OMISSÃO TECNOLÓGICA E RESPONSABILIDADE JURÍDICA: AS PLATAFORMAS DE CONTEÚDO ADULTO FRENTE À EXPLORAÇÃO SEXUAL DE MENORES

Danielle Alves Fonseca[1]
Estefane Paula Xavier Silva[2]
Maxilene Soares Correa[3]

RESUMO
O presente trabalho analisa a responsabilidade jurídica das plataformas de conteúdo adulto frente à exploração sexual de menores no ambiente digital, destacando a intensificação dessas violações com o avanço tecnológico. A pesquisa busca compreender como se configura a responsabilização dessas plataformas em casos de conteúdos ilícitos envolvendo menores. Adota-se metodologia bibliográfica, com abordagem qualitativa, baseada em doutrina, legislação e jurisprudência. Verificou-se que os elementos da responsabilidade civil sofrem adaptações no ambiente digital, permitindo a responsabilização por condutas diretas e omissões, especialmente diante da ciência da ilicitude e da ausência de medidas eficazes de remoção. No âmbito penal, admite-se a responsabilização de gestores em casos de omissão relevante. Conclui-se que a proteção de crianças e adolescentes exige abordagem ampliada, com medidas preventivas, desenvolvimento tecnológico e atuação conjunta entre Estado, plataformas e sociedade civil.

PALAVRAS-CHAVE: Responsabilização de plataformas digitais; Exploração sexual de crianças e adolescentes; Conteúdo ilícito online; Marco Civil da Internet; Direito digital.

INTRODUÇÃO

O avanço das tecnologias digitais e o crescimento exponencial das interações no ambiente virtual transformaram significativamente as relações sociais e os modos de comunicação contemporâneos. A internet, enquanto espaço dinâmico de circulação de informações, tem permitido novas formas de expressão e compartilhamentos de conteúdos, mas também potencializado práticas ilícitas que afetam direitos fundamentais. Nesse cenário, destaca-se a preocupante exploração sexual de crianças e adolescentes, que tem encontrado nas plataformas digitais um ambiente propício para a disseminação de conteúdos ilícitos e para a perpetuação de danos psicológicos e morais às vítimas.

Entre plataformas que mais suscitam debates ético-jurídicos estão as de conteúdo adulto, que, embora operem sob a alegação de liberdade de expressão e autonomia dos usuários, frequentemente se tornam meio de veiculação de posts não autorizados, inclusive envolvendo menores de idade. A ausência de fiscalização eficiente e a omissão tecnológica na remoção de materiais ilegais reforçam a necessidade de discutir a responsabilidade jurídica dessas plataformas e de seus gestores diante da vulnerabilização de crianças e adolescentes.

[1] Aluna do curso de Direito da Faculdade Evangélica Raízes. Email: danielledireito7@gmail.com
[2] Aluna do curso de Direito da Faculdade Evangélica Raízes. Email: estefanepaula113@gmail.com
[3] Docente da Faculdade Evangélica Raízes, onde coordena o curso de Direito. Mestre em Direito pela Universidade de Coimbra. Doutoranda em Direito Constitucional pelo Instituto Brasileiro de Desenvolvimento e Pesquisa – IDP – Brasília. Email: maxilene.correa@faculdaderaizes.edu.br

Tal debate é fundamental em um contexto em que as fronteiras entre liberdade e violação de direitos tornam-se cada vez mais tênues, exigindo do Direito uma atuação compatível com os desafios da era digital.

A partir deste contexto, a pesquisa procura responder a seguinte problemática: como se configura a responsabilidade jurídica das plataformas de conteúdo adulto frente à exploração sexual de menores? Essa investigação se justifica diante do aumento alarmante de casos de exploração sexual infantil no ambiente virtual, sendo impulsionado pela expansão das tecnologias digitais e pelo uso massivo das redes sociais. Crianças e adolescentes, em situação de vulnerabilidade, têm sidos expostos a riscos graves, muitas vezes sem que os mecanismos de fiscalização acompanhem a velocidade da disseminação digital. Nesse contexto, torna-se indispensável analisar a atuação do ordenamento jurídico na prevenção e repressão dessas práticas, identificando lacunas, desafios e possíveis soluções para proteger os direitos fundamentais das vítimas.

Para alcançar seus objetivos, esta pesquisa se dará através de metodologia bibliográfica, analisando dados e conceitos trazidos de livros, artigos científicos, relatórios públicos e outros documentos, sendo abordados de modo qualitativo. A pesquisa será analítica, uma vez que busca analisar a legislação nacional penal e civil acerca de suas responsabilidades jurídicas a partir do viés da exploração sexual na internet.

Para que se cumpra seus objetivos, a pesquisa se iniciará levantando-se descritivamente dos requisitos para a responsabilidade civil e criminal da internet. Posteriormente, de forma dedutiva, a pesquisa buscará aplicar os elementos civis e criminais às plataformas de conteúdo adulto, gestores e usuários, especialmente no que tange posts não autorizados ou envolvendo crianças e adolescente, analisando especificamente seu objeto.

Por fim, a estrutura deste trabalho está organizada em três partes principais, além desta introdução e da conclusão. Na primeira parte, será abordada a responsabilização jurídica na era digital, com ênfase na aplicação da legislação civil e penal no ambiente virtual. A segunda parte analisa a responsabilidade civil e criminal das plataformas, gestores e usuários de conteúdo adulto, especialmente em situações de posts não autorizados ou que envolvam crianças e adolescentes.

Já a terceira parte discute os impasses tecnológicos e jurídicos que dificultam a efetiva responsabilização das plataformas e o combate à exploração sexual de menores. Por fim, a conclusão apresentará as considerações finais, sintetizando os resultados obtidos e apontando

caminhos para o fortalecimento da tutela jurídica dos direitos das crianças e adolescentes na internet.

1. RESPONSABILIDADE JURIDICA NA ERA DIGITAL: A LEI CIVIL E PENAL NO AMBIENTE VIRTUAL

A expansão das interações no ambiente digital trouxe novos desafios para a compreensão dos institutos tradicionais da responsabilidade civil. A circulação veloz de informações, a permanência de conteúdos e a atuação de múltiplos intermediários intensificam tanto a possibilidade de dano quanto a complexidade na análise do nexo causal. Nesse contexto, torna-se essencial revisitar conceitos fundamentais — como conduta, dano e causalidade — para compreender como eles se comportam diante de um cenário tecnológico marcado pela instantaneidade e pela dificuldade de controle.

Da mesma forma, esse panorama de crescente digitalização também exige que outras áreas do Direito, como o Direito Penal, reavaliem seus parâmetros de imputação e resposta estatal. A lógica que orientava a responsabilização no mundo físico não se aplica automaticamente aos espaços virtuais, sendo necessário adaptar fundamentos dogmáticos e examinar novas formas de conduta ilícita mediadas por tecnologias e plataformas digitais. Assim, os debates sobre responsabilidade civil e penal se conectam ao evidenciar a necessidade de interpretação jurídica compatível com a realidade digital contemporânea.

1.1. Responsabilização Jurídica Na Era Digital: A Lei Civil No Ambiente Virtual.

Atualmente, a sociedade está vivenciando mudanças profundas, uma vez que a internet se estabeleceu como um canal fundamental de comunicação, ampliando as interações entre pessoas à medida que o processo comunicativo avança. O ambiente virtual serve como um espaço de convivência e expressão das ideias e comunicações humanas; no entanto, também representa um terreno onde ocorrem violações dos direitos humanos, cujos impactos podem ser significativos no contexto atual. Portanto, o Direito Civil precisa se adaptar ao novo ambiente social para que um quadro constitucional funcione efetivamente devido à forma como tais instituições de responsabilidade protegem a dignidade humana.

Existem princípios fundamentais que definem o conceito de responsabilidade civil no sistema jurídico brasileiro, e esse equilíbrio é restaurado quando uma pessoa causa danos a outra. O princípio da reparação integral é um deles, pois visa que a vítima recupere danos morais e materiais para não perder, especialmente na presença da proliferação generalizada e

contínua de conteúdo no ambiente virtual. O princípio da solidariedade, em grande parte, ajuda os atores sociais (no caso das plataformas digitais) a fazerem um bom e até melhor trabalho juntos para prevenir e mitigar danos (Schreiber, 2022).

