve a definição de procedimentos, responsabilidades e mecanismos capazes de orientar a atuação da plataforma diante de situações de risco. No contexto da proteção infantojuvenil, esses mecanismos precisam estar relacionados ao princípio da proteção integral e à prioridade absoluta assegurados pelo ordenamento jurídico brasileiro. A existência de normas internas, entretanto, não é suficiente por si só. É necessário que os procedimentos previstos possam ser aplicados, acompanhados e avaliados de maneira objetiva (Brasil, 2024).

A qualidade dessa estrutura depende, em parte, da capacidade de transformar princípios gerais em procedimentos verificáveis. Uma plataforma pode estabelecer regras contra conteúdos ilícitos, mas precisa também possuir meios para receber denúncias, analisar ocorrências, registrar decisões e acompanhar os resultados das medidas adotadas. A definição de responsáveis e de critérios para situações de maior gravidade contribui para reduzir respostas improvisadas. No caso de conteúdos envolvendo crianças e adolescentes, essa organização ganha maior relevância porque o tempo de exposição pode interferir diretamente na extensão do dano.

As métricas de desempenho também podem contribuir para a avaliação das políticas de proteção. Indicadores relacionados ao tempo de resposta, à quantidade de conteúdos removidos, à identificação de novas cópias e aos resultados da revisão das decisões permitem observar o funcionamento dos mecanismos de moderação. Outros dados, como a proporção de decisões automatizadas posteriormente modificadas e o tempo necessário para preservar informações relevantes, podem complementar essa análise. Quando interpretados de forma adequada, esses indicadores aproximam a dimensão técnica da discussão jurídica sobre diligência, permitindo verificar como a plataforma responde depois de tomar conhecimento de uma situação ilícita (Brasil, 2014).

A transparência, por sua vez, precisa estar acompanhada de critérios que permitam compreender os dados apresentados. Um relatório que apenas informa o número total de denúncias ou remoções oferece pouca informação sobre a efetividade da política adotada. É necessário conhecer, dentro dos limites de segurança e proteção de dados, os critérios utilizados para classificar as ocorrências, os

períodos considerados e os métodos empregados na produção dos indicadores. Essa documentação pode assumir importância na análise posterior da conduta do provedor, sobretudo quando existe discussão sobre culpa, nexo causal ou extensão do dano (Brasil, 2023).

A cooperação com organizações especializadas constitui outro elemento da governança. Canais de denúncia mantidos por entidades com experiência na proteção de crianças e adolescentes podem ampliar as possibilidades de comunicação das violações e facilitar o encaminhamento das ocorrências. No Brasil, a atuação da SaferNet demonstra a importância de estruturas especializadas para o recebimento e encaminhamento de denúncias relacionadas a violações ocorridas no ambiente digital (SaferNet Brasil, 2024).

A estrutura de governança, contudo, não depende apenas de sistemas tecnológicos. As pessoas responsáveis pela análise das denúncias também precisam estar preparadas para lidar com situações de elevada complexidade. A formação das equipes pode envolver conhecimentos relacionados à identificação de conteúdos ilícitos, preservação de evidências, proteção de dados e comunicação adequada com vítimas, familiares e autoridades. O trabalho de moderação de conteúdos potencialmente violentos ou abusivos pode produzir desgaste emocional e fadiga decisória, o que torna relevantes medidas de supervisão, distribuição adequada das tarefas e acompanhamento das condições de trabalho. A ampliação da presença de crianças e adolescentes nos ambientes digitais reforça a necessidade de estruturas capazes de acompanhar esse aumento de demanda (CGI.br, 2024).

A proteção também pode ser incorporada ao próprio desenho dos produtos e serviços. Em vez de depender exclusivamente da reação após a ocorrência de um incidente, as plataformas podem desenvolver recursos destinados a reduzir determinados riscos desde o início. Ferramentas de denúncia acessíveis, mecanismos de identificação etária, restrições específicas para determinados tipos de interação, configurações de privacidade mais protetivas e mensagens educativas são exemplos de medidas que podem fazer parte dessa abordagem.

Entre essas ferramentas estão os mecanismos de correspondência por hash, que podem auxiliar na identificação de arquivos anteriormente reconhecidos como ilícitos. O bloqueio de novas tentativas de disponibilização de materiais identificados também pode reduzir a recirculação. A revisão humana em situações de dúvida, acompanhada de registros sobre os critérios utilizados, contribui para aumentar a confiabilidade da moderação e reduzir decisões equivocadas (Frazão, 2022).

