Scientia et Ratio
ISSN 2525-8532

RESPONSABILIDADE PENAL NOS CRIMES CIBERNÉTICOS CONTRA CRIANÇAS E ADOLESCENTES: OS DESAFIOS DA INVESTIGAÇÃO TECNOLÓGICA

CRIMINAL LIABILITY FOR CYBERCRIMES AGAINST CHILDREN AND ADOLESCENTS: THE CHALLENGES OF TECHNOLOGICAL INVESTIGATION

Artigo submetido em 10 de novembro de 2026
Artigo aprovado em 11 de novembro de 2026
Artigo publicado em 11 de novembro de 2026

Scientia et Ratio
Volume 6 – Número 10 – 2026
ISSN 2525-8532

.

Autor:
Silvia Kelly Dias Gomes[1]
Ênio Walcacer de Oliveira Filho[2]

.

RESUMO: Este artigo examina os desafios jurídicos, periciais e tecnológicos inerentes à investigação e à persecução penal dos crimes cibernéticos cometidos contra crianças e adolescentes. Para compreender a transnacionalidade do ciberespaço, o estudo analisa as

principais manifestações da violência digital infantojuvenil, com foco no aliciamento virtual (grooming), na difusão de Material de Abuso Sexual Infantil (MASI), na extorsão sexual (sextorsão), no cyberbullying e nos riscos da adultização e do sharenting. Investiga-se a tensão entre as barreiras de anonimato e criptografia, a volatilidade das evidências digitais, a preservação da cadeia de custódia (art. 158-A do CPP) e os limites da automação pericial e da inteligência artificial diante de grandes volumes de dados. Sob a perspectiva da proteção integral e da prioridade absoluta (art. 227 da Constituição Federal de 1988), analisa-se o Marco Civil da Internet (Lei nº 12.965/2014), o Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025, a "Lei Felca") e a Resolução nº 245/2024 do CONANDA, considerando também a atualização penal promovida pela Lei nº 15.487/2026. A metodologia adota abordagem qualitativa, exploratória e bibliográfico-documental. Conclui-se que a prevenção e a repressão exigem modernização forense, cooperação internacional, cumprimento dos deveres das plataformas e acompanhamento familiar, sem confundir responsabilidade compartilhada pela proteção com imputação penal automática.

Palavras-chave: Crimes cibernéticos. Proteção infantojuvenil. Prova digital. ECA Digital. Responsabilidade penal.

Abstract: This article examines the legal, forensic, and technological challenges inherent in the investigation and criminal prosecution of cybercrimes committed against children and adolescents. To understand the transnational nature of cyberspace, the study analyzes the main forms of digital violence against children and adolescents, focusing on online grooming, the dissemination of Child Sexual Abuse Material (CSAM), sexual extortion (sextortion), cyberbullying, and the risks associated with adultification and sharenting. It investigates the challenges posed by anonymity and encryption, the volatility of digital evidence, the preservation of the chain of custody (Article 158-A of the Brazilian Code of Criminal Procedure), and the limitations of forensic automation and artificial intelligence when dealing with large volumes of data. From the perspective of comprehensive protection and absolute priority (Article 227 of the 1988 Brazilian Federal Constitution), the study analyzes the

Brazilian Civil Rights Framework for the Internet (Law No. 12,965/2014), the Digital Statute for Children and Adolescents (Law No. 15,211/2025, known as the “Felca Law”), and CONANDA Resolution No. 245/2024, also considering the criminal law amendments introduced by Law No. 15,487/2026. The research adopts a qualitative, exploratory, and bibliographic-documentary approach. It concludes that prevention and law enforcement require forensic modernization, international cooperation, compliance with digital platforms’ legal obligations, and family supervision, without confusing shared responsibility for protection with automatic criminal liability.

Keywords: Cybercrimes. Child and Adolescent Protection. Digital Evidence. Digital Statute for Children and Adolescents. Criminal Liability.

INTRODUÇÃO

A expansão vertiginosa das tecnologias da informação e da comunicação no século XXI reconfigurou de forma irreversível a arquitetura das relações sociais, econômicas e culturais. Se, por um lado, o advento da rede mundial de computadores e a popularização dos dispositivos móveis democratizaram o acesso à informação, ao aprendizado colaborativo e ao lazer, por outro lado, erigiram um ecossistema virtual marcado pela hiperconectividade desregulada e pela intangibilidade das fronteiras geográficas. Nesse novo paradigma da “sociedade digital”, a infância e a juventude emergem como os segmentos mais vulneráveis, expostos a dinâmicas predatórias e a modalidades inéditas de violência que se alastram com velocidade incontrolável.

O ordenamento jurídico brasileiro estabeleceu, a partir da Constituição Federal de 1988 (artigo 227) e da promulgação do Estatuto da Criança e do Adolescente – ECA (Lei nº 8.069/1990), o postulado da prioridade absoluta e a doutrina da proteção integral. De acordo com tais preceitos normativos, a criança e o adolescente são reconhecidos como sujeitos de direitos em peculiar condição de desenvolvimento, incumbindo à família, à sociedade e ao

Estado o dever de colocá-los a salvo de toda forma de negligência, exploração, violência, crueldade e opressão. Todavia, a transposição dessas garantias para a esfera cibernética enfrenta obstáculo monumental: o ambiente virtual opera frequentemente como uma arena desprovida de controle geográfico e fiscalizatório tradicional, na qual os agressores se valem de escudos tecnológicos de anonimização e criptografia para perpetrar gravíssimas violações aos direitos fundamentais infantojuvenis.

Nesse sentido, Ambrosio, Barbosa e Moraes (2026) situam a proteção infantojuvenil em uma discussão que envolve tanto a segurança quanto a inclusão digital. A resposta jurídica não deve reduzir o acesso à internet a uma situação de perigo permanente, pois a participação nesse ambiente também permite o exercício de direitos. O desafio consiste em assegurar condições de uso compatíveis com o desenvolvimento da criança e do adolescente, enfrentando as práticas abusivas sem transformar a exclusão digital em uma solução geral.