O princípio da função social também enfatiza que a responsabilidade civil tem uma natureza preventiva e pedagógica, direcionando e desencorajando atos ou comportamentos inadequados. E enquanto os danos podem fazer você pagar ou perder algo, a responsabilidade civil precisa continuar a defender a dignidade humana e garantir um comportamento ético, pois não é mais essencial nos ambientes digitais (Cavalieri Filho, 2021). Por fim, a articulação desses princípios permite que o Direito Civil atue de modo mais eficaz perante as violações que são evidenciadas na era tecnológica.

No entanto, com o surgimento das interações digitais e o aumento considerável das complexidades dos relacionamentos no meio digital, tornou-se necessário ampliar a compreensão tradicional dos elementos da responsabilidade civil — ação ou omissão, culpa ou dolo, dano e nexo causal — para abarcar condutas omissivas tecnológicas e situações em que o dano decorre da inércia ou negligência de intermediários digitais.

Nesse cenário, quando a conduta ou a ausência de uma participação das plataformas digitais violam uma exigência legal e causa danos, surge o dever de responsabilização. Nesse sentido, o papel da omissão desempenha total relevância, visto que os operadores dessas plataformas possuem capacidade técnica para interromper o ato prejudicial, contudo, impossibilita sua prevenção e detenção.

Como observado por Cavalieri Filho (2021), a omissão deve equivaler-se a uma quebra do dever de cuidado, pois se torna eticamente condenável a ação quando existe uma obrigação de agir. Nesse sentido, considera-se o subjetivo. A intenção (se há intenção deliberada) ou a negligência (descuido, imprudência ou falta de habilidade) são consideradas. Schreiber (2022) leva essa ideia adiante quando introduz a "negligência algorítmica", onde a moderação ou os controles automatizados falham e o conteúdo prejudicial continua a circular, uma violação do dever de vigilância, apesar de não haver intenção direta.

A partir dessa compreensão, o dano, como demonstra Diniz (2023), é o prejuízo efetivo a um direito legal — material ou moral, sendo este último especialmente agravado no ambiente digital devido à fácil disseminação e permanência de informações ofensivas, o que amplifica o sofrimento psicológico e seus efeitos duradouros. Deve haver também uma conexão causal, ou seja, a demonstração de que a conduta — ativa ou omissiva — foi decisiva para o dano, como aponta Cavalieri Filho (2021), para que haja responsabilidade. Neste

cenário virtual, essa análise é ainda mais complicada pelo fato de existirem intermediários que podem ajudar a facilitar a transmissão do dano, mas isso por si só não rompe a relação causal que serve para sustentar o dever de reparação.

Diante dessas particularidades, a responsabilidade civil pode surgir tanto de uma ação quanto de uma omissão negligente, que se caracteriza quando o agente, tendo o dever legal de agir, se abstém de fazê-lo. Em ambientes virtuais, essa omissão é frequentemente observada em plataformas digitais e redes sociais que, mesmo quando notificadas sobre a existência de conteúdo ilícito, demoram a removê-lo ou falham completamente em agir diante de violações de direitos. Esse tipo de comportamento se classifica como "omissão tecnológica", um conceito da doutrina jurídica contemporânea que descreve uma forma de negligência própria da era digital, caracterizada pela falta de mecanismos eficazes para controle, moderação e prevenção (Filho, 2024).

O Marco Civil da Internet (Lei nº 12.965/2014) representa um avanço significativo na regulamentação, estabelecendo diretrizes e obrigações sobre o uso responsável da internet. O artigo 19 dessa legislação estabelece que os provedores de aplicações—ou seja, as empresas que oferecem serviços e funcionalidades online—podem ser responsabilizados por danos decorrentes do conteúdo gerado por terceiros em casos de descumprimento de ordens judiciais, mesmo que não adotem medidas para remover o material em questão e, consequentemente, causem prejuízos a outros. Este não é um grande exemplo de liberdade de expressão versus provedores de serviços, pois a lei acima não é totalmente apoiada pelos estudos, já que em um caso flagrante de compartilhamento de fotos privadas (por exemplo, no caso de menores), é necessário ter a ordem judicial prévia.

De acordo com a lei brasileira, as plataformas devem reagir prontamente sempre que tiverem certeza de que viram algum conteúdo ilegal. Isso levou a um julgamento pelo Superior Tribunal de Justiça, que declarou que a falha em remover o conteúdo ofensivo após notificação constitui uma falha na prestação de serviço e leva à responsabilidade civil, mas o autor deve recorrer ao tribunal. Assim como os casos REsp 1.660.168/RS e REsp 1.771.866/SP mostram, o problema deve ser resolvido imediatamente, por qualquer meio necessário, ou devemos sofrer os danos resultantes a curto prazo, já que esse conteúdo não desaparece tão imediatamente.

De acordo com essa mesma linha interpretativa, o Supremo Tribunal Federal concordou com o Tema 987 (RE 1.037.396), de modo que as plataformas têm um dever de cuidado. Desse modo, não se pode depender estritamente de uma ordem judicial quando se

aborda graves violações aos direitos fundamentais. Para o Tribunal, conteúdos notoriamente ilegais (como discurso de ódio, incitação à violência ou exploração sexual) devem ser removidos de forma autônoma, sob pena de responsabilidade. Tais entendimentos demonstram como a responsabilidade civil tem se deslocado, em uma plataforma digital em direção aos valores constitucionais — em especial ao da dignidade humana e a preservação da honra e imagem.

À luz dessas premissas, uma plataforma digital também pode estar sujeita a responsabilidade civil em certas circunstâncias com base em sua conduta e na medida em que ativamente mantém ou perpetua o dano causado. A primeira é a responsabilidade subjetiva por omissão, que ocorre quando a plataforma, mesmo sabendo que seu conteúdo era ilegal, não o remove ou é negligente no atraso da ação.

Cavalieri Filho (2024) explica que a omissão se torna juridicamente relevante quando um agente tem o dever de agir e se abstém de fazê-lo, contribuindo para a perpetuação do dano. Além disso, há a responsabilidade objetiva pelo risco da atividade — que se aplica a empresas que lucram com a circulação de conteúdo produzido por terceiros. Segundo Anderson Schreiber (2022), as plataformas de redes sociais e de compartilhamento de vídeos lucram economicamente com o engajamento dos usuários devido à exposição ao risco (seja o conteúdo legal ou não).

Continuamente a isso, a responsabilidade civil pode assumir uma natureza solidária em casos em que o provedor obtém vantagem econômica direta ou indireta com a disseminação de material ofensivo ou quando sua estrutura tecnológica impede a identificação do autor direto do dano.

Bioni (2021) afirma que essa solidariedade surge da função social da empresa digital, segundo a qual aqueles que se beneficiam da atividade devem também arcar com os riscos dela decorrentes. Essa lógica está diretamente relacionada ao princípio da reparação integral, conforme explicado por Diniz (2023), que afirma que a vítima deve ser restituída, tanto quanto possível, ao estado anterior à lesão. Desse modo, a responsabilidade das plataformas no ambiente virtual é construída a partir de uma combinação de fundamentos doutrinários e da necessidade de proteção efetiva dos direitos da personalidade na era digital.

No que se refere às consequências jurídicas dessas violações, o dano moral no ambiente virtual é uma das principais consequências de condutas ilícitas. Ele se manifesta em dor, humilhação e sofrimento psicológico resultantes de exposição indevida ou ataques à reputação. A velocidade de propagação e a dificuldade de controle tornam a lesão mais grave

e duradoura. Como observa Diniz (2023), o dano moral digital tem uma natureza difusa e afeta não apenas o indivíduo, mas também sua integração social e profissional. Assim, a determinação do valor da indenização deve considerar não apenas a compensação individual, mas também o caráter preventivo e educativo da medida.

De modo complementar, o dano material é definido como perda econômica concreta, incluindo perda de oportunidades, quebra de contratos, uso indevido de imagem comercial ou apropriação de dados pessoais. Para quantificar esses danos, é necessário pensar nesses danos de forma analítica, de acordo com o nível de perda e as consequências financeiras para a vítima. Nesse sentido, ambos os tipos de dano exigem que o Judiciário seja sensível e adaptável às peculiaridades do ambiente digital, que não permite soluções uniformes ou rígidas.