A adoção de mecanismos de revisão também se relaciona ao devido processo. Quando uma decisão automatizada ou humana produz consequências relevantes para determinado usuário, a possibilidade de revisão pode contribuir para identificar erros e aperfeiçoar os procedimentos internos. No caso específico de conteúdos ilícitos envolvendo crianças e adolescentes, essa preocupação precisa ser equilibrada com a urgência da proteção da vítima.

Essa distinção também possui importância para a responsabilidade civil. A responsabilização por um conteúdo produzido por terceiro não se confunde necessariamente com a responsabilidade decorrente de uma eventual falha do próprio provedor em cumprir

deveres que estavam sob seu controle. A natureza do serviço, os recursos disponíveis, o conhecimento sobre o risco e a resposta oferecida depois da ciência da situação são elementos que podem ser considerados nessa avaliação. Assim, plataformas que administram feeds, perfis e mecanismos de recomendação possuem possibilidades de intervenção diferentes daquelas existentes para agentes que apenas fornecem conexão à internet (Lima, 2015).

A cooperação com autoridades exige, ainda, atenção à preservação das evidências e à proteção dos dados pessoais. Informações relevantes para uma investigação precisam ser mantidas de forma segura, com controle sobre os acessos e registro das operações realizadas. Ao mesmo tempo, a coleta e o compartilhamento devem observar os limites legais, evitando o tratamento de informações que não sejam necessárias para a finalidade pretendida. A cadeia de custódia assume importância nesse processo porque permite demonstrar como determinada evidência foi obtida, preservada e posteriormente disponibilizada às autoridades. Guias elaborados para orientar a atuação diante de crimes contra a dignidade sexual contribuem para compreender essa relação entre investigação, preservação da prova e proteção de direitos (Ministério Público do Paraná, 2018).

A partir desses elementos, a governança pode ser compreendida como um processo de desenvolvimento contínuo. Em uma estrutura mais básica, a plataforma pode concentrar sua atuação no recebimento de denúncias e na retirada dos conteúdos identificados. Em um estágio mais desenvolvido, pode incorporar prazos definidos, revisão humana, indicadores de desempenho e cooperação estruturada com entidades especializadas. Em

estruturas mais maduras, a avaliação de riscos pode fazer parte do próprio desenvolvimento dos produtos, acompanhada por auditorias, testes periódicos e mecanismos de verificação independente. Essa evolução permite relacionar as medidas adotadas pela empresa com sua capacidade efetiva de prevenção e resposta.

Desse modo, governança, transparência e desenho de produto não devem ser analisados separadamente. As três dimensões se relacionam na construção de um sistema de proteção capaz de responder aos riscos presentes no ambiente digital. Para a discussão da responsabilidade civil, essa estrutura também oferece elementos para avaliar a diligência dos provedores, uma vez que permite verificar quais medidas foram adotadas, como funcionaram e se foram aperfeiçoadas diante de falhas identificadas. No caso de conteúdos ilícitos envolvendo crianças e adolescentes, essa análise contribui para aproximar a proteção jurídica da realidade técnica das plataformas e para compreender em que medida os mecanismos existentes conseguem reduzir a continuidade das violações.

3. METODOLOGIA

A pesquisa foi desenvolvida a partir de uma abordagem qualitativa, de natureza bibliográfica e documental, tendo como objeto de análise a responsabilidade civil de redes sociais e provedores de internet diante da divulgação de conteúdos ilícitos envolvendo crianças e adolescentes no Brasil. A escolha dessa abordagem esteve relacionada à necessidade de compreender, de forma interpretativa, os deveres atribuídos aos provedores, os critérios utilizados para sua responsabilização e as medidas de prevenção, resposta e reparação previstas no ordenamento jurídico. O estudo não envolveu contato

direto com vítimas ou participantes, sendo utilizado exclusivamente material textual de acesso público, proveniente de fontes jurídicas, acadêmicas e institucionais (Brasil, 2024).

O universo da pesquisa foi constituído por documentos relacionados à proteção de crianças e adolescentes no ambiente digital e à responsabilidade dos provedores de internet. Foram considerados, nesse conjunto, normas brasileiras, decisões judiciais, documentos institucionais, trabalhos doutrinários, termos de uso, políticas de segurança e relatórios de transparência disponibilizados publicamente por plataformas digitais. O recorte temporal compreendeu o período de 2014 a 2025, tendo como referência inicial a entrada em vigor do Marco Civil da Internet e, como limite final, mudanças legislativas e discussões recentes relacionadas à proteção infantojuvenil no ambiente digital (Brasil, 2014).