Frente a esse cenário de crescente complexidade criminal, a investigação de delitos cibernéticos contra vulneráveis impõe desafios profundos ao sistema de justiça e aos órgãos de persecução penal. A atribuição de autoria delitiva, a obtenção tempestiva de registros de conexão e de aplicação de acordo com o Marco Civil da Internet (Lei nº 12.965/2014), a manutenção rigorosa da cadeia de custódia das evidências eletrônicas (conforme os artigos 158-A e seguintes do Código de Processo Penal) e o enfrentamento de volumes massivos de dados digitais constituem gargalos operacionais que muitas vezes inviabilizam a resposta estatal oportuna. O advento recente da Lei nº 15.211, de 17 de setembro de 2025 (oficialmente denominada Estatuto Digital da Criança e do Adolescente e popularmente conhecida como “Lei Felca”), assim como o Decreto nº 12.880/2026 e a Resolução nº 245/2024 do CONANDA, introduziu no cenário nacional novos deveres de prevenção, mitigação de riscos, supervisão parental e responsabilização das plataformas digitais, reforçando uma estrutura de proteção compartilhada que exige interpretação segundo as atribuições de cada agente.

Diante dessas questões, o problema que orienta a pesquisa pode ser assim formulado: de que modo os obstáculos tecnológicos à obtenção e à análise da prova interferem na responsabilização penal por crimes cibernéticos contra crianças e adolescentes, e como os deveres preventivos do ECA Digital podem contribuir para seu enfrentamento? O objetivo central é relacionar as exigências jurídicas da imputação aos limites concretos da investigação, distinguindo a identificação de conteúdo suspeito da comprovação da materialidade e da autoria.

Para compreender analiticamente a amplitude dessa temática, este estudo adota uma metodologia de natureza qualitativa e finalidade exploratório-descritiva, desenvolvida mediante revisão bibliográfica e análise documental integrada. O *corpus* analítico compõe-se de diplomas normativos primários (Constituição Federal, ECA, Código Penal, Código de Processo Penal, Marco Civil da Internet, Lei nº 15.211/2025 e decretos regulamentadores), doutrina jurídico-penal e estudos sobre investigação forense, em diálogo com os trabalhos de Santos, Viana e Pinto (2026) e de Ambrosio, Barbosa e Moraes (2026). A discussão dos desafios tecnológicos reúne estudos sobre acesso aos dados, preservação dos vestígios, capacidade pericial e confiabilidade das ferramentas automatizadas. Sem limitar a discussão a recortes geográficos locais, o artigo examina a tipologia dos crimes virtuais, os gargalos periciais da prova digital e o alcance regulatório do ECA Digital. A abordagem permite discutir a adequação das normas e os obstáculos descritos na literatura, sem pretender medir empiricamente sua efetividade no Brasil.

2 VULNERABILIDADE INFANTOJUVENIL E A TIPOLOGIA DOS CRIMES CIBERNÉTICOS

A especial vulnerabilidade de crianças e adolescentes no espaço virtual decorre não apenas da facilidade de manuseio das ferramentas tecnológicas, mas sobretudo do contínuo desenvolvimento cognitivo e emocional desses indivíduos, que influencia a percepção dos riscos inerentes ao ambiente conectado (PINHEIRO, 2024). Pesquisas sobre o uso da internet no Brasil, a exemplo dos levantamentos promovidos pelo Comitê Gestor da Internet (CGI.br)

e pelo CETIC.br, permitem compreender a presença desse público em mídias sociais e aplicativos de mensagens, bem como as diferentes condições de acompanhamento familiar. A familiaridade com os recursos digitais, portanto, não deve ser confundida com capacidade plena de reconhecer abordagens abusivas.

Conforme adverte Rogério Greco (2022), a responsabilidade penal exige a demonstração analítica de conduta típica, ilícita e culpável. No campo dos crimes digitais cometidos contra menores de idade, a doutrina distingue infrações cibernéticas próprias, quando o sistema informático é o bem jurídico diretamente atingido, e impróprias, quando a tecnologia funciona como meio de execução de delitos também praticáveis fora da rede. As condutas previstas nos artigos 240 a 241-D do Estatuto da Criança e do Adolescente, interpretadas à luz da definição do artigo 241-E, podem ser executadas ou ampliadas por meios digitais. A classificação doutrinária, contudo, não dispensa o exame dos elementos específicos de cada tipo penal.

A precisão desse enquadramento merece atenção também diante das alterações legislativas. A Lei nº 15.487/2026 atualizou dispositivos do ECA sobre violência sexual digital, contemplando conteúdos produzidos ou manipulados com inteligência artificial e modificando o artigo 241-D, que passou a alcançar o aliciamento de pessoa menor de quatorze anos (crianças), sendo que essa atualização não teve o condão de automatizar os delitos, permanecendo, no tipo, a necessidade de examinar-se a conduta, finalidade, e dos demais elementos legais, observada a irretroatividade da lei penal mais gravosa (BRASIL, 2026b).

Entre as modalidades delitivas de maior incidência e gravidade no espaço virtual, destaca-se o *grooming,* termo consagrado na literatura internacional e traduzido no ordenamento pátrio como aliciamento virtual de menores (SANTOS, 2021). Essa prática consiste no movimento progressivo de aproximação efetuado por adultos em redes sociais, fóruns e jogos online. O agressor assume perfis falsos ou manipula a identidade (inclusive simulando ser outra criança), estabelece vínculos de confiança afetiva com a vítima e, mediante coerção

psicológica ou oferta de benefícios digitais, induz o menor a produzir e compartilhar material de cunho sexual ou a agendar encontros presenciais para a prática de abusos.

