Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v11i5.19180

RESPONSABILIDADE PENAL NO ANONIMATO DIGITAL: OS DESAFIOS DE INVESTIGAÇÕES E PROVA À LUZ DA LEI 14.811/2024

CRIMINAL LIABILITY IN DIGITAL ANONYMITY: CHALLENGES OF INVESTIGATION AND EVIDENCE UNDER LAW NO. 14,811/2024

Dyéssica Thaís Santos Oliveira[1]
Aline Sales da Cunha[2]
Hernando Fernandes Silva[3]

RESUMO: O presente artigo científico teve como objetivo analisar os principais desafios enfrentados pelas autoridades brasileiras na responsabilização penal de crimes praticados sob anonimato digital, à luz da Lei nº 14.811/2024. A pesquisa foi conduzida por meio do método dedutivo, utilizando material doutrinário, legislação constitucional e infraconstitucional, jurisprudência nacional, artigos científicos, monografias e documentos técnicos. O estudo abordou aspectos como as limitações jurídicas impostas pelo Marco Civil da Internet, pela Lei Geral de Proteção de Dados e pela Constituição Federal, bem como os obstáculos técnicos relacionados à produção de provas digitais e à atuação das plataformas online. Também foram exploradas propostas de reformas legislativas, investimentos em tecnologia forense, mediação de conflitos e educação digital como medidas de aprimoramento. A análise demonstrou que, embora a legislação tenha avançado, a efetividade da responsabilização penal ainda depende de ajustes normativos, operacionais e institucionais.

Palavras-chave: Responsabilidade Penal. Anonimato Digital. Cyberbullying. Lei nº 14.811/2024. Provas Digitais.

ABSTRATC: This scientific article aimed to analyze the main challenges faced by Brazilian authorities in the criminal liability of offenses committed under digital anonymity, in light of Law No. 14,811/2024. The research followed a deductive method, using doctrinal material, constitutional and infra-constitutional legislation, national jurisprudence, academic articles, monographs, and technical documents. The study addressed legal constraints imposed by the Brazilian Internet Civil Framework, the General Data Protection Law, and the Federal Constitution, as well as technical barriers to the production of digital evidence and the role of online platforms. It also explored proposals for legislative reform, investment in forensic technology, conflict mediation, and digital education as measures for improvement. The analysis showed that, although the legislation has progressed, the effectiveness of criminal liability still depends on normative, operational, and institutional adjustments.

Keywords: Criminal Liability. Digital Anonymity. Cyberbullying. Law No. 14,811/2024. Digital Evidence.

[1]Acadêmica do curso de Direito do Centro Universitário Una, campus Bom Despacho, da rede Ânima Educação.
[2]Acadêmica do curso de Direito do Centro Universitário Una, campus Bom Despacho, da rede Ânima Educação. Orientadora.
[3]Advogado. Professor Universitário. Mestre em Educação. Especialista em Direito e Processo do Trabalho. Especialista em Direito Administrativo. Especialista em Gerenciamento de Micro e Pequena Empresa. Especialista em Direito Civil e Processo Civil. Bacharel em Direito. Especialista em Advocacia no Direito Digital e Proteção de Dados. Graduado em História.

1. INTRODUÇÃO

O avanço tecnológico e a digitalização das relações sociais impulsionaram uma nova configuração da criminalidade, marcada pela crescente incidência de delitos praticados no meio virtual. Entre esses crimes, destacaram-se condutas como fraudes eletrônicas, disseminação de conteúdos ofensivos, divulgação de imagens íntimas sem consentimento e, especialmente, o cyberbullying. A principal dificuldade enfrentada pelas autoridades judiciais e policiais residiu na responsabilização penal de infratores que se ocultaram sob o manto do anonimato digital (Soares, 2023).

A utilização de mecanismos como redes privadas virtuais (VPNs), perfis falsos e redes descentralizadas tornou recorrente a prática de crimes com a ocultação da identidade do autor, o que dificultou a atuação do Estado na persecução penal. Conforme apontado por Nunes (2022), a identificação do agente criminoso passou a depender de processos técnicos sofisticados, muitas vezes inacessíveis às autoridades brasileiras em razão de limitações estruturais e jurídicas.

Para enfrentar esse cenário, o legislador brasileiro promulgou a Lei nº 14.811/2024, que incluiu no Código Penal o artigo 146-A, tipificando as condutas de bullying e cyberbullying, com previsão expressa para atos praticados em ambientes virtuais e com uso de anonimato. Segundo Dos Santos e Taporosky Filho (2024), a referida lei buscou preencher lacunas legais e ampliar a proteção a crianças e adolescentes, em conformidade com os direitos fundamentais garantidos pela Constituição Federal.

Entretanto, a simples criação de tipos penais não solucionou integralmente os desafios das investigações digitais. A obtenção de provas válidas e a identificação dos autores dos crimes continuaram a esbarrar em limites legais estabelecidos por diplomas como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), os quais, embora essenciais para a proteção da privacidade dos usuários, também restringiram o acesso indiscriminado a dados por parte das autoridades (Brasil, 2014; Brasil, 2018).