A seleção do material ocorreu mediante levantamento em repositórios oficiais, bases de tribunais e fontes institucionais reconhecidas. Foram utilizadas combinações de termos relacionados ao objeto do estudo, entre eles “criança”, “adolescente”, “provedor”, “responsabilidade civil”, “conteúdo ilícito”, “notice and takedown”, “hash” e “staydown”. Na seleção dos documentos, foram priorizados materiais que apresentassem relação direta com o problema investigado e que permitissem verificar integralmente as informações utilizadas na análise. Documentos incompletos, registros sem identificação de fonte primária e materiais cuja origem não pudesse ser confirmada foram excluídos do corpus (Lima, 2015).

Como instrumentos de coleta e organização das informações, foram utilizados um roteiro de extração normativa e jurisprudencial e uma

ficha de codificação dos documentos de plataformas. O primeiro instrumento permitiu registrar informações como tribunal, identificação do processo, entendimento adotado sobre o dever de agir, circunstância relacionada à responsabilidade do provedor, medida determinada e resultado da decisão. A ficha destinada aos documentos de plataformas contemplou aspectos como existência de canais de denúncia, procedimentos de resposta, mecanismos de identificação ou bloqueio de conteúdos, possibilidade de recurso, preservação de registros e informações sobre transparência. Esses instrumentos foram utilizados para organizar os dados e facilitar a comparação entre diferentes fontes (Supremo Tribunal Federal, 2023).

Durante a coleta, foram registrados os dados necessários para identificação e posterior conferência das fontes, incluindo data de acesso, endereço eletrônico e identificação dos documentos analisados. No caso de decisões judiciais que apresentavam informações relacionadas a situações envolvendo violência sexual contra crianças e adolescentes, foram considerados somente os elementos necessários à compreensão da questão jurídica. Não houve armazenamento ou reprodução de arquivos ilegais, imagens ou qualquer outro material de natureza ilícita. Essa delimitação também contribuiu para preservar a minimização de dados e evitar a exposição desnecessária de informações sensíveis (Ministério Público do Paraná, 2018).

Após a organização do corpus, os dados foram submetidos a uma análise temática e descritiva. Na etapa temática, os conteúdos foram agrupados de acordo com categorias relacionadas ao tipo de provedor, origem do dever de agir, forma de conhecimento da ocorrência, medidas adotadas, mecanismos de prevenção e

resultado da atuação. A análise descritiva permitiu organizar a ocorrência dessas categorias nos diferentes documentos examinados. Em seguida, foi realizada uma triangulação entre legislação, jurisprudência, produção doutrinária e documentos institucionais, buscando identificar aproximações, diferenças e possíveis lacunas na definição dos deveres atribuídos aos provedores (Frazão, 2022).

Para conferir maior consistência ao procedimento de análise, foi realizada uma etapa preliminar de teste dos instrumentos, utilizando um conjunto inicial de decisões judiciais e documentos de plataformas. Essa etapa permitiu verificar a adequação das categorias utilizadas e realizar ajustes antes da análise ampliada do material. Nos casos em que houve dúvida quanto ao enquadramento de determinado documento ou trecho, foi realizada nova leitura do conteúdo, buscando manter critérios uniformes durante a classificação. O registro das decisões metodológicas também contribuiu para tornar mais claro o percurso seguido durante a pesquisa (SaferNet Brasil, 2024).

3.1. Categorias Identificadas na Análise Documental

A análise das normas, decisões judiciais, documentos institucionais e políticas públicas das plataformas permitiu organizar os principais elementos relacionados à responsabilidade dos provedores em cinco categorias analíticas. A organização apresentada no Quadro 1 facilita a visualização dos aspectos encontrados na documentação examinada.