O aliciamento online de menores (*Grooming*) consiste no trajeto inicial que orienta ao possível abuso sexual de crianças, mediante o uso de tecnologias, através das quais se estabelece uma relação de confiança com uma ou mais crianças, com o propósito de desenvolver condutas de cariz sexual." (SANTOS, 2021, p. 14)

A aproximação descrita pode ocorrer por etapas, com deslocamento da conversa de um espaço público para mensagens privadas e solicitação progressiva de segredo. Para a investigação, interessa compreender a sequência das interações, e não apenas localizar uma palavra ou uma imagem isolada. A idade declarada pelos interlocutores, as promessas e as ameaças precisam ser apreciadas no contexto, porque o sentido da abordagem pode depender de mensagens anteriores ou de contatos distribuídos entre diferentes serviços.

Outra manifestação predatória de extrema gravidade é a circulação de mídias designadas como Material de Abuso Sexual Infantil (MASI), expressão que evidencia a violência envolvida e evita tratar o conteúdo como simples produto pornográfico. Conforme documentado por Lowenkron (2015), a circulação dessas imagens permite examinar redes de produção, armazenamento, negociação e distribuição que podem utilizar tanto serviços abertos quanto ambientes de acesso restrito. A *deep web* compreende conteúdos não indexados pelos mecanismos de busca comuns e não se confunde integralmente com a *dark web*, que depende de recursos específicos de acesso. Transações em criptomoedas e conexões com outras formas de exploração podem integrar determinadas investigações, mas não constituem características necessárias de todo caso (CAMPOS, 2012).

Santos, Viana e Pinto (2026) contribuem para essa discussão ao aproximarem o aliciamento *online* das situações de exposição e exploração que podem favorecer o tráfico infantojuvenil, não sendo uma associação que permita a equivalência automática, o abuso pode ocorrer,

também, à distância, sem a necessidade de aproximação física com a vítima, enquanto para o tráfico é necessário pelo menos o animus voltado ao transporte físico da vítima. Nem todo compartilhamento de material ilícito integra uma rede de tráfico, assim como a inexistência de deslocamento internacional não afasta, por si só, a necessidade de investigar formas de exploração.

Ademais, verifica-se a proliferação da *sextorsão* e do *cyberbullying*. A *sextorsão* configura-se quando o agressor obtém fotos ou vídeos íntimos da vítima, seja por meio do *grooming*, da invasão de dispositivos ou de relacionamentos virtuais prévios, e passa a extorqui-la sob a ameaça de divulgar o conteúdo em redes sociais ou canais de mensagens instantâneas. Exige-se da vítima nova produção de mídias explícitas ou vantagens financeiras, gerando impactos emocionais devastadores que podem conduzir à automutilação e ao suicídio. Por sua vez, o *cyberbullying*, expressamente tipificado no Código Penal brasileiro pela Lei nº 14.811/2024, diferencia-se do *bullying* tradicional por sua capacidade de disseminação massiva e perenidade dos rastros virtuais, expondo o menor a agressões e humilhações públicas reiteradas sob a aparente proteção do anonimato.

No caso da *sextorsão*, a expressão descreve uma dinâmica de ameaça e exigência, cujo enquadramento depende do comportamento efetivamente praticado e da finalidade do agente. No *cyberbullying*, a investigação deve reconstruir a reiteração, o contexto e a participação dos envolvidos, sem confundir qualquer conflito pontual com intimidação sistemática. A pluralidade de participantes e o compartilhamento sucessivo de publicações tornam especialmente importante individualizar as condutas, em vez de atribuir a todos os usuários a mesma contribuição para o resultado.

A vulnerabilidade de crianças e adolescentes pode ser agravada pelo fenômeno do *sharenting*, caracterizado pelo compartilhamento da vida e da imagem dos filhos pelos pais ou responsáveis, que pode assumir formas excessivas ou abusivas (SCHERER; SANTOS, 2024). Essa exposição deixa registros digitais que podem ser copiados, retirados de contexto

e utilizados por terceiros, inclusive mediante ferramentas de inteligência artificial generativa na criação de conteúdos sintéticos ou *deepfakes* sexualizados. A possibilidade de reutilização indevida exige atenção à privacidade e ao melhor interesse da criança, sem permitir que qualquer publicação familiar seja automaticamente equiparada a crime.

A exposição familiar abusiva também exige afastar a culpabilização da vítima. O fato de uma criança utilizar redes sociais ou produzir uma imagem não transfere a ela a responsabilidade pela violência posterior, isso seria permitir uma criminalização e uma revitimização da criança. Conforme a discussão de Ambrosio, Barbosa e Moraes (2026), a proteção da privacidade deve acompanhar a inclusão digital. Isso envolve orientar responsáveis e usuários, mas também examinar como as aplicações ampliam a circulação do conteúdo e oferecem mecanismos de denúncia e proteção.

3 GARGALOS TECNOLÓGICOS, PERICIAIS E PROCESSUAIS NA INVESTIGAÇÃO

Se a tipificação penal dos crimes contra a infância encontra respaldo normativo sólido no Brasil, a efetiva persecução penal desses delitos esbarra em complexas barreiras tecnológicas e operacionais. A investigação digital demanda a transposição de obstáculos que vão desde a arquitetura de privacidade das redes até a sobrecarga das estruturas periciais oficiais (CULLEN et al., 2020; BREWER et al., 2026).

O primeiro grande gargalo investigativo reside nas barreiras de anonimato e criptografia. O emprego de criptografia de ponta a ponta (*end-to-end encryption*) nos aplicativos de mensagens limita o acesso ao conteúdo durante sua transmissão e pode impedir que o próprio provedor disponha de mensagens em formato legível. A existência de ordem judicial, por si só, não elimina essa limitação técnica, embora outras fontes de prova possam estar disponíveis. Somado a isso, a utilização de redes de anonimização, como a rede *Tor*, e de ambientes da *dark web* pode dificultar a identificação da origem das comunicações e das transações investigadas (DEMETIS; KIETZMANN, 2021).