Diante de todo o exposto, a responsabilidade civil na era digital desempenha um papel essencial na construção de um ambiente virtual mais seguro e ético. Esse dever de indenizar não é apenas uma exigência legal, mas também um compromisso social para restaurar a confiança nas relações digitais e garantir que a inovação tecnológica caminhe lado a lado com a proteção dos seres humanos.

A internet, como espaço de liberdade, também não pode se tornar um território de impunidade. Assim, é dever do Direito Civil estabelecer parâmetros claros para a reparação de danos e para a responsabilização de agentes que, por ação ou omissão, contribuem para a violação de direitos pessoais.

Por conseguinte, pode-se argumentar que o conceito de responsabilidade civil no mundo virtual deve ser interpretado de forma ampla, incorporando considerações constitucionais, função social e o dever de prevenção. A omissão tecnológica e a inércia diante de violações de direitos não podem ser toleradas em um estado construído sobre a dignidade da pessoa humana. Por essa razão, a proteção civil deve se transformar para fazer mais do que a reparação de danos; deve forjar um novo espaço digital mais justo e solidário, sobre o qual serão construídos os aspectos mais fundamentais da convivência humana, nas quais são criadas fundações normativas que contribuem para uma proteção eficaz dos direitos fundamentais em um ambiente virtual.

No entanto, a complexidade das dinâmicas digitais, manifestada a descentralização das ações, a volatilidade das evidências e a prevalência do anonimato dos agentes, indica que mesmo a proteção civil é insuficiente para enfrentar os desafios legais relacionados ao crime na rede.

A dificuldade de identificar os perpetradores e suas práticas sofisticadas está no cerne desta problemática, deste problema e sua resposta reside em um estudo mais aprofundado e como os conceitos de atribuição legal podem ser comprometidos no ciberespaço. Portanto, é importante perguntar como o anonimato digital lança nova luz sobre as fundações conceituais estabelecidas para autoria e responsabilidade criminal e explorar estruturas conceituais dogmáticas de atribuição legal em risco no contexto do crime digital.

1.2. Entre anonimato e imputação penal: desafios dogmáticos da criminalidade na era digital

No seu início, a internet foi saudada como um paradigma de liberdade, uma zona imune ao olhar curioso das autoridades públicas, um espaço onde os usuários da internet poderiam exercer um poder de ação ilimitado que se estendia a todos os cantos do planeta. A propriedade intelectual deveria ser compartilhada, e a privacidade seria garantida, com a comunicação mantida anônima. Não obstante esse libertário inicial, toda essa evolução intelectual também trouxe problemas que testam os limites de toda essa liberdade.

Devido a esse contexto de transformação social e tecnológica que se observa diante da análise jurídica desse fenômeno, o Direito Penal estudou apenas condutas físicas ocorrendo em espaços definidos e com autoria aparente. Sob essa perspectiva, a responsabilidade criminal envolvia atribuir responsabilidade individual a uma pessoa pelas consequências legais de uma conduta típica, ilícita e culpável.

Ademais, pela tradição típica, tal imputação era construída com base na constatação dos atos humanos e seus aspectos subjetivos, além da definição e verificação de um contexto fático definido e verificável. Ocorre que, para dar conta do desenvolvimento tecnológico e do crescimento desenfreado da migração das relações sociais para ambientes virtuais, a estrutura clássica também foi desafiada, à medida que a autoria, a materialidade e a dinâmica da conduta se tornaram mais difusas, anônimas e tecnicamente mais complexas.

Diante desse abalo nos paradigmas tradicionais de imputação, a teoria da sociedade de risco criada por Urich Beck (1986) apresentou um quadro interpretativo significativo. Em virtude dessa perspectiva teórica, a modernidade cria riscos globalizados e insensíveis que são difíceis de atribuir a um único agente, um fenômeno que se intensifica no ciberespaço. Nesse sentido, crimes cometidos virtualmente trazem à tona deficiências do modelo clássico de responsabilidade criminal, de modo que uma recomposição dogmática pode ser necessária para lidar com ameaças emergentes e novas incertezas trazidas pela sociedade tecnológica.

Por conseguinte, dadas essas mudanças estruturais e a necessidade de desenvolver e modernizar esses marcos legislativos, elas são seguidas por medidas legislativas que respondem à complexidade na vanguarda do espaço virtual.

Como expressão concreta desse movimento de atualização normativa, principal foco do Brasil foi a necessidade de normas contra a criminalização de condutas típicas em ambientes virtuais. A Lei Carolina Dieckmann (Lei nº 12.737/2012), reconheceu que invasões de dispositivos, captura de dados e violações de dados e mecanismos de segurança podem causar danos a bens jurídicos relevantes. Tal lei representou uma mudança altamente significativa no Direito Penal, pois ampliou a noção desatualizada de inviolabilidade de dados, reforçando ainda mais a ideia de que a privacidade digital é uma extensão da intimidade, concedendo maior proteção penal a essas informações pessoais.

Por outro lado, sob tais circunstâncias, a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD) mencionada no parágrafo anterior (que por si só não é uma lei penal), teve um grande impacto no Direito Penal: estabeleceu as regras para o manuseio, armazenamento e compartilhamento de dados pessoais no governo. Desde que foi promulgada, o uso indevido de informações tornou-se a grande questão, e a comercialização ilegal e/ou aquisição abusiva dessas informações recebeu maior atenção.

Desse modo, efeito nas normas do Direito Penal é perceptível em duas direções – (1) reafirmando a proteção da privacidade como um direito básico, que por sua vez afeta a interpretação de delitos como invasão de dispositivos informáticos, divulgação indevida de conteúdo, bem como chantagem virtual; (2) para formar as responsabilidades legais das empresas e agentes de processamento de dados por seu trabalho, fornecendo regulamentos para estudar omissões ou atos negligentes que resultarão em responsabilidade criminal, incluindo discussão sobre crimes corporativos e responsabilidade legal por entidades jurídicas.

Para além da dimensão normativa, adaptar-se a esta nova era tecnológica não deve ser apenas técnico, mas principalmente ético e humanitário, já que com a expansão deste meio virtual, surgiram novas formas de violar a honra, a imagem e a privacidade de muitos usuários da internet, causando danos que muitas vezes podem ser irreversíveis. Comentários ofensivos, compartilhamento não consensual de uma fotografia e até mesmo a manipulação de informações comprometem reputações e causam sérios problemas emocionais para as vítimas.

Assim, a responsabilidade criminal na internet não deve ser apenas punitiva, mas também protetiva, pois é necessário proteger a dignidade humana em um espaço totalmente marcado pelo anonimato e pela progressão da disseminação de conteúdos nocivos. Sob essa

ótica, vale ressaltar que o debate sobre proteção de dados e privacidade é, acima de tudo, uma forma de preservar a integridade moral e emocional dos indivíduos diante das novas vulnerabilidades criadas pelo mundo digital (Doneda, 2019).

Nessa perspectiva de tutela ampliada de direitos, na era digital, a maneira de responder sobre a responsabilidade criminal, se levarmos isso em consideração, é se nossa lei deve garantir que a sociedade sinta que não está sob o domínio de pessoas que usam a tecnologia de forma ofensiva. Assim sendo, a punição deve ser repressiva, preventiva e socialmente educativa, porque o direito penal funciona de maneira equilibrada, resistindo à tentação do punitivismo tecnológico de sucumbir a crimes que violam os direitos humanos. Em decorrência disso, o desafio atual continua sendo construir um regime jurídico que acompanhe a velocidade da informação, mas que também se baseie nos princípios de legalidade, proporcionalidade e humanidade da punição (Lima, 2023).

Como desdobramento dessa evolução interpretativa e normativa, temos uma noção ampliada de responsabilidade criminal na era digital que se estende aos espaços de conteúdo adulto, que ressaltam ainda mais sensivelmente os perigos de um mundo estreitamente conectado. Ao fornecer um meio pelo qual imagens, vídeos, dados pessoais e mais são amplamente circulados e consumidos, essas plataformas estão expostas a atos criminosos, incluindo exploração sexual e disseminação não autorizada de material íntimo. Nessa concepção, motivada pela sociedade de risco, elas deixam de servir como simples intermediárias, tornando-se agentes ativos contra danos e devem estabelecer meios adequados de controle e proteção.