Quadro 1. Categorias de análise identificadas na pesquisa

Categoria analisada	Principais elementos identificados	Relação com a responsabilidade civil
Prevenção	Ferramentas de segurança, mecanismos de detecção, correspondência por hash e medidas de proteção	Permite avaliar a existência de medidas razoáveis para reduzir riscos previsíveis
Notificação e resposta	Canais de denúncia, recebimento de informações, análise e retirada de conteúdos	Permite verificar a conduta adotada após o conhecimento da ocorrência
Preservação de evidências	Registros, metadados, identificadores, documentação das decisões e cadeia de custódia	Contribui para a investigação e para a demonstração da atuação do provedor
Contenção da recirculação	Bloqueio de reuploads, mecanismos de correspondência e monitoramento de novas ocorrências	Reduz a continuidade da exposição e a repetição do dano
Governança e transparência	Políticas internas, registros, relatórios, revisão humana e mecanismos de controle	Permite avaliar a organização, a previsibilidade e a diligência dos procedimentos

Fonte: Elaboração própria (2026).

A organização das categorias demonstra que a responsabilidade dos provedores não está relacionada a uma única etapa da circulação do conteúdo. A prevenção atua antes da ocorrência ou identificação do ilícito, enquanto os mecanismos de notificação e resposta assumem maior importância depois que a plataforma toma conhecimento da situação. A preservação das evidências e a contenção da recirculação, por sua vez, ampliam a análise para além da retirada

inicial, considerando a possibilidade de continuidade da violação. Essa estrutura é compatível com a compreensão de que a atuação dos provedores deve ser analisada conforme suas possibilidades concretas de intervenção e os deveres relacionados à atividade desempenhada (Brasil, 2014; Frazão, 2022).

A análise também evidencia que governança e transparência funcionam como elementos que atravessam as demais categorias. A existência de procedimentos formalizados e registros das decisões permite verificar como determinada ocorrência foi tratada, enquanto mecanismos de revisão podem contribuir para identificar falhas e aperfeiçoar os procedimentos. Dessa forma, os resultados encontrados não indicam apenas a necessidade de retirada de conteúdos, mas uma estrutura mais ampla de prevenção, resposta e acompanhamento das ocorrências.

3.2. Comparação Entre os Diferentes Tipos de Provedores

A análise documental também permitiu identificar diferenças entre os principais tipos de provedores considerados no estudo. Essas diferenças são relevantes porque o grau de controle técnico e operacional sobre o conteúdo varia conforme a função desempenhada no ecossistema digital.

Quadro 2. Relação entre tipo de provedor, possibilidade de intervenção e medidas analisadas

Tipo de provedor	Atuação predominante	Possibilidades de intervenção identificadas	Elementos relevantes para análise da responsabilidade
			e

Provedor de aplicação/plataforma	Gerenciamento de perfis, conteúdos, interações e recomendações	Moderação, retirada, bloqueio de reenvios, canais de denúncia e revisão	Grau de controle, ciência da ocorrência e resposta adotada
Provedor de hospedagem	Armazenamento e disponibilização de arquivos e conteúdos	Identificação de arquivos, retirada e mecanismos de prevenção de novos envios	Controle sobre o conteúdo hospedado e medidas disponíveis
Provedor de acesso	Fornecimento de conexão à internet	Disponibilização de registros nos limites legais e cumprimento de determinações judiciais	Limites técnicos, legais e grau reduzido de controle sobre o conteúdo
Serviços especializados de denúncia/apoio	Recebimento, encaminhamento e tratamento de denúncias	Triagem, encaminhamento, orientação e cooperação institucional	Capacidade de articulação e encaminhamento das ocorrências

Fonte: Elaboração própria (2026).

O Quadro 2 demonstra que os deveres e possibilidades de atuação não podem ser atribuídos de maneira uniforme aos diferentes agentes. As plataformas que administram conteúdos, perfis e sistemas de recomendação apresentam maior capacidade de intervenção direta sobre aquilo que é disponibilizado em seus ambientes. Os serviços de hospedagem também possuem possibilidades específicas relacionadas ao armazenamento dos arquivos, enquanto os provedores de acesso apresentam atuação predominantemente relacionada à conexão e aos registros sujeitos às exigências legais. Essa diferenciação encontra respaldo na literatura sobre responsabilidade dos provedores, que considera a

natureza do serviço e o nível de controle exercido sobre o conteúdo como elementos relevantes para a análise jurídica (Lima, 2015).

A comparação permite observar que a diligência esperada não deve ser medida por um padrão único. Uma ferramenta disponível para uma plataforma de aplicação pode não ser tecnicamente aplicável a um provedor de acesso, assim como uma obrigação relacionada à moderação de conteúdo não pode ser automaticamente transferida para agentes que não possuem controle sobre aquilo que os usuários publicam. A responsabilidade civil, nesse sentido, exige uma análise contextualizada da atividade, das possibilidades concretas de intervenção e da conduta adotada diante da ocorrência.