Cumpre observar que criptografia e anonimização possuem usos legítimos na proteção da intimidade e da segurança das comunicações. Sua presença não constitui indício suficiente de atividade criminosa. O problema investigativo está no acesso lícito aos elementos necessários à apuração, respeitadas as garantias aplicáveis. A busca por respostas não autoriza equiparar a privacidade ao favorecimento do crime, sobretudo quando os próprios dados de crianças e adolescentes dependem dessa proteção.

A imputação de um delito cibernético exige mais do que associar um endereço IP a determinada pessoa. A análise deve considerar quem utilizava o dispositivo no momento do fato, o vínculo temporal entre os registros e a conduta investigada, a integridade dos dados obtidos e as hipóteses alternativas compatíveis com a prova (GRECO, 2022, p. 115).

Conforme ressalta a doutrina pericial, a mera identificação do titular de uma conta ou do proprietário de um endereço IP não estabelece, por si só, a autoria delitiva. O ambiente doméstico ou empresarial frequentemente conta com redes Wi-Fi compartilhadas, múltiplos usuários em um mesmo equipamento ou a possibilidade de invasões cibernéticas por softwares maliciosos (*malwares*). Assim, cabe à investigação policial demonstrar, com rigor técnico, o nexo de causalidade entre o indivíduo investigado e a ação criminosa específica praticada no ambiente virtual.

A reconstrução da autoria exige, portanto, o cruzamento de informações temporalmente compatíveis. Registros de acesso, dados do equipamento e comunicações podem se reforçar ou apontar inconsistências. Um arquivo encontrado em dispositivo compartilhado precisa ser relacionado às circunstâncias de sua obtenção e ao usuário investigado. A convergência desses elementos fortalece a atribuição, enquanto suas divergências devem ser explicitadas, inclusive para permitir o contraditório sobre as conclusões técnicas.

O segundo desafio crucial refere-se à preservação da prova digital e à observância da cadeia de custódia. O Código de Processo Penal, em seus artigos 158-A a 158-F, incluídos pelo

Pacote Anticrime, disciplina os procedimentos destinados a manter e documentar a história cronológica do vestígio. Diante da volatilidade das evidências digitais, que podem ser apagadas, alteradas ou corrompidas, a coleta exige procedimentos técnicos compatíveis com a fonte examinada. Cópias bit a bit, quando cabíveis, e funções *hash* permitem documentar a aquisição e verificar a integridade dos arquivos. Embora MD5 e SHA-256 apareçam na literatura forense, não oferecem as mesmas propriedades de segurança, portanto a escolha do método e suas limitações precisam ser justificadas no procedimento adotado (ELGOHARY et al., 2022).

A função *hash* auxilia a verificar se um conjunto de dados permaneceu igual entre dois momentos de comparação, mas não demonstra, isoladamente, que o conteúdo retrata um fato verdadeiro ou que foi produzido pelo investigado. Por isso, sua utilização precisa estar acompanhada do registro de origem, data, responsável pela coleta, ferramenta empregada e operações realizadas. A cadeia de custódia deve permitir reconstruir o percurso do vestígio e examinar a confiabilidade do resultado, como exige a preocupação com a documentação forense discutida por Elgohary et al. (2022).

De igual modo, uma captura de tela pode fornecer uma pista relevante, mas costuma apresentar apenas parte da interação. Sempre que possível e juridicamente autorizado, sua análise deve ser complementada por elementos que esclareçam a conta utilizada, o contexto e a sequência das mensagens. A recuperação de conteúdo apagado varia conforme o aplicativo, o dispositivo e as condições de extração, de modo que não pode ser prometida como resultado inevitável da perícia.

No que tange às regras de obtenção de dados, o Marco Civil da Internet (Lei nº 12.965/2014) fixou importantes parâmetros normativos. O artigo 13 estabelece a guarda dos registros de conexão pelo prazo de um ano, sob sigilo e em ambiente seguro. Já o artigo 15 prevê a retenção dos registros de acesso a aplicações por seis meses para os provedores abrangidos por seus requisitos. A preservação cautelar não se confunde com a entrega dos registros: os

artigos 10 e 22 disciplinam sua disponibilização mediante controle judicial, ressalvadas as hipóteses legais específicas. Também é necessário distinguir esses registros dos dados cadastrais referidos no artigo 10, § 3º. A investigação deve atuar prontamente e formular pedidos delimitados, evitando que o transcurso dos prazos comprometa a disponibilidade da prova.

A delimitação dos pedidos também permite diferenciar o registro de conexão, o acesso a uma aplicação e o conteúdo de uma conversa. Essas categorias não possuem a mesma função nem se submetem indistintamente às mesmas regras. Preservar dados antes de sua eliminação pode evitar uma perda irreversível, mas não autoriza acesso irrestrito ao material armazenado. A autoridade deve indicar a pertinência das informações e observar o procedimento legal correspondente.

Cabe registrar a hipótese específica introduzida no artigo 190-F do ECA pela Lei nº 15.487/2026: em situações qualificadas identificadas durante ronda virtual, admite-se a requisição direta dos registros de conexão ou dados cadastrais indicados na norma, com comunicação judicial em até quarenta e oito horas, sendo essa norma uma exceção que, por si só não autoriza acesso geral ao conteúdo das comunicações (BRASIL, 2026b).

O terceiro gargalo de magnitude dramática é o volume massivo de dados digitais e a limitação da capacidade pericial oficial. Investigações de combate à exploração infantil frequentemente resultam na apreensão de computadores, telefones celulares e servidores contendo *terabytes* de armazenamento. A triagem e a análise detalhada desse montante multimídia excedem a capacidade humana de processamento dos órgãos periciais de informática, gerando atrasos significativos na conclusão dos inquéritos policiais e esgotamento psíquico nos peritos incumbidos de visualizar materiais de extrema violência (LINDHOLM et al., 2024).