Desse modo, como consequência lógica desse dever de atuação, a responsabilização criminal – embora excepcional e limitada pela legalidade – torna-se necessária diante da omissão, falta de segurança mínima ou falhas que favorecem crimes graves, especialmente contra crianças, adolescentes e mulheres. Nessa medida seus efeitos ampliam a proteção dos usuários e incentivam modelos mais éticos de governança digital, com políticas de moderação eficientes e respostas rápidas a violações de direitos.

Em arremate, um ambiente onde o virtual produz danos tão concretos quanto os do mundo físico, esse compromisso torna-se essencial para alinhar a inovação tecnológica com a liberdade, segurança e dignidade humana que o Direito Penal busca salvaguardar, impondo-se sob a análise específica dos regimes de responsabilização aplicáveis aos diversos atores que operam no ambiente digital. É sob essa perspectiva que se insere o exame da

responsabilização civil e criminal de plataformas, gestores e usuários de conteúdo adulto envolvendo crianças e adolescentes.

2. A RESPONSABILIZAÇÃO CIVIL E CRIMINAL DE PLATAFORMAS, GESTORES E USUÁRIOS DE CONTEÚDO ADULTO ENVOLVENDO CRIANÇAS E ADOLESCENTES

O Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025), emerge como um conjunto de normas destinadas à proteção de menores de 18 anos no ciberespaço, especialmente contra as práticas de exploração sexual, pornografia infantil e demais condutas ilícitas, agravadas pela tecnologia digital. Sob essa perspectiva, a construção de um esquema normativo se torna indispensável diante da complexidade das interações digitais contemporâneas. De fato, consolida-se cada vez mais desafiador se encarregar das dinâmicas do ambiente digital sem um "microssistema jurídico integrado", capaz de conciliar com as constantes mudanças tecnológicas vivenciadas na sociedade da informação (Bioni, 2021).

Nesse microssistema jurídico também destaca a noção constitucional de prioridade absoluta (Artigo 227 da Constituição Federal, 1988) que se encontra no Estatuto da Criança e do Adolescente (ECA, 1990), Crimes Cibernéticos, Marco Civil da Internet (2014) e Lei Geral de Proteção de Dados (LGPD, 2018) como uma das leis mais abrangentes para criminalizar material sexual sobre jovens, porque produzi-lo, fazer uso desse tipo (em parte) e passar isso para as mãos dos mais jovens é simplesmente uma ameaça para eles. Essa severidade legislativa decorre do argumento de que o dano moral causado a criança ao vivenciar pornografia digital é irreparável, replicável e impossível de atenuar completamente.

No âmbito da regulação da atuação dos provedores, o Marco Civil da Internet, Lei nº 12.965/2014 embora pretendido como uma expressão de liberdade e proteção dos provedores contra responsabilidade, impõe deveres de ação quando exposto a material manifestamente ilícito.

A doutrina majoritária, conforme lecionam Nucci e Brice (2025), sustenta que, em casos evolvendo crianças e adolescentes, o artigo 19 do Marco Civil da Internet não comporta interpretação isolada, sobretudo quando presentes violações graves de direitos impõem um dever imediato de atuação por parte das plataformas digitais. Dessa forma, a inércia tecnológica das plataformas diante da ciência da distribuição de conteúdo ilícito envolve uma falha no dever de segurança, sendo caracterizada como uma conduta negligente ensejada a responsabilidade civil dos provedores.

Sob a perspectiva da proteção de dados pessoais, a Lei Geral de Proteção de Dados (2018), por sua vez, reafirma a sensibilidade da proteção dos dados pessoais de menores (artigo 14), o que cria deveres das empresas de adotar padrões de dados mais seguros, consentimentos específicos e mecanismos de prevenção de riscos.

Como aponta por Doneda (2019), a proteção sobre os dados das crianças não se trata apenas de privacidade, mas também de proteção contra contextos de vulnerabilidade, dado que a exposição digital é o fator mais significativo para a possibilidade de *grooming,* monitoramento indevido e exploração sexual.

Dentro desse arcabouço normativo protetivo, as plataformas de conteúdo adulto têm um papel maior dentro desse quadro normativo porque existem em um ambiente que são inerentemente predispostos a facilitar a produção e o fluxo de material sexualizado. A posição social de tais empresas obtendo dinheiro da interação e visibilidade dos usuários exige que elas "organizem estruturas regulatórias digitais conducentes à proteção de crianças e jovens", as plataformas digitais devem estruturar modelos de governança e prevenção de riscos compatíveis com a proteção de grupos vulneráveis, como crianças e adolescentes. Assim, políticas de validação de idade, filtragem de conteúdo, moderação ativa e remoção imediata de material suspeito não são mais práticas recomendadas, mas uma responsabilidade legal. (Bioni, 2021)

Desse modo, o Estatuto Digital da Criança e do Adolescente (1990) é um livro de regras, não apenas um código de conduta, mas um paradigma de ação preventiva e repressiva contra a exploração sexual na Internet. Nessa lógica, se estabelece limites mínimos de conduta para todas as plataformas, orienta sobre suas responsabilidades civis e criminais, e sublinha que proteger crianças e adolescentes como um todo é uma prioridade crítica mesmo no espaço digital. Em última análise, a proteção da internet para crianças e adolescentes não pode repousar apenas na reação do estado ao dano, mas requer que intermediários tecnológicos se tornem "agentes ativos de prevenção", com responsabilidade por omissão tecnológica (Schreiber, 2022). No aspecto da omissão como geradora autônoma do dever jurídico, é necessário inserir o exame pontual da responsabilidade civil das plataformas digitais na tutela infantojuvenil.

2.1. Responsabilidade Civil por Omissão das Plataformas Digitais na Proteção de Crianças e Adolescentes

Plataformas de conteúdo adulto estão sujeitas a uma responsabilidade civil mais rigorosa quando os meios a serem circulados incluem o compartilhamento de material sexual não autorizado ou material que pode levar à exposição de crianças e adolescentes, de acordo com a prioridade absoluta dada pela Constituição à proteção de crianças e adolescentes (Artigo 227 da Constituição Federal, 1988). Nesse cenário, esse dano é repetitivo, agravado e multiplicado no ambiente digital, pois todo o espaço de conteúdo pode ser replicado infinitamente. Cada novo compartilhamento renova a lesão, razão pela qual o dever de prevenção para as plataformas é significativamente ampliado. (Schreiber, 2022)

Sob a perspectiva da fundamentação jurídica dessa responsabilização, a responsabilidade civil pode ser subjetiva decorrente de uma violação do dever de cuidado, ou objetiva decorrente do risco associado à atividade. No primeiro caso, a negligência relevante é definida pela chamada omissão tecnológica, que é caracterizada pela falta de mecanismos eficazes de moderação ou pelo atraso na remoção de conteúdo ilícito (Bioni, 2021). Considero essa negligência ainda pior se soubermos antes que a festa tenha feito isso ou quando o conteúdo é claramente ilegal (o que ocorre com a pornografia infantil definida pelo Estatuto da Criança e do Adolescente (ECA, 1990). Pelo mesmo raciocínio, a jurisprudência é reforçada por esses fatos: No caso de ser notificada, a plataforma precisa excluir imediatamente o conteúdo ofensivo sob o princípio legal de co-responsabilidade (REsp 1.660.168/RS).[4]

Para além da responsabilidade subjetiva, com base na lógica objetiva, aplica-se a teoria do risco da atividade: tais empresas lucram com o tráfego e o engajamento. Por isso, empresas que realizam atividades lucrativas e induzem riscos previsíveis devem ser responsáveis pelos danos de qualquer consequência que resulte dessas atividades, mesmo que não haja culpa direta (Cavalieri Filho, 2021). Sob essa perspectiva, plataformas de conteúdo adulto, cujo propósito é a circulação de conteúdo sensível, têm uma responsabilidade aumentada tanto pela vigilância quanto pela verificação de idade, bem como por filtros de segurança.