Os dois quadros, quando analisados conjuntamente, reforçam um dos principais achados da pesquisa: a proteção de crianças e adolescentes no ambiente digital depende da combinação entre prevenção, resposta, preservação de evidências, contenção da recirculação e governança. A literatura e os documentos examinados demonstram que esses elementos se relacionam de maneira diferente conforme o tipo de serviço, razão pela qual a avaliação da responsabilidade civil precisa considerar as características específicas de cada provedor.

Os resultados da análise documental e bibliográfica foram interpretados em diálogo com dados públicos sobre a presença de crianças e adolescentes no ambiente digital. Essas informações foram utilizadas como elemento contextual para compreender a dimensão dos riscos associados à circulação de conteúdos ilícitos e a relevância de mecanismos de prevenção e resposta. Dessa forma, a metodologia permitiu relacionar os fundamentos jurídicos da

responsabilidade civil com as práticas de governança, notificação, retirada, preservação de evidências e prevenção da recirculação de conteúdos envolvendo crianças e adolescentes (CGI.br, 2024).

4. RESULTADOS E DISCUSSÕES OU ANÁLISE DOS DADOS

A análise do material bibliográfico e documental permitiu identificar que a responsabilidade civil de redes sociais e provedores de internet, diante da divulgação de conteúdos ilícitos envolvendo crianças e adolescentes, está relacionada principalmente à capacidade de prevenção, identificação, resposta e contenção da continuidade da violação. A análise das normas, decisões judiciais e documentos institucionais demonstrou que a proteção não se limita à retirada de determinado conteúdo, uma vez que a possibilidade de cópias, novos compartilhamentos e reuploads amplia a duração e o alcance dos danos. Nesse contexto, os mecanismos de governança e de resposta das plataformas passam a ter relevância para a avaliação de sua conduta (Brasil, 2014; Frazão, 2022).

Um dos principais resultados encontrados foi a existência de diferentes níveis de atuação entre os provedores. A análise demonstrou que não é adequado atribuir os mesmos deveres a todos os agentes que participam do funcionamento da internet. Provedores responsáveis por aplicações, perfis, sistemas de recomendação e distribuição de conteúdo possuem possibilidades de intervenção diferentes daquelas encontradas em serviços de hospedagem ou de acesso. Essa distinção interfere diretamente na avaliação da responsabilidade, pois o grau de controle técnico e operacional sobre determinada atividade constitui um dos elementos que podem ser considerados na análise da diligência esperada (Lima, 2015).

Outro resultado identificado refere-se à importância da ciência sobre a existência do conteúdo ilícito. A documentação analisada indica que a existência de mecanismos adequados para recebimento e processamento de denúncias possui relevância tanto para a proteção da vítima quanto para a posterior avaliação da conduta do provedor. A partir da ciência de uma ocorrência, tornam-se relevantes o registro da comunicação, a análise do conteúdo denunciado, a adoção das providências cabíveis e a preservação das informações necessárias à investigação. Essa compreensão aproxima a discussão sobre responsabilidade civil da necessidade de demonstrar concretamente como o provedor atuou diante de determinada situação (Brasil, 2014).

A análise também evidenciou a importância da preservação de provas. Em situações envolvendo conteúdos ilícitos de natureza sexual, a retirada do material não elimina necessariamente a necessidade de preservar informações relacionadas ao fato, especialmente quando essas informações podem contribuir para a identificação dos responsáveis ou para a reconstrução dos acontecimentos. Registros técnicos, identificadores e demais elementos disponíveis devem ser tratados de acordo com as exigências legais e com a proteção dos dados pessoais. A literatura institucional analisada reforça que a preservação adequada das evidências pode contribuir para a continuidade das investigações sem exigir a reprodução ou circulação desnecessária do material ilícito (Ministério Público do Paraná, 2018).

Outro aspecto relevante encontrado na pesquisa foi o papel dos mecanismos tecnológicos de prevenção da recirculação. Recursos baseados em correspondência por hash podem auxiliar na identificação de arquivos previamente reconhecidos, dificultando

novos envios do mesmo material. Entretanto, a análise da literatura demonstrou que a utilização de sistemas automatizados não deve ser compreendida como solução isolada. A possibilidade de erros de classificação torna importante a existência de mecanismos de revisão humana, especialmente em situações nas quais a decisão automatizada possa produzir consequências relevantes. Dessa forma, a tecnologia pode ampliar a capacidade de resposta das plataformas, mas não elimina a necessidade de governança e supervisão (Frazão, 2022).