O dimensionamento de um caso, ademais, pode se alterar durante a apuração. Uma

denúncia inicialmente restrita a um perfil pode revelar outros interlocutores, dispositivos e vítimas. Lindholm et al. (2024), ao examinarem a organização das investigações na Suécia, identificam dificuldades de alocação de recursos e de colaboração entre unidades, problema também enfrentado no Brasil, dada as limitações de capacidade computacional também aqui existentes.

A definição de prioridades deve levar em conta a possibilidade de violência em curso e a necessidade de localizar e proteger as vítimas, pois a atenção prioritária sempre deve ser a preservação da vida, ainda que com isso possa se comprometer uma eventual produção de provas. A questão central não é otimizar a apreensão de um grande volume de provas, mas permitir que vidas sejam salvas.

Muitas das investigações relacionadas à crimes sexuais contra crianças e adolescentes cometidos na internet envolvem uma análise de grandes volumes de arquivos, como já dissemos, mas não é apenas o volume que apresentam dificuldades à investigação, há diversos outros fatores, conforme apresenta Cullen et al. (2020), como recursos, formação e trabalho multidisciplinar integram as condições da investigação. Além disso é essencial nessas análises a proteção das equipes diante da exposição reiterada a materiais violentos também merece atenção institucional, sem que o cuidado profissional seja visto como questão secundária à produção da prova.

Embora algoritmos de inteligência artificial e visão computacional possam acelerar a triagem de fotos e vídeos, essas ferramentas apresentam limitações técnicas, a comparação por funções *hash* perceptuais está sujeita a falhas e deve ser avaliada conforme as transformações aplicadas ao conteúdo, enquanto sistemas de estimativa de idade enfrentam dificuldades diante da qualidade da imagem ou da oclusão facial, e modelos de processamento de linguagem natural (NLP) podem não reconhecer a intenção de aliciamento em conversas aparentemente comuns, em todos os casos sendo necessária a supervisão humana para correção dessas falhas (SANTOS et al., 2024; RAJA; BOURS, 2023). Além disso,

mídias sintéticas geradas por IA exigem distinguir a autenticidade do registro, a forma de produção e a adequação jurídica da conduta, pois podem ser questionadas dada a problemática da possibilidade de alucinação, vieses, etc.

Nesse ponto, é necessário distinguir tarefas que frequentemente aparecem reunidas sob a expressão inteligência artificial. Reconhecer a semelhança com uma imagem conhecida, estimar idade e interpretar uma conversa são problemas diferentes enfrentados por tecnologias diversas. O resultado de uma ferramenta não pode ser transportado automaticamente para outra finalidade. A comparação perceptual discutida por Santos et al. (2024), por exemplo, deve ser compreendida conforme os objetivos e os limites do método utilizado, qualidade da resposta e eventuais limitações

A validação dessas ferramentas exige considerar falsos positivos e falsos negativos, isso é essencial pois uma classificação indevida pode direcionar recursos para material sem pertinência, enquanto uma omissão pode impedir a identificação de conteúdo relevante, em abos os casos isso pode gerar tanto a impunidade quanto injustiça. Modelos voltados ao *grooming* precisam lidar com a evolução da conversa e a linguagem indireta, além das palavras explícitas, questão relacionada à pesquisa de Raja e Bours (2023), que aponta para o que já foi dito, a necessidade da revisão humana e permitindo explicar os critérios empregados.

Por fim, a dimensão transnacional das redes sociais e a localização de servidores corporativos em jurisdições estrangeiras impõem morosidade às solicitações de cooperação jurídica internacional. O trâmite burocrático para o cumprimento de Cartas Rogatórias ou pedidos baseados no MLAT (Acordo de Assistência Jurídica Mútua em Matéria Penal) frequentemente colide com a urgência exigida para fazer cessar a exposição de crianças ou interromper ciclos ativos de abuso. Frisa-se, também, que a cooperação internacional não se limita, porém, à remessa de um pedido, não é apenas nisso que a questão se resume, é preciso identificar o serviço envolvido, formular solicitações suficientemente específicas e

acompanhar a preservação dos registros enquanto se busca o acesso autorizado. O problema pode decorrer tanto da localização dos dados quanto das exigências jurídicas incidentes sobre sua disponibilização, e as características e entreves legais em cada país. Da mesma forma, a fragmentação entre plataformas também exige integrar informações sem perder a identificação da origem de cada vestígio.

As transmissões ao vivo acrescentam uma dificuldade própria, pois nem sempre o conteúdo permanece armazenado no serviço, em alguns casos, inclusive, há uma impossibilidade de gravação dos registros ou uma criptografia que impede o seu registro, neste casos, registros de sessão, pagamentos e comunicações anteriores ou posteriores podem auxiliar a reconstrução, mas são provas indiretas que não substituem a prova do fato. A referência de Prinz e De Roos (2026) à detecção de autores nessa modalidade reforça a necessidade de examinar o conjunto dos vestígios disponíveis, evitando presumir tanto a ausência completa de registros quanto a recuperação garantida da transmissão.

Diante do exposto, o Quadro 1 relaciona os principais desafios às consequências para a apuração e aos cuidados que podem contribuir para uma resposta tecnicamente verificável. A síntese não propõe soluções universais, pois cada procedimento depende das características do caso e das autorizações legalmente exigidas.

Quadro 1 – Desafios da investigação tecnológica de crimes contra crianças e adolescentes

Desafio	Consequência investigativa	Cuidados necessários
Autoria e anonimização	Dificuldade de vincular contas e dispositivos à pessoa que praticou a conduta.	Cruzar registros, horários e contexto; examinar usos compartilhados e hipóteses alternativas.
Preservação dos vestígios	Perda ou alteração de dados e dúvidas sobre sua origem e integridade.	Preservar tempestivamente; documentar coleta, transferências e operações; verificar integridade.