Complementando a responsabilização das plataformas, os gestores são civilmente responsáveis por culpa *in vigilando e culpa in omittendo,* sobretudo onde controles internos

---

[4] "A partir do momento em que o provedor de aplicações de internet é notificado acerca da existência de conteúdo ilícito em sua plataforma, surge o dever de agir de forma diligente para a sua imediata remoção, sob pena de responder solidariamente pelos danos decorrentes da manutenção indevida do material ofensivo." (STJ, REsp 1.660.168/RS).

sistêmicos permitem que conteúdo seja compartilhado em relação a menores. A falta de políticas eficazes de moderação, treinamento de equipe ou ferramentas de detecção automatizadas equivale a uma falha organizacional que pode gerar responsabilidade. Concomitante a isso, usuários que publicam, compartilham ou armazenam conteúdo ilegal são não apenas criminalmente responsáveis sob o ECA (1990), mas também civilmente responsáveis por danos morais e materiais. Dessa forma, a questão punitiva dessas ações se torna muito mais amplas do que a reparatória, devendo ser necessário uma análise detalhada da responsabilização penal tanto por ação quanto por omissão na propagação de conteúdo adulto envolvendo crianças e adolescentes.

2.3. Responsabilidade Criminal por Ação e Omissão na Disseminação de Conteúdo Adulto Envolvendo Crianças e Adolescentes.

A responsabilidade criminal pelo uso de conteúdo adulto para crianças e adolescentes hoje pode ser amplamente atribuída aos Artigos 240 a 241-E do Estatuto da Criança e do Adolescente (ECA, 1990), incluindo tipos criminais para produção, armazenamento, disseminação e facilitação de pornografia infantil, e um nível muito alto de aplicação que foi feito com o Estatuto da Criança e do Adolescente. A extensão em que a pornografia infantil é ilegal é a razão pela qual a lei penal será extremamente severa. A circulação de pornografia infantil é tão ruim quanto sempre foi, pois, a dignidade da vítima é danificada a cada visualização subsequente, e o efeito negativo nos humanos é para toda a vida (Pereira, 2022). Nesse contexto, qualquer pessoa que faça, compartilhe ou, de fato, possua tal conteúdo se enquadra no escopo normal do ECA (1990), independentemente de ganho econômico ou papel preciso.

No que se refere especificamente a plataformas e gestores, a responsabilidade por infração penal está amplamente relacionada à omissão imprópria conforme definido no Artigo 13, §2 do Código Penal (1940).

O garantidor é responsável quando ele ou ela, tendo o dever legal de evitar o resultado, não agiu, e sua omissão é equivalente à da ação típica (Greco, 2023). Desse modo, essa vigilância aumentada é adotada por plataformas de conteúdo adulto que lidam com atividades de alto risco. Diante disso, se permitirem com descuido e se não fornecerem, ou não puderem fornecer, mecanismos adequados para a circulação de material contendo conteúdo de menores, podem ser acusados de participar disso por omissão relevante. A

omissão imprópria requer uma posição de garantidor para evitar o resultado que seria compatível com empresas que têm controle sobre seus sistemas (Pierangeli, 2021).

Além disso, a negligência administrativa grave pode se manifestar como negligência nos mecanismos de verificação de idade e na falha de moderação, falha em remover material notoriamente ilegal em tempo hábil ou falha em tratar reclamações. Em delitos de omissão imprópria, a responsabilidade criminal emerge se a inação contribui causalmente para a perpetuação do crime, tratando-se de um fenômeno regularmente presente em espaços digitais onde não há restrições robustas em vigor (Busato, 2022). Nesse mesmo sentido, demonstra se que as plataformas que não utilizam ferramentas mínimas de prevenção tecnológica são capazes de promover crimes de exploração infantil, que se aproximam da figura criminal daqueles que, em especial, contribuem para o crime (Peck, 2022).

Por outro lado, embora, no ordenamento jurídico brasileiro, a pessoa jurídica, geralmente, não seja passível de responsabilidade penal, exceto pelos ilícitos ambientais, a responsabilidade criminal é de natureza subjetiva, ou seja, decorre da conduta de pessoas físicas que concorreram com a sua ação ou omissão para o resultado ilícito. Desta forma, caso seja demonstrado que gestores, moderadores e representantes aspectos da plataforma digital devessem agir, nos termos do artigo 13, §2º, do Código Penal (1940), estes poderão ser responsabilizados solidariamente.

Nesse cenário, a omissão torna-se penalmente relevante quando evidenciado o elemento subjetivo da conduta, consistente no dolo ou na culpa grave, especialmente diante da previsibilidade do dano e da vulnerabilidade das vítimas. Desse modo, a violação consciente do dever de garante é suficiente para caracterizar a comissão por omissão, ainda que o agente não tenha praticado diretamente a conduta típica (Capez, 2023).

Cumpre acrescentar que a relevância da presente pesquisa é evidenciada por dados que demonstram o crescimento expressivo da exploração sexual de crianças e adolescentes no ambiente digital. Segundo levantamentos internacionais, milhares de casos de material de abuso sexual infantil são identificados anualmente, com ampla circulação por meio de plataformas digitais, o que revela a dimensão global e persistente do problema. Organizações de proteção à infância alertam que a facilidade de armazenamento, compartilhamento e reutilização dessas imagens potencializa danos contínuos às vítimas, exigindo respostas jurídicas mais rigorosas.

Desse modo, o Código Penal (1940) e a Lei 12.737/2012 (Lei Carolina Dieckmann) são outros relevantes para esses casos, pois o conteúdo relacionado a crianças é usado para

extorsão, aliciamento, é armazenado sem autorização ou pode ser compartilhado com potencial de dano grave. Diante desse cenário, justifica-se ainda que o Direito Penal deve desempenhar função preventiva e protetiva nesses casos, já que a proteção da dignidade sexual infantil exige uma resposta mais rigorosa que agora enfrenta os problemas crescentes associados ao cenário digital (Bitencourt, 2022).

Dessa forma, a responsabilidade criminal no âmbito das plataformas digitais não se limita aos agentes que praticam diretamente a exploração sexual online, alcançando igualmente usuários, gestores e responsáveis técnicos que, por conduta omissiva juridicamente relevante, contribuam para a manutenção ou propagação do conteúdo ilícito. Como reflexo direto, a omissão do garantidor integra o próprio desenvolvimento do delito, uma vez que a inércia daquele que tinha o dever legal de agir equipara-se à prática da ação típica (Greco, 2023). Assim, a ausência de providências eficazes para impedir a circulação de material envolvendo crianças e adolescentes pode configurar responsabilidade penal, sobretudo quando evidenciado o descumprimento do dever de proteção imposto pela posição ocupada no ambiente digital.

Por mais que existam normas que estabeleçam fundamentos relevantes para a responsabilização, é fato que a efetividade da tutela jurídica ainda enfrente entraves estruturais, tecnológicos e probatórios que dificultam a prevenção e repressão dessas práticas no ambiente virtual. Desse modo, a pesquisa impõe o objetivo de examinar os principais desafios jurídicos e operacionais para responsabilizar os agentes envolvidos e fortalecer os mecanismos de combate à exploração sexual de menores em plataformas de conteúdo adulto.

3. DESAFIOS PARA RESPONSABILIZAR E COMBATER À EXPLORAÇÃO SEXUAL DE MENORES EM PLATAFORMAS DE CONTEÚDO ADULTO

Plataformas digitais para conteúdo adulto, apoiadas por modelos de pagamento centrados em assinaturas, produção descentralizada e circulação audiovisual estão surgindo em um mundo de riscos reais para a saúde e bem-estar de crianças e adolescentes online. Elas não são apenas uma instituição adulta; na verdade, desenvolveram-se no espaço digital onde novos tipos de usuários contribuem para o crescimento de jovens criando e disseminando conteúdo inadequado e podem ainda mais enraizar pedófilos que podem ajudar a aliciar crianças e adultos para o conteúdo ilegal e vender suas imagens sexuais.

Com isso em mente, estudos internacionais recentes agora mostram a importância desse problema. Houve mais de 36 milhões de relatos suspeitos de exploração sexual infantil

online em 2023, de acordo com o Centro Nacional para Crianças Desaparecidas e Exploradas [NCMEC], reiterando assim a natureza global bem reconhecida deste problema (NCMEC, 2024). Portanto, as evidências dos dados de exploração sexual digital indicam que isso não é um problema isolado, mas sim uma realidade sistemática e habitual, devido à infraestrutura tecnológica que ameaça os sistemas tradicionais de controle estatal (CSAT, 2016).