A discussão sobre esses mecanismos também se relaciona à transparência. Os documentos analisados indicam que relatórios e políticas internas podem fornecer informações importantes sobre os procedimentos adotados pelas plataformas, mas sua utilidade depende da qualidade e da clareza dos dados apresentados. Informações sobre canais de denúncia, procedimentos de moderação, mecanismos de bloqueio e possibilidades de recurso permitem compreender melhor como cada serviço organiza sua resposta.

Os resultados encontrados também apontaram para a relevância da cooperação entre plataformas, autoridades públicas e organizações especializadas. A atuação de entidades voltadas ao recebimento e encaminhamento de denúncias pode facilitar a identificação de ocorrências e contribuir para o direcionamento adequado dos casos. Da mesma forma, a cooperação com autoridades pode favorecer a preservação e o fornecimento de informações necessárias às investigações, respeitando os procedimentos legais aplicáveis. Dados e relatórios produzidos por organizações como a SaferNet Brasil demonstram a importância de estruturas especializadas no

enfrentamento das violações praticadas no ambiente digital (SaferNet Brasil, 2024).

No que se refere à prevenção, a pesquisa identificou uma aproximação crescente entre proteção infantojuvenil e desenho dos próprios produtos digitais. Recursos de denúncia acessíveis, configurações de privacidade, mecanismos de identificação de riscos, sistemas de detecção de conteúdos previamente identificados e medidas voltadas à redução de contatos inadequados podem ser incorporados às plataformas desde sua concepção. Essa perspectiva desloca parte da discussão de uma lógica exclusivamente reativa para uma abordagem que considera a prevenção como componente da própria arquitetura dos serviços digitais. A presença cada vez maior de crianças e adolescentes na internet reforça a relevância desse debate (CGI.br, 2024).

A análise dos documentos jurídicos e da literatura também permitiu observar que a responsabilização civil não decorre simplesmente da existência de um conteúdo ilícito dentro de determinado serviço. Essa compreensão é particularmente importante para evitar uma responsabilização automática das plataformas, ao mesmo tempo em que permite reconhecer situações nas quais uma eventual omissão pode assumir relevância jurídica (Brasil, 2014; Lima, 2015).

Outro ponto identificado foi a relação entre prevenção, resposta e reparação. A reparação dos danos não deve ser analisada apenas sob a perspectiva da compensação financeira, especialmente quando a permanência ou recirculação do conteúdo contribui para prolongar a violação. Nesse sentido, a tutela inibitória e outras medidas destinadas a impedir a continuidade da conduta podem

complementar a discussão sobre indenização, dependendo das circunstâncias do caso (Frazão, 2022).

A análise conjunta dos resultados demonstra, ainda, que a diligência dos provedores deve ser avaliada a partir de múltiplos fatores. Não se trata apenas de verificar se determinada plataforma possui uma ferramenta de denúncia ou utiliza determinada tecnologia, mas de observar como esses mecanismos funcionam diante de situações concretas. A existência de políticas internas, recursos técnicos e canais de comunicação ganha maior significado quando acompanhada de capacidade efetiva de implementação, monitoramento e correção de falhas.

Os achados indicam que os desafios relacionados à proteção de crianças e adolescentes no ambiente digital não podem ser solucionados exclusivamente por uma medida jurídica ou tecnológica. A efetividade da proteção depende da combinação entre normas, atuação judicial, governança das plataformas, mecanismos de prevenção, preservação de evidências, transparência e cooperação institucional. A literatura analisada converge para a necessidade de aprimoramento contínuo desses mecanismos, especialmente diante das transformações dos serviços digitais e da ampliação da participação de crianças e adolescentes nesses espaços (Brasil, 2023; CGI.br, 2024).

Os resultados obtidos, dessa maneira, sustentam a compreensão de que a responsabilidade civil dos provedores deve ser examinada de forma contextualizada, considerando tanto os limites técnicos e jurídicos de cada serviço quanto as possibilidades concretas de prevenção e resposta. A discussão realizada evidencia que a proteção infantojuvenil no ambiente digital exige mecanismos

capazes não apenas de reagir às denúncias, mas também de reduzir a recirculação dos conteúdos, preservar elementos probatórios e aperfeiçoar continuamente as estruturas de segurança. Esses achados constituem a base para as considerações finais do estudo.