Desafio	Consequência investigativa	Cuidados necessários
Volume de dados	Atraso na análise e dificuldade de reconhecer situações de violência em curso.	Priorizar riscos às vítimas; combinar triagem, revisão técnica e coordenação entre equipes. Importante a preservação da equipe quanto a superexposição de violência.
Automação e IA	Erros de classificação e interpretação insuficiente das interações.	Validar ferramentas; registrar limitações; submeter resultados à análise contextual e humana.
Transmissões ao vivo	Possível indisponibilidade do registro audiovisual após a transmissão.	Investigar vestígios de sessão, transações e comunicações, avaliando seu alcance probatório.
Dados em diferentes países	Dependência de plataformas e procedimentos de cooperação internacional.	Delimitar pedidos, preservar registros e acompanhar as vias de acesso legalmente cabíveis.

Fonte: elaboração dos autores, com base em Cullen et al. (2020), Lindholm et al. (2024), Santos et al. (2024), Raja e Bours (2023) e Prinz e De Roos (2026).

4 O ESTATUTO DIGITAL DA CRIANÇA E DO ADOLESCENTE (LEI Nº 15.211/2025) E A PROTEÇÃO COMPARTILHADA

Diante do descompasso entre a velocidade da criminalidade cibernética e a capacidade de resposta do aparato repressivo tradicional, o Poder Legislativo brasileiro promoveu avanço regulatório com a aprovação da Lei nº 15.211, de 17 de setembro de 2025. Denominada Estatuto Digital da Criança e do Adolescente e popularmente conhecida como “Lei Felca”, a norma complementa a proteção já estabelecida pelo ECA ao prever deveres específicos para fornecedores de produtos e serviços digitais e reforçar obrigações dos agentes envolvidos na proteção infantojuvenil (BETANIN, 2025).

A promulgação do ECA Digital ocorreu em meio à mobilização da sociedade civil e a debates institucionais sobre a erotização e a adultização de menores de idade em plataformas de

vídeos e redes sociais. Conforme destacado por Patrícia Peck Pinheiro (2025), a Lei nº 15.211/2025 fortalece um modelo de tutela fundado no dever de prevenção e na segurança desde a concepção dos serviços (*safety by design*). A participação de diferentes agentes nesse sistema deve ser compreendida segundo os deveres que a lei atribui a cada um, preservando a distinção entre proteção compartilhada e os regimes específicos de responsabilização.

O Estatuto Digital da Criança e do Adolescente é mais do que uma lei: é um manifesto pela infância. Ao redefinir os limites da publicidade, do design de plataformas e da monetização de conteúdo, o Brasil dá um passo firme rumo a um ambiente digital mais ético, inclusivo e protetivo (PECK, 2025, p. 3).

Entre os dispositivos de maior impacto investigativo da Lei nº 15.211/2025, destaca-se o artigo 27, dispositivo que obriga os fornecedores abrangidos a remover e comunicar às autoridades competentes os conteúdos de aparente exploração, abuso sexual, sequestro e aliciamento detectados em seus produtos ou serviços, na forma do regulamento. Seus parágrafos também disciplinam a retenção dos dados associados aos relatórios, em articulação com o artigo 15 do Marco Civil da Internet. A finalidade é permitir que a retirada de circulação seja acompanhada da preservação dos elementos necessários à apuração.

A remoção e a preservação atendem, portanto, a finalidades complementares. A primeira procura interromper a exposição e limitar a continuidade do dano; a segunda resguarda os elementos destinados à investigação. A comunicação de conteúdo aparente não equivale a uma decisão definitiva sobre a prática de crime, que deverá ser analisado pelas autoridades competentes para verificar os fatos, identificar os responsáveis e examinar a confiabilidade das informações encaminhadas.

A nova legislação também estabelece, em seu artigo 6º, medidas de prevenção e mitigação de riscos desde a concepção e ao longo da operação das aplicações, complementadas pelas

configurações protetivas do artigo 7º. Além disso, o artigo 23 veda a monetização e o impulsionamento dos conteúdos que retratem crianças e adolescentes de forma erotizada ou sexualmente sugestiva, buscando com isso atingir os incentivos econômicos dessa exposição, sem que a proibição dispense o exame dos requisitos de eventual infração penal.

Paralelamente aos deveres das empresas de tecnologia, o ECA Digital reforçou a supervisão parental. O artigo 6º, § 1º, preserva a atuação dos pais e responsáveis na prevenção de violações, enquanto os artigos 17 e 18 disciplinam ferramentas acessíveis de acompanhamento. Entre suas funções estão o gerenciamento das opções de conta e privacidade, a restrição de transações financeiras, a identificação dos perfis de adultos com os quais a criança ou o adolescente se comunica e o acesso a métricas consolidadas de tempo de uso. Tais recursos devem ser compreendidos segundo a autonomia progressiva e o melhor interesse dos usuários protegidos.

De outro lado está, nas casas, o acompanhamento familiar do uso da internet, que não deve significar a instauração de um "regime de vigilância constante" nas casas, devendo pautar-se pela idade, o desenvolvimento da criança, a necessidade de construir confiança e autonomia para que ameaças sejam comunicadas, e permitindo o amadurecimento do jovem no uso da internet. A atuação extremamente dura dos responsáveis, com punições, ameaças, acaba por atrapalhar mais do que auxiliar a resolver o problema, pois dissuade o jovem a pedir ajuda, neste caso o controle excessivo pode dificultar o conhecimento da violência. A atuação dos responsáveis deve, assim, combinar orientação, uso adequado dos recursos disponíveis e acolhimento diante de indícios de abuso.