Diante desse panorama, o presente artigo teve como objetivo geral analisar de que forma a Lei nº 14.811/2024 contribuiu para superar os principais desafios à responsabilização penal de autores de crimes praticados sob anonimato digital. A partir desse objetivo central, foram definidos os seguintes objetivos específicos:

> Identificar os dispositivos legais da Lei nº 14.811/2024 relacionados à investigação e responsabilização penal de crimes cibernéticos;
> Discutir os limites legais impostos pelo Marco Civil da Internet, pela LGPD e pela Constituição Federal ao rastreamento de criminosos no ambiente digital;

Analisar os desafios técnicos enfrentados por autoridades competentes no processo de investigação digital;
Apontar soluções normativas, operacionais e técnicas que possam aprimorar a efetividade das medidas legais no combate ao anonimato criminoso online.

A justificativa para a escolha do tema fundamentou-se na urgência da discussão sobre o uso da tecnologia como instrumento de perpetração de crimes e sobre os mecanismos legais disponíveis para responsabilizar penalmente os infratores, especialmente em um contexto marcado pelo crescente número de ataques virtuais, muitos deles direcionados a crianças e adolescentes (Araújo, 2024).

Além disso, dados de 2023 da Polícia Federal indicaram que as denúncias de crimes praticados por meio de perfis anônimos aumentaram em mais de 40%, revelando a importância da atualização das ferramentas investigativas e da revisão do aparato normativo nacional (Fernandez; Corrêa, 2024). A responsabilidade das plataformas digitais e sua colaboração com o sistema de justiça também emergiram como pontos críticos, conforme exposto por Cristiny, Correia e Queiroz (2025), que analisaram o papel da mediação tecnológica na identificação de agressores virtuais.

Observou-se, ainda, que o fenômeno do anonimato digital está diretamente associado à sensação de impunidade. Isso intensificou os riscos e danos gerados pelas condutas criminosas na internet. Para Taborda e Sippert (2024), a ausência de medidas eficazes de responsabilização comprometeu os direitos das vítimas, limitando o acesso à justiça e a pacificação social, pilares fundamentais do Estado Democrático de Direito.

Dessa forma, este artigo propôs-se a investigar os instrumentos legais e operacionais disponíveis para enfrentar o desafio do anonimato nas práticas delituosas cibernéticas, sob a perspectiva da recente Lei nº 14.811/2024. O estudo teve como base uma abordagem qualitativa e descritiva, centrada na análise documental da legislação, de artigos científicos e de pareceres jurídicos atualizados entre os anos de 2020 a 2025.

A relevância do tema residiu no fato de que, embora o ordenamento jurídico brasileiro venha avançando no campo da proteção penal digital, ainda persiste um descompasso entre a velocidade da evolução tecnológica e a capacidade normativa e institucional do Estado em acompanhar essas transformações (Santos; Braz, 2024). Essa lacuna revelou-se especialmente preocupante quando se consideraram os crimes com impacto direto sobre a saúde mental e a integridade psíquica de vítimas em fase de desenvolvimento, como ocorre com o cyberbullying.

Concluiu-se, portanto, que discutir a responsabilização penal no contexto do anonimato digital tornou-se imperativo diante dos impactos sociais, jurídicos e psicológicos dos crimes cibernéticos. A Lei nº 14.811/2024, nesse sentido, representou uma oportunidade para revisar os instrumentos existentes, estabelecer novos parâmetros de atuação investigativa e refletir sobre os limites entre privacidade, liberdade de expressão e dever de punir.

2. O ANONIMATO DIGITAL E OS DESAFIOS DA RESPONSABILIZAÇÃO PENAL

2.1 CONCEITO DE ANONIMATO DIGITAL E SUA APLICAÇÃO NO CIBERESPAÇO

O anonimato digital consistiu na ocultação deliberada da identidade de um indivíduo em ambientes virtuais, com o objetivo de dificultar ou impedir sua identificação. Essa prática tornou-se comum no ciberespaço, sendo utilizada tanto por usuários legítimos, que desejavam preservar sua privacidade, quanto por agentes mal-intencionados, que se valiam dessa condição para a prática de crimes. De acordo com Nunes (2022), o anonimato digital envolveu a supressão ou disfarce de informações que permitiriam a identificação do usuário, tais como endereço de IP, localização geográfica, ou dados de login e autenticação.

A internet, por sua estrutura descentralizada e pela possibilidade de navegação sem autenticação obrigatória, favoreceu a disseminação do anonimato como fenômeno social e jurídico. Soares (2023) observou que, nas redes sociais, fóruns e aplicativos de mensagens, tornou-se comum o uso de perfis falsos ou identidades anônimas para disseminar discursos de ódio, ameaças e conteúdo difamatório. Essa prática não apenas fragilizou as relações interpessoais, mas também representou um obstáculo à atuação do Estado na apuração de crimes, especialmente aqueles que afetaram direitos fundamentais de crianças e adolescentes.