5. CONCLUSÃO

A pesquisa conclui que a responsabilidade civil das redes sociais e dos provedores de internet diante da divulgação de conteúdos ilícitos envolvendo crianças e adolescentes depende da análise concreta da atuação de cada provedor, considerando a natureza do serviço, o grau de controle sobre o conteúdo, a possibilidade de intervenção e a conduta adotada diante do conhecimento da ocorrência.

O objetivo geral é atingido ao demonstrar que a responsabilização civil não decorre simplesmente da presença de conteúdo ilícito em determinado ambiente digital. Ela está relacionada à existência de deveres compatíveis com a atividade exercida e à capacidade concreta de prevenção, resposta e contenção da continuidade da violação. Dessa forma, a análise da conduta do provedor ocupa posição central para a definição de eventual responsabilidade.

A pesquisa também demonstra que a proteção de crianças e adolescentes no ambiente digital exige uma compreensão que ultrapassa a retirada isolada de conteúdos. A prevenção da recirculação, a preservação de evidências, a existência de mecanismos adequados de denúncia e a adoção de procedimentos de revisão integram uma estrutura mais ampla de proteção. Esses elementos contribuem para tornar a atuação das plataformas mais verificável e compatível com a gravidade das violações analisadas.

Como contribuição, o estudo aproxima a discussão jurídica sobre responsabilidade civil dos mecanismos técnicos e organizacionais utilizados pelas plataformas digitais. Essa aproximação permite compreender que a avaliação da diligência não depende de um único recurso, mas da relação entre os instrumentos disponíveis, os riscos envolvidos e a capacidade efetiva de atuação do provedor.

Conclui-se, ainda, que a proteção infantojuvenil no ambiente digital constitui responsabilidade que envolve diferentes atores e requer articulação entre instrumentos jurídicos, tecnológicos e institucionais. A atuação das plataformas possui papel relevante nesse processo, mas não substitui a função das autoridades públicas, do sistema de justiça e das instituições especializadas na proteção de crianças e adolescentes.

A principal limitação do estudo está relacionada ao caráter bibliográfico e documental da pesquisa, que não permite observar diretamente o funcionamento interno das plataformas ou mensurar, em ambiente real, a efetividade dos mecanismos analisados. Estudos futuros podem ampliar essa investigação por meio de análises comparativas entre plataformas, acompanhamento de decisões judiciais e avaliação empírica dos mecanismos de prevenção e resposta utilizados no ambiente digital.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Constituição (1988). **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: 7 set. 2026.

BRASIL. **Decreto nº 12.880, de 18 de março de 2026.** Regulamenta a Lei nº 15.211, de 17 de setembro de 2025, que dispõe sobre a proteção de crianças e adolescentes em ambientes digitais, e institui a Política Nacional de Promoção e Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital. Brasília, DF: Presidência da República, 2026. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12880.htm. Acesso em: 7 set. 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 17 set. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 7 set. 2026.

BRASIL. **Lei nº 13.718, de 24 de setembro de 2018.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941. Brasília, DF: Presidência da República,

2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13718.htm. Acesso em: 7 set. 2026.

BRASIL. **Lei nº 15.211, de 17 de setembro de 2025.** Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm. Acesso em: 7 out. 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, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 27 set. 2026.

CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil.** 15. ed. São Paulo: Atlas, 2020.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br); CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO (Cetic.br). **Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2023.** São Paulo: Comitê Gestor da Internet no Brasil, 2024. Disponível em: https://www.cetic.br/media/docs/publicacoes/2/20241104103339/tic_kids_online_2023_livro_eletronico.pdf. Acesso em: 18 set. 2026.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Protocolo para julgamento com perspectiva de proteção integral de crianças e adolescentes.** Brasília, DF: CNJ, 2022.

DINIZ, Maria Helena. **Curso de direito civil brasileiro: responsabilidade civil**. 34. ed. São Paulo: Saraiva, 2021.

DONEDA, Danilo; MENDES, Laura Schertel. **Privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2021.

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. 2022. Disponível em: https://professoraanafraza.com.br/files/publicacoes/2022-02-24-Responsabilidade_civil_de_provedores_de_aplicacoes_por_conteudo_s_de_terceiros_O_art_19_do_Marco_Civil_nao_e_nem_pode_ser_a_unica_referencia_normativa_para_o_assunto.pdf. Acesso em: 7 set. 2026.

INTERPOL. **International guidelines on child sexual exploitation material**. Lyon: Interpol, 2021.