A atuação da família coincide com o pensamento de Nucci (2025), apara quem a proteção infantojuvenil no ambiente digital não pode recair exclusivamente sobre as forças policiais ou sobre o Poder Judiciário. O acompanhamento parental ativo constitui uma frente de proteção contra o aliciamento virtual, sem garantir também, por si só, que toda violência será evitada, tornando-se mais uma frente de proteção, interna, às crianças e adolescentes. Da mesma

forma deve haver uma consciência dos responsáveis quanto a exposição abusiva da imagem e da intimidade dos filhos, que pode produzir consequências civis e administrativas e, quando preenchidos os elementos de um tipo penal, e também consequências criminais.

A regulamentação da Lei nº 15.211/2025 foi desenvolvida pelo Decreto Presidencial nº 12.880/2026, que também instituiu a Política Nacional de Promoção e Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital. O diploma deve ser lido em articulação com as diretrizes da Resolução nº 245/2024 do CONANDA, reafirmando que o acesso à internet deve ser acompanhado de segurança, educação digital e respeito aos direitos de crianças e adolescentes.

A responsabilidade compartilhada pela proteção não elimina a distinção entre os planos administrativo, civil e penal. Falhas de prevenção podem justificar a atuação fiscalizatória e outras consequências previstas em lei, mas a imputação criminal exige identificar a conduta da pessoa investigada e sua adequação a um tipo penal. Não se presume responsabilidade penal pela simples participação em uma plataforma, pelo vínculo familiar ou pela posição ocupada em uma empresa. Essa delimitação mantém a responsabilidade penal vinculada à conduta comprovada, sem enfraquecer os deveres preventivos.

No atendimento às vítimas, a obtenção da prova precisa respeitar a condição peculiar de desenvolvimento, e para isso a Lei nº 13.431/2017 disciplina a escuta especializada e o depoimento especial, instrumentos que são essenciais para reduzir a revitimização, pois a necessidade de esclarecer os fatos não justifica a repetição desnecessária de relatos nem a circulação indevida de imagens íntimas da vítima. Preservar a prova e limitar o acesso ao conteúdo sensível são providências compatíveis com uma investigação comprometida com os direitos das crianças e dos adolescentes (BRASIL, 2017).

Santos, Viana e Pinto (2026) destacam a relevância dos instrumentos preventivos no Brasil para enfrentar o aliciamento e a exploração, da mesma forma que Ambrosio, Barbosa e

Moraes (2026), que defendem a ampliação da segurança nas redes sob a ótica formal. Contudo, a existência formal de deveres mais específicos não é suficiente, por si só, redução dos crimes ou maior rapidez investigativa, a materialização desse conjunto na prática dependerá da implementação do conjunto normativo, a qualidade de atuação das agências envolvidas e a própria avaliação prática das políticas concretamente aplicadas.

CONCLUSÃO

A transposição da vida social para a esfera virtual reconfigurou os contornos da criminalidade, impondo ao ordenamento jurídico e aos órgãos de persecução penal a imperiosa necessidade de modernização conceitual e operacional. A proteção de crianças e adolescentes contra os crimes cibernéticos, tais como o *grooming*, a difusão de material de abuso sexual infantil, a sextorsão, o cyberbullying e as práticas de erotização precoce, consubstancia uma exigência premente do Estado Democrático de Direito, fundada no princípio constitucional da prioridade absoluta e na doutrina da proteção integral (art. 227 da Constituição Federal).

Conforme demonstrado ao longo desta reflexão, a investigação tecnológica de delitos praticados no ciberespaço enfrenta complexos gargalos operacionais. O emprego de mecanismos de criptografia e anonimização para dificultar a identificação de crimes, a volatilidade das evidências eletrônicas, a necessidade de documentar a cadeia de custódia (art. 158-A do CPP) e a escassez de infraestrutura pericial diante de grandes volumes de dados representam obstáculos à elucidação dos fatos. A automação por inteligência artificial, embora útil à triagem, não substitui o exame pericial nem resolve, isoladamente, as ambiguidades contextuais das interações virtuais.

Nesse cenário, o Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025 – "Lei Felca"), regulamentado pelo Decreto nº 12.880/2026, ampliou os deveres de proteção no ambiente digital. A comunicação e a remoção de conteúdos abrangidos pelo artigo 27,

acompanhadas da retenção dos dados previstos em lei, aproximam a prevenção das necessidades investigativas. As medidas sobre configurações protetivas, supervisão parental e incentivos econômicos da exposição infantil também contribuem para esse sistema, cuja efetividade depende da aplicação concreta e da fiscalização.

A discussão permite responder ao problema de pesquisa ao indicar que as barreiras tecnológicas interferem na responsabilização quando dificultam a preservação dos vestígios, sua interpretação e a vinculação da conduta a uma pessoa determinada. Os deveres preventivos podem contribuir para interromper violações e disponibilizar elementos úteis, mas não substituem a investigação. O cuidado com a cadeia de custódia, a contextualização dos registros e a individualização das condutas permanecem condições para uma resposta penal fundamentada.

Conclui-se que o combate aos crimes cibernéticos contra crianças e adolescentes não pode ser alcançado mediante o simples recrudescimento do punitivismo penal. Exige-se a consolidação de uma rede de proteção compartilhada entre o Estado, as empresas de tecnologia, as instituições de ensino e a família, com atribuições e responsabilidades juridicamente delimitadas. Para que as garantias legais não se convertam em letra morta, é indispensável investir na capacitação das equipes especializadas, na cooperação internacional e no letramento digital. A resposta estatal deve proteger as vítimas em tempo oportuno e produzir provas verificáveis, assegurando simultaneamente as condições de uma responsabilização penal individualizada.

REFERÊNCIAS

AMBROSIO, Gleiner Pedroso Ferreira; BARBOSA, André Luís Jardini; MORAES, Ana Paula Bagaiolo. Sociedade digital e o ECA: um estudo sobre proteção de crianças e adolescentes no ambiente de rede e o combate à violência digital. Revista Juris UniToledo, Araçatuba, v. 11, n. 1, p. 1-25, 2026.

ARENDT, Hannah. Sobre a violência. Tradução de Maria Claudia Drummond Trindade. Brasília: Editora Universidade de Brasília, 1985.