Há uma clara lacuna entre esses rápidos desenvolvimentos na tecnologia e na lei em como a lei decide como regulá-los. A velocidade com que a informação está sendo compartilhada, o uso de ferramentas de informação para privacidade e a hospedagem de dados em vários países torna difícil responsabilizar agentes e controlar os danos causados às vítimas. Ao examinar as barreiras tecnológicas e legais para políticas bem-sucedidas por parte dos governos para manter crianças e adolescentes seguros de conteúdo adulto através do ciberespaço, este cenário questiona se é possível para eles fazerem isso de forma eficaz.

Nesses termos, pode-se argumentar a tensão essencial que existe entre o avanço tecnológico, que expande as possibilidades de comunicação e interação no ambiente digital, e as limitações operacionais enfrentadas tanto pelo Estado quanto pelas próprias plataformas na identificação e supressão de conteúdo ilícito.

Este paradoxo mostra que as ferramentas para conectividade e compartilhamento de informações também impedem a gestão e o monitoramento dessas práticas, exigindo um exame mais aprofundado das fronteiras tecnológicas e legais que existem para conter a exploração sexual digital, um tópico que será elaborado em seções posteriores da pesquisa.

3.1. Anonimização, Transnacionalidade e Sofisticação Tecnológica: A Estrutura Criminológica da Exploração Sexual Digital

Criminologicamente, a exploração sexual de crianças e adolescentes online é um fenômeno global, adaptável e intrincadamente organizado. Diferentemente das formas tradicionais de abuso, a mediação tecnológica dispensa a necessidade de um contato físico imediato, o que permite que o aliciamento, a criação, o armazenamento e a disseminação do material aconteçam de forma descentralizada e em diferentes países. Essa dinâmica evidência como o ambiente digital amplia as possibilidades de atuação doa agentes criminosos e dificultam sua contenção pelas estruturas tradicionais de controle.

Nesse cenário os dados empíricos reforçam a dimensão concreta do problema. Em 2023, o Canal Nacional de Denúncias de Crimes Cibernéticos da SaferNet Brasil recebeu dezenas de milhares de relatos sobre abuso e exploração sexual infantil online, que foram a

maior parte das denúncias na plataforma (SaferNet Brasil, 2024). Diante desses números, esse cenário evidencia, além da persistência da prática, seu fortalecimento como uma das mais proeminentes formas de violência contra crianças e adolescentes no meio digital contemporâneo.

Para que se compreenda melhor como se dá a dinâmica criminosa no meio digital, a criminologia digital aponta que tais condutas têm três características fundamentais. A primeira diz respeito à massificação, pois a disseminação ilimitada de conteúdos potencializa enormemente o caráter lesivo, transformando um único evento em uma ofensa constante à dignidade da vítima. A segunda, porque o uso de VPNs, a criptografia de ponta a ponta e os ambientes da *deep web* dificultam que as autoridades competentes identifiquem os responsáveis. Por último, menciona-se a transnacionalidade, visto que tanto os servidores quanto os usuários e as vítimas do crime frequentemente se situam em diferentes nações, o que fragmenta a jurisdição e atrasa as investigações.

Essas características estruturais do fenômeno formam ainda mais complexo o seu enfrentamento. A Pesquisa acadêmica sobre redes anônimas indica que uma parte considerável do tráfego na rede Tor, por exemplo, é destinada à busca ou ao compartilhamento de material de abuso sexual infantil, o que evidencia o caráter oculto e descentralizado do fenômeno (Oakes et al., 2024, arXiv). A rápida adaptação dos criminosos às novas tecnologias — como o emprego de inteligência artificial para a criação ou alteração de imagens — demonstra que se trata de uma criminalidade em evolução, que avança junto com as inovações digitais.

Paralelamente as dimensões tecnológicas e estruturais do problema a exploração sexual digital acontece em um contexto social que amplifica a vulnerabilidade. A exposição precoce de crianças e adolescentes às redes sociais, sem a devida supervisão e educação digital insuficiente, facilita o aliciamento virtual. Esse processo, muitas vezes dificultado por manipulação psicológica e chantagem, leva a vítima a se tornar uma produtora involuntária de conteúdo exploratório, o que intensifica o dano e torna a prática mais difícil de interromper.

Com base nesses fatores tecnológicos, estruturais e sociais, do ponto de vista da criminologia, a exploração sexual de crianças e adolescentes na internet é organizada como uma ação com grande habilidade em se esconder e um alto potencial de dano, influenciando diretamente a eficácia das ferramentas de responsabilização e enfrentamento. As dinâmicas criminológicas de interesse são essenciais para essa perspectiva, pois permitem considerar até que ponto o quadro legal relevante, bem como as políticas regulatórias, está sendo projetados

para abordar tais questões. Segue-se, então, que é importante examinar como as ferramentas legais existentes — em particular os instrumentos referentes à responsabilização de agentes e plataformas digitais — respondem às novas formas de violência sexual contra crianças transmitidas pela tecnologia.

3.2. O Paradoxo Tecnológico e os Limites Operacionais na Identificação e Repressão da Exploração Sexual Digital.

O surgimento das tecnologias digitais abriu uma desconexão muito fundamental na luta contra a exploração sexual de crianças e adolescentes: as ferramentas de comunicação são usadas para comunicação, informação com direitos e para disseminação, de modo que os mesmos meios se tornam ainda mais amplos, perpetuando e massificando a comunicação de conteúdo ilegal. Graças à descentralização embutida na internet e à velocidade dos dados e à amplitude das plataformas disponíveis, a repressão criminal e a responsabilidade civil não podem ocorrer sem uma tecnologia que esteja em boa forma, mas ainda longe disso. A questão, portanto, não é se a conduta criminosa existe, mas sim se a estrutura tem a capacidade de capturá-la e preveni-la antes que cause danos.

Neste domínio, o primeiro obstáculo é o conteúdo digitalizado. Todos os dias, milhares de conteúdos são criados, hospedados e enviados em redes sociais e até compartilhados em aplicativos de mensagens. A quantidade de conteúdo gerado e enviado torna os moderadores humanos virtualmente impossíveis. Relatórios internacionais sobre exploração sexual infantil *online* estão principalmente preocupados com sistemas de detecção automatizada, como IA e *hashmatch,* que detectam conteúdo já sinalizado como ilícito (OCDE/Tech Coalition, 2025). Mas esses sistemas enfrentam desafios técnicos difíceis, como a falha em detectar novos conteúdos e identificar situações de aliciamento, onde a análise comportamental deve ser feita em vez do trabalho de reconhecimento de imagens.

Existem também questões qualitativas em relação à falta de anonimização. VPNs, criptografia de ponta a ponta e redes anônimas tornaram muito mais difícil rastrear aqueles que geraram e compartilharam material de abuso sexual infantil. Pesquisas na rede Tor demonstraram que existem muitos domínios onde esse tipo de conteúdo está se espalhando (Nurmi et al., 2024) e mostram como essas ferramentas digitais para proteger a privacidade podem ser colocadas a serviço de atividades criminosas. Esse aspecto tecnológico, portanto, aumenta o custo e o tempo para descobrir quem (se alguém) estava por trás disso.

Além disso, os desenvolvimentos recentes em inteligência artificial generativa levam a um problema adicional, pois a inteligência artificial aumentou em complexidade no mundo. Relatórios globais relataram o uso mais recente de IA na produção de imagens artificiais de menores, especialmente *deepfakes* realistas (Internet Watch Foundation, 2024). Esse aumento na quantidade de material em circulação e os desafios das abordagens convencionais foram considerados incapazes de identificar arquivos conhecidos e produzir novos conteúdos gerados por inteligência artificial.

Junto aos problemas tecnológicos em torno da detecção e identificação dos culpados de tais problemas, também temos os requisitos de política e técnicos nas e das plataformas digitais. Embora muitas empresas anunciem soluções de detecção automatizada e equipes especializadas em relatórios de transparência, a implementação e resposta a reclamações são em grande parte inconsistentes em relação à eficácia do sistema (OCDE, 2025) e vídeos ao vivo e outros tipos de mídia são muito mais difíceis de monitorar e o abuso pode ocorrer no meio da situação porque uma ação de bloqueio deve ser tentada.