KAYE, David. **Speech police**: the global struggle to govern the Internet. New York: Columbia Global Reports, 2020.

LIMA, Cíntia Rosa Pereira de. A responsabilidade civil dos provedores de aplicação de internet por conteúdo gerado por terceiro antes e depois do Marco Civil da Internet (Lei nº 12.965/14). **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 110, p. 155-176, jan./dez. 2015. Disponível em: <https://revistas.usp.br/rfdusp/article/view/115489>. Acesso em: 2 out. 2026.

MARTINS, Guilherme Magalhães. **Direito digital e responsabilidade civil**. Belo Horizonte: Fórum, 2020.

MENDES, Laura Schertel. **Direito civil na era digital**. São Paulo: Revista dos Tribunais, 2020.

MINISTÉRIO PÚBLICO DO PARANÁ. **Lei nº 13.718/2018: mudanças nos crimes contra dignidade sexual**. Curitiba: Ministério Público do Paraná, 2018. Disponível em: https://site.mppr.mp.br/sites/hotsites/arquivos_restritos/files/migrados/File/Estudo_Lei_13718_2018_Mudancas_nos_Crimes_Sexuais_versao_final_2.pdf. Acesso em: 10 set. 2026.

RODRIGUES, Sérgio Victor de Almeida; MELO, Daniela de Castro. Prevenção aos crimes sexuais praticados contra crianças e adolescentes na internet: estratégias e desafios no contexto brasileiro. **Revista Avante**, Belo Horizonte, v. 1, n. 8, 2025. DOI: <https://doi.org/10.70365/2764-0779.2025.128>.

SAFERNET BRASIL. **Central Nacional de Denúncias**: relatório 2024. São Paulo: SaferNet Brasil, 2024. Disponível em: https://new.safernet.org.br/sites/default/files/content_files/safernet_-_central_nacional_de_denuncias_2024.pdf. Acesso em: 21 set. 2026.

SAFERNET BRASIL. **Relatório anual 2021**. São Paulo: SaferNet Brasil, 2021. Disponível em: <https://www.safernet.org.br>. Acesso em: 25 set. 2026.

SANTOS, Plinyo Paccioly Rodrigues. Estatuto Digital da Criança e do Adolescente: desafios regulatórios e de fiscalização. **Revista Ibero-Americana de Humanidades, Ciências e Educação (REASE)**, São Paulo, v. 11, n. 10, p. 427-441, out. 2025. DOI: <https://doi.org/10.51891/rease.v11i10.20972>.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Direito, Internet e sociedade**. Rio de Janeiro: FGV, 2022.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **Recurso Especial nº 1.785.092/SP**. Relatora: Ministra Nancy Andrighi. Quarta Turma. Julgado em: 15 fev. 2022. Brasília, DF: Superior Tribunal de Justiça, 2022.

SUPREMO TRIBUNAL FEDERAL (STF). **Ação Direta de Inconstitucionalidade nº 5.527**. Relator: Ministro Dias Toffoli. Julgado em: 7 jun. 2023. Brasília, DF: Supremo Tribunal Federal, 2023.

SUPREMO TRIBUNAL FEDERAL (STF). **Responsabilização civil de provedores por conteúdo ilícito gerado por terceiros**: bibliografia selecionada. Brasília, DF: Supremo Tribunal Federal, 2023. Disponível em:

https://www.stf.jus.br/arquivo/cms/bibliotecaConsultaProdutoBibliotecaBibliografia/anexo/Responsabilizacao_civil_2.pdf. Acesso em: 1 out. 2026.

ZANATTA, Rafael A. F.; MONTEIRO, Felipe. **Regulação de plataformas digitais**. São Paulo: JOTA, 2021.

¹ Discente do Curso Superior de Direito do Centro Universitário Santa Terezinha – CEST. E-mail: [acesse o artigo original para visualizar o e-mail](#)

² Especialista em Docência do Ensino Superior pela Faculdade Cândido Mendes, Bacharela em Direito pela Universidade Federal do Maranhão, Licenciada em Letras pela Universidade Federal do Maranhão, advogada, servidora pública da Rede Estadual do

Maranhão e Professora do Centro Universitário Santa Terezinha-
CEST. E-mail: [acesse o artigo original para visualizar o e-mail](#)

³ Coorientadora Profa. Dra. em Linguística e Língua Portuguesa. E-
mail: [acesse o artigo original para visualizar o e-mail](#)