BETANIN, Camila. “Lei Felca”: O ECA Digital que redefine a proteção infantil na internet brasileira. Migalhas, 2 out. 2025. Disponível em: https://www.migalhas.com.br. Acesso em: 15 out. 2026.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Brasília, DF: Presidência da República, 1940.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Brasília, DF: Presidência da República, 1941.

BRASIL. Decreto nº 12.880, de 18 de março de 2026. Regulamenta a Lei nº 15.211/2025. Brasília, DF: Presidência da República, 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.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Brasília, DF: Presidência da República, 2014.

BRASIL. Lei nº 14.811, de 15 de janeiro de 2024. Altera o Código Penal e o Estatuto da Criança e do Adolescente para instituir medidas de proteção à criança e ao adolescente contra a violência nos estabelecimentos educacionais e no ambiente virtual. Brasília, DF: Presidência da República, 2024.

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.

BREWER, Christopher G. et al. "…it's Google that's big brother": The symbiosis between ICAC investigators and the private sector regarding encryption and privacy. International Journal of Police Science & Management, v. 28, p. 113-125, 2026.

CAMPOS, Bruno Digiovanni Lins Cajazeira de Macedo. Criança: o canivete suíço do tráfico de pessoas. 2012. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal do Paraná, Curitiba, 2012.

CONSELHO NACIONAL DOS DIREITOS DA CRIANÇA E DO ADOLESCENTE (CONANDA). Resolução nº 245, de 5 de abril de 2024. Dispõe sobre os direitos de crianças e adolescentes em ambiente digital. Brasília, DF: CONANDA, 2024.

CULLEN, Olivia et al. "Our Laws Have Not Caught up with the Technology": Understanding Challenges and Facilitators in Investigating and Prosecuting Child Sexual Abuse Materials in the United States. Laws, v. 9, n. 4, p. 28, 2020.

DEMETIS, Dionysios S.; KIETZMANN, Jan. Online Child Sexual Exploitation: A New MIS Challenge. Journal of the Association for Information Systems, v. 22, n. 1, p. 9, 2021.

ELGOHARY, Hany M.; DARWISH, S.; ELKAFFAS, S. Improving Uncertainty in Chain of Custody for Image Forensics Investigation Applications. IEEE Access, v. 10, p. 14669-14679, 2022.

GALTUNG, Johan. Nonviolence and deep culture: Some hidden obstacles. Peace Research, v. 27, p. 21-37, 1995.

GRECO, Rogério. Curso de Direito Penal: parte geral. 24. ed. Niterói: Impetus, 2022.

LINDHOLM, Alva et al. The Investigation of Online Child Sexual Abuse Cases in Sweden. Nordic Journal of Studies in Policing, v. 11, n. 1, p. 7, 2024.

LOWENKRON, Laura. Pornografia infantil na internet: pedofilia e exploração sexual de crianças e adolescentes. Rio de Janeiro: Ed. UERJ, 2015.

NUCCI, Guilherme de Souza. ECA digital e responsabilidade dos pais. São Paulo: Guilherme Nucci, 2025. Disponível em: https://guilhermenucci.com.br. Acesso em: 10 out. 2026.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Protocolo Adicional à Convenção das Nações Unidas contra o Crime Organizado Transnacional Relativo à Prevenção, Repressão e Punição do Tráfico de Pessoas, em Especial Mulheres e Crianças (Protocolo de Palermo). Promulgado pelo Decreto nº 5.017, de 12 de março de 2004. Brasília, DF, 2004.

PINHEIRO, Patrícia Peck. Direito digital: responsabilidade legal e ética para a era da inteligência artificial. 10. ed. São Paulo: Saraiva Educação, 2024.

PECK, Patrícia. O novo Estatuto Digital da Criança e do Adolescente e seus efeitos. Meio & Mensagem, São Paulo, 30 set. 2025.

PRINZ, M.; DE ROOS, Melissa S. Profiling the Invisible: A Scoping Review of Characteristics and Detection of Live-Streaming Child Sexual Abuse Offenders. Journal of Child Sexual Abuse, v. 35, p. 589-613, 2026.

RAJA, K.; BOURS, P. Detecting Online Grooming By Simple Contrastive Chat Embeddings. In: ACM INTERNATIONAL WORKSHOP ON SECURITY AND PRIVACY ANALYTICS, 9., 2023. Proceedings... New York: ACM, 2023.

ROUSSEAU, Jean-Jacques. O contrato social. Tradução de Lourdes Santos Machado. São Paulo: Abril Cultural, 1973.

SANTOS, Gabriele Alice da Silva; VIANA, Johnnatan Reges; PINTO, Emanuel Vieira. ECA Digital (Lei 15.211/2025): o aliciamento online no Brasil e a sua relação com o tráfico de crianças e adolescentes. Revista Ibero-Americana de Humanidades, Ciências e Educação, São Paulo, v. 12, n. 7, p. 1-22, 2026.

SANTOS, Hericson dos et al. ChaSAM: An Architecture Based on Perceptual Hashing for Image Detection in Computer Forensics. IEEE Access, v. 12, p. 104611-104628, 2024.

SCHERER, Débora Kelly; SANTOS, Jordana Borba dos. O Sharenting e a Responsabilidade Parental na Proteção de Dados Pessoais de Crianças e Adolescentes. Revista de Direito da FADERGS, Porto Alegre, v. 9, n. 1, p. 1-17, 2024.

---

[1] Graduanda em Direito pela Faculdade Serra do Carmo (FASEC).

[2] Doutorando em Educação UFPA/UFT. Mestre em Prestação Jurisdicional e Direitos Humanos. Especialista em Direito Administrativo e em Ciências Criminais. Graduado em Direito e em Comunicação Social (jornalismo) – todos pela Universidade Federal do Tocantins (UFT). Delegado da Polícia Civil do Tocantins.