Além das barreiras técnicas e institucionais nas próprias plataformas, a fragmentação jurisdicional também tem a ver com tecnologia. Os países agora devem trabalhar juntos em provas digitais para garantir que possam acessar e preservar provas digitais armazenadas em vários territórios do mundo. Sem um padrão em vigor e informações lentas e menos disponíveis entre os estados, ainda podemos evitar investigações e arriscar a segurança das vítimas conosco.

Portanto, o escopo que é o técnico, é claro, afeta a eficiência do próprio sistema de justiça. Assim, a situação tecnológica não é apenas uma questão de problema técnico, mas vemos que a tecnologia não é meramente o problema das soluções tecnológicas, ela impacta o sistema de justiça não apenas resolvendo o problema técnico, mas também pode levar a uma falta de justiça para as vítimas quando se trata de investigação de crimes, acusação e punição para levar tais crimes à justiça.

Não há um bom caso contra, mas ainda mais a justiça é culpada pela falta de uma investigação de caso sendo feita corretamente. Assim, é fundamental interrogar como os marcos regulatórios legais e digitais têm buscado resolver tais questões em torno da responsabilidade e deveres das plataformas, conforme definido pelas leis dentro do cenário digital.

3.3. O Descompasso Normativo e os Limites da Responsabilização no Sistema Jurídico Contemporâneo

Os desafios tecnológicos citados anteriormente indicam que a exploração sexual infantil virtual não é meramente uma consequência da falta de supervisão digital. Efetivamente, ainda existem obstáculos legais e estruturais no próprio sistema jurídico, que nem sempre acompanha as rápidas mudanças tecnológicas.

No sistema jurídico brasileiro, o Estatuto da Criança e do Adolescente (1990) trata de crimes como produção, posse (fabricação) e circulação de material que explora sexualmente crianças. Sim, essas leis são um paradigma para a proteção infantil hoje, mas elas nascem em um estágio tardio de nossas vidas e são construídas como sociedades diferentes agora do que nunca foram. Graças ao uso generalizado de redes sociais, aplicativos de mensagens criptografadas, canais ao vivo e outros mecanismos de manipulação digital, o crime é diferente e o comportamento criminoso mudou com base em um cenário totalmente novo.

Somado a esses entraves relacionados à própria tipificação penal, quanto à responsabilidade de provedores, o Marco Civil da Internet (2014) criou um modelo que, em geral, exige uma ordem judicial para a remoção de conteúdo. A escolha legislativa visou encontrar um equilíbrio entre a liberdade de expressão e a segurança jurídica. Entretanto, quando se trata de situações de exploração sexual de menores, sua aplicação pode criar conflitos, especialmente considerando a urgência em proteger a vítima. A necessidade de provocação judicial, somada à lentidão crônica do sistema processual, pode atrasar a remoção de material ilegal, possibilitando sua propagação constante.

Aliado a essas limitações normativas internas, a natureza transnacional desses delitos também destaca as fragilidades na cooperação jurídica internacional. Apesar de haver instrumentos multilaterais, como a Convenção de Budapeste (2001), as disparidades nas leis e nos procedimentos entre os Estados podem impedir uma troca rápida de informações e a obtenção de provas digitais.

Cada vez mais, sem uma legislação clara e em vista dos tratados internacionais, a perseguição criminal em ambiente virtual é muito difícil. Os problemas de cooperação internacional devem ser complementados pela relação entre a segurança das crianças e outros direitos humanos fundamentais, incluindo a privacidade, a liberdade de expressão e a proteção de dados pessoais, garantidos por legislações como a Lei Geral de Proteção de Dados (2018).

Devido à ausência de orientações normativas mais precisas sobre os deveres preventivos das plataformas, há também uma falta generalizada de aplicação e, portanto, menos foco em como as plataformas devem cuidar das pessoas, de modo que o entendimento

é muito restrito, podendo também não estar dispostas e pouco podem fazer sobre o que está sendo feito para o bem daqueles em risco.

Como reflexo direto dessas limitações jurídicas e institucionais, as consequências legais dessas vulnerabilidades são significativas. As investigações se alongam devido à dificuldade de obtenção de informações, as provas digitais podem ser perdidas ou se tornarem inviáveis, e a responsabilização penal se torna mais complicada. Para as vítimas, a permanência e a reprodução de conteúdo ilegal na internet geram uma revitimização constante, o que vai contra o princípio da proteção integral que é garantido pela legislação.

À luz desse cenário, conclui-se que a continuidade da exploração sexual de crianças e adolescentes na internet demonstra que simplesmente tipificar penalmente a conduta não é suficiente para garantir uma proteção efetiva. Considero esses impedimentos tecnológicos e legais a manifestação da dissonância estrutural da sociedade digital contemporânea e o modelo tradicional de responsabilidade, atualizado hoje, como um dos principais desafios enfrentados pelo sistema jurídico adulto atualmente.

É fundamental revisar (se não as ferramentas tecnológicas e institucionais já existentes, se acreditarmos que os mecanismos estão funcionando em grande parte, mas precisam ser melhorados) o tratamento das novas formas de violência sexual infantil trazidas pela tecnologia, tanto no âmbito legal e normativo quanto no regulatório e jurídico da nossa era, para facilitar uma proteção mais eficaz de crianças e adolescentes no ambiente digital.

CONSIDERAÇÕES FINAIS

Assim, as tecnologias digitais e a intensificação do contato social em nosso novo ambiente virtual estão mudando a forma como nossa sociedade pode criar e distribuir informações e usar dados. Não apenas existem outras formas de violações em que direitos básicos são violados, porque no mundo da geração digital, jovens e adolescentes têm sido sexualizados no mundo virtual, o que é parte do que agora pode acontecer. O contexto da pesquisa para este artigo é o seguinte: como se dá a responsabilidade jurídica das plataformas de conteúdo adulto em situações de posts não autorizados ou que envolvam crianças e adolescentes?

A investigação demonstrou que a resposta a essa questão exige uma análise que deve ser complementada por considerações de Direito Civil, Direito Penal e Direito Digital, além de considerar as particularidades tecnológicas do ambiente virtual. No entanto, o fenômeno da exploração sexual infantil na Internet vai além de um único crime para ser enquadrado como

uma questão estrutural que envolve as ações de vários atores, como usuários, gestores das plataformas e os próprios intermediários tecnológicos. Nesse sentido, se olharmos para as responsabilidades “legais” das plataformas mencionadas, deve-se ver não apenas do ponto de vista de seu próprio comportamento sob ataque, mas também de uma de suas insuficiências tecnológicas, a falta ou fraquezas de ferramentas ativas para detectar, prevenir e remover conteúdo ilegal.

No primeiro momento da pesquisa, verificou-se que os institutos clássicos da responsabilidade civil precisaram ser reinterpretados para acompanhar as transformações da sociedade digital. Conduta, dano e nexo causal assumiram, no contexto da rápida disseminação de informações e da variedade de intermediários atuando na circulação de conteúdo online na internet, essas novas formas de estrutura. A análise mostrou que a responsabilidade sob o princípio da responsabilidade civil para plataformas pode se desenvolver a partir de uma conduta direta, bem como da falha em responder contra conteúdo ilegal, especialmente se as plataformas estão cientes da irregularidade e não existem medidas eficazes para parar a disseminação e propagação do dano do conteúdo. Nesse cenário, a tomada de decisão recente reconheceu a negligência algorítmica, que é frequentemente descrita como a omissão de um processo automatizado ou até mesmo a falta de moderação decente.

O estudo ilustrou que o modelo que descreve em detalhe o Marco Civil da Internet Brasileiro, como se relaciona à necessidade de uma ordem judicial para a responsabilidade dos provedores, tem defeitos profundos quando se trata de violações graves de direitos de acordo com o requisito. Para casos de exploração sexual infantil, a decisão judicial prévia obrigatória pode levar a atrasos na ação corretiva para conteúdo ilegal, o que pode levar à destruição de ainda mais crianças e revitimização das vítimas. Nesse sentido, a jurisprudência brasileira tende a relaxar o critério, reconhecendo que, uma vez que uma plataforma digital está plenamente ciente de material manifestamente ilegal, deve um dever de diligência adequada.