A utilização do anonimato em ambientes digitais suscitou, portanto, uma tensão entre o direito à liberdade de expressão e o dever de responsabilização penal. Segundo Araújo (2024), embora o anonimato estivesse protegido constitucionalmente em alguns contextos, sua aplicação indiscriminada em crimes virtuais exigiu uma revisão do papel das ferramentas jurídicas disponíveis, dado o elevado número de delitos cometidos sob essa condição.

2.2 MEIOS TECNOLÓGICOS DE OCULTAÇÃO DA IDENTIDADE ONLINE (VPN, DEEP WEB, PERFIS FALSOS)

Diversos recursos tecnológicos foram empregados para ocultar a identidade de usuários em ambientes digitais. Entre os mais utilizados, destacaram-se as redes privadas virtuais

(VPNs), a navegação pela deep web e a criação de perfis falsos em plataformas digitais. Conforme Nunes (2022), o uso de VPN permitiu mascarar o endereço de IP do usuário, redirecionando a conexão para servidores localizados em outros países e dificultando, assim, a identificação da origem da comunicação.

A navegação pela deep web, por meio de navegadores como o Tor, também viabilizou a prática de crimes em redes que não eram indexadas pelos mecanismos de busca convencionais. Soares (2023) alertou que ambientes como esses foram amplamente explorados por criminosos digitais para a comercialização de dados roubados, exploração infantil, tráfico de drogas e incitação à violência. O caráter criptografado e descentralizado dessas redes inviabilizou, em muitos casos, a atuação de autoridades nacionais.

A criação de perfis falsos, por sua vez, foi amplamente empregada em redes sociais e aplicativos de mensagens, com o intuito de difamar, ameaçar ou assediar outros usuários, sem risco de identificação imediata. De acordo com Santos e Braz (2024), essa prática foi observada com maior frequência entre adolescentes e jovens, que criavam contas paralelas para praticar cyberbullying ou incitar comportamentos violentos. Tais condutas, embora passíveis de responsabilização penal, eram frequentemente negligenciadas pela dificuldade em comprovar a autoria.

Esse conjunto de ferramentas tecnológicas de ocultação, ao mesmo tempo em que serviu como instrumento de proteção à privacidade, também foi apropriado por infratores com o objetivo de frustrar a ação penal. Araújo (2024) ressaltou que a sofisticação dessas estratégias exigiu das autoridades uma resposta jurídica e técnica igualmente complexa, o que nem sempre foi possível diante das limitações estruturais do sistema de justiça criminal.

2.3 DIFICULDADES JURÍDICAS NA IDENTIFICAÇÃO DE AUTORES ANÔNIMOS

A identificação de autores de crimes cibernéticos, especialmente quando cometidos sob anonimato digital, revelou-se um dos maiores desafios enfrentados pelas autoridades públicas. Conforme Soares (2023), a coleta de informações em ambiente virtual dependia de ordens judiciais, cooperação com provedores de serviço e respeito à legislação de proteção de dados, o que tornava o processo investigativo lento e muitas vezes ineficaz.

A legislação brasileira, embora avançada em termos de garantias individuais, mostrou-se deficiente quanto à articulação entre normas penais e ferramentas digitais de investigação. Nunes (2022) destacou que a ausência de regulamentação clara sobre a rastreabilidade de

usuários em redes sociais e aplicativos de mensagens comprometeu a eficácia de medidas cautelares, como a quebra de sigilo de dados cadastrais.

Além disso, a jurisdição internacional das plataformas digitais, cujos servidores estavam, em sua maioria, localizados fora do território nacional, impôs entraves adicionais. Segundo Araújo (2024), a obtenção de informações por meio de cartas rogatórias ou acordos de cooperação internacional nem sempre resultava em respostas tempestivas, o que comprometia a cadeia de custódia das provas e favorecia a impunidade.

Do ponto de vista penal, o Código Penal brasileiro não foi suficientemente atualizado para acompanhar a evolução dos crimes virtuais. Embora o Decreto-Lei nº 2.848/1940 previsse sanções para crimes contra a honra, ameaças e outros delitos cometidos por meios eletrônicos, sua aplicação dependia da identificação do agente e da materialização da conduta, elementos muitas vezes inviabilizados pelo anonimato (Brasil, 1940).

2.4 IMPACTOS DO ANONIMATO NA PERSECUÇÃO PENAL E IMPUNIDADE

A impossibilidade de identificar autores de crimes virtuais anônimos repercutiu diretamente na eficácia da persecução penal. Conforme Santos e Braz (2024), muitos inquéritos foram arquivados por ausência de autoria conhecida, mesmo havendo indícios claros de materialidade delitiva. Esse cenário contribuiu para a sensação de impunidade e para a banalização do crime cibernético entre usuários.

A fragilidade investigativa decorrente do anonimato também impactou negativamente as vítimas, que se sentiram desamparadas diante da lentidão e da ineficácia do sistema judicial. Araújo (2024) destacou que esse sentimento de insegurança jurídica foi particularmente grave em casos que envolveram crianças e adolescentes, cujos danos psicológicos foram potencializados pela ausência de respostas estatais.

Por fim, a percepção de que o ambiente virtual era "terra sem lei" incentivou a prática recorrente de delitos digitais. Soares