No âmbito penal, o estudo mostrou que a responsabilidade criminal em conexão com a exploração sexual de crianças e jovens na internet é amplamente sujeita às disposições do Estatuto da Criança e do Adolescente que delineia claramente a pornografia que deve ser produzida, armazenada e disseminada contra crianças menores. Apesar de não haver a responsabilidade penal das plataformas enquanto pessoas jurídicas, a análise expôs o potencial de a responsabilidade criminal se estender além dos infratores diretos da conduta

para aqueles que, atuando como garantidores, são incapazes de agir para limitar a continuação do crime. Nesse sentido, gestores de plataformas digitais e gestores técnicos podem ser responsabilizados quando sua ausência apoia a manutenção de conteúdo ilegal, especialmente quando a existência de um dever legal de agir é demonstrada.

Outra questão identificada na pesquisa é o estabelecimento de um microssistema de direito para a proteção digital da infância que inclui várias ferramentas normativas, como o Estatuto da Criança e do Adolescente, o Marco Civil da Internet Brasileiro, a Lei Geral de Proteção de Dados e instrumentos legais individuais sobre crimes cibernéticos. Esse acordo normativo mostra que a proteção de crianças e jovens no ciberespaço não requer que qualquer lei seja implementada, mas necessita de um movimento cooperativo da instituição legal, ancorado na regra constitucional de prioridade absoluta. As plataformas digitais ocupam um papel vital em sustentar isso, pois determinam a arquitetura tecnológica para a circulação de conteúdo e são fundamentais na aplicação dessas regras para a execução. Mas o estudo também mostrou que a responsabilidade legal é complicada pela natureza tecnológica do terreno virtual. A anonimização dos usuários, a estrutura de rede transnacional das infraestruturas digitais e tecnologias sofisticadas como criptografia e IA dificultam a identificação dos responsáveis e impedem a rápida interrupção da circulação de material ilícito.

Esses elementos revelam uma discrepância entre a taxa de mudança tecnológica e a força jurídico-regulatória da lei, o que representa desafios para o sucesso da política de proteção infantil. Além disso, a dimensão internacional da internet impõe restrições às ações unilaterais dos estados nacionais. Muitas das atividades de exploração sexual infantil online ocorrem por usuários, servidores e plataformas em outros países, e, portanto, são necessários mecanismos de cooperação internacional mais eficientes para investigar e interromper esses atos. A ausência de padrões normativos harmonizados e a ausência de vias rápidas para procedimentos de cooperação jurídica internacional contribuem para manter deficiências de responsabilização por parte dos atores.

Com base nessa situação, é claro que a solução para o problema da exploração sexual de crianças e adolescentes em plataformas digitais nunca pode se limitar a simplesmente punir após o dano ter sido causado. A prevenção está no cerne disso e as plataformas devem implementar segurança estrutural, incluindo sistemas de verificação de idade, ferramentas automatizadas para detectar conteúdo ilegal, relatórios avançados e moderadores. Elas devem

ser entendidas não apenas como boas práticas comerciais, mas como deveres legais genuínos que decorrem dos propósitos sociais das atividades digitais.

Com base na teoria da avaliação crítica, podemos concluir que a base central desta pesquisa enfatiza que não é possível limitar de forma restrita a responsabilidade das plataformas digitais, especialmente quando os mais vulneráveis estão implicados. Essa lógica que posiciona esses intermediários como técnicos neutros que fornecem infraestrutura tecnológica é inadequada atualmente, quando esses intermediários realmente fornecem organização, filtragem e amplificação de conteúdo.

Desse modo, em resposta à pergunta principal levantada na presente pesquisa, conclui-se que as plataformas de conteúdo adulto devem assumir responsabilidade legal quando há falha legal clara e inegável de acesso a conteúdo ilegal, onde crianças e adolescentes estão envolvidos nesse conteúdo. Há uma responsabilidade nascida de leis infraconstitucionais, mas também de princípios constitucionais de ampla proteção de crianças e adolescentes e respeito pela dignidade humana.

Por fim, conclui-se que a construção de um ambiente digital seguro depende de uma atuação articulada entre o Estado, as plataformas tecnológicas e a sociedade civil. Apesar de ser fundamental para criar parâmetros de responsabilização, a lei não pode operar isoladamente. Para esse fim, é vital formular uma política pública comum de educação digital, ampliar a colaboração internacional e instar a criação de salvaguardas que melhor se adaptem ao cenário em mudança das ameaças no ciberespaço. Somente por meio dessa abordagem integrada será possível reduzir as vulnerabilidades existentes e garantir que a internet continue sendo um espaço de liberdade, sem se transformar em um território de impunidade para violações graves de direitos fundamentais.

REFERÊNCIAS

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. São Paulo: Forense, 2021.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal: parte geral**. 28. ed. São Paulo: Saraiva, 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Diário Oficial da União, Brasília, DF, 5 out. 1988.

BRASIL. **Decreto-Lei nº 2.848**, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, RJ, 31 dez. 1940.

BRASIL. **Lei nº 8.069**, de 13 de julho de 1990. Estatuto da Criança e do Adolescente. Diário Oficial da União: Brasília, DF, 16 jul. 1990.

BRASIL. **Lei nº 12.737,** de 30 de novembro de 2012. Dispõe sobre crimes informáticos (Lei Carolina Dieckmann). Diário Oficial da União, Brasília, DF, 3 dez. 2012.

BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. **Marco Civil da Internet.** Diário Oficial da União: Brasília, DF, 24 abr. 2014.

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

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.660.168/RS**. Relatora: Min. Nancy Andrighi. Brasília, DF, 2017.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.771.866/SP.** Relator: Ministro Nancy Andrighi. Julgado em 2019.

BRASIL. **Supremo Tribunal Federal. Recurso Extraordinário nº 1.037.396 (Tema 987)**. Relator: Ministro Dias Toffoli. Julgado em 2021.

BUSATO, Paulo César. **Direito Penal:** parte geral. 3. ed. São Paulo: Atlas, 2022.

CAPEZ, Fernando. **Curso de Direito Penal**: parte geral. 25. ed. São Paulo: Saraiva, 2023.

CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 15. ed. São Paulo: Atlas, 2021.

CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 16. ed. São Paulo: Atlas, 2024.

CONSELHO DA EUROPA. **Convenção sobre o Cibercrime (Convenção de Budapeste).** Budapeste, 2001.

DINIZ, Maria Helena. **Curso de direito civil brasileiro: responsabilidade civil**. São Paulo: Saraiva, 2023.

DONEDA, Danilo**. Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

GRECO, Rogério. **Curso de Direito Penal**: parte geral. 26. ed. Rio de Janeiro: Impetus, 2023.

INTERNET WATCH FOUNDATION (IWF). **Annual Report 2024**. Cambridge, 2024.

LIMA, Renato Brasileiro de. **Manual de processo penal**. Salvador: JusPodivm, 2023.

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN (NCMEC). **CyberTipline Report** 2023. Alexandria, 2024.

NURMI, J. et al. **Hidden services and illicit content distribution on Tor networks**. 2024.

OAKES, J. et al**. An analysis of illegal content distribution on the Tor network**. arXiv preprint, 2024.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **Digital services and content moderation transparency report.** Paris, 2025.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD); TECH COALITION. **Online child safety: detecting and combating child sexual exploitation**. Paris, 2025.

PECK, Patrícia. **Direito digital aplicado**. 6. ed. São Paulo: Saraiva, 2022.

PIERANGELI, José Henrique. **Manual de Direito Penal brasileiro**. São Paulo: Revista dos Tribunais, 2021.

PINHEIRO, Patricia Peck. **Direito digital**. São Paulo: Saraiva, 2021.

SAFERNET BRASIL. **Relatório anual de denúncias de crimes cibernéticos** – 2023. Salvador, 2024.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. 13. ed. Porto Alegre: Livraria do Advogado, 2022.

SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil**. 6. ed. São Paulo: Atlas, 2022.

TEPEDINO, Gustavo. **Temas de direito civil**. Rio de Janeiro: Renovar, 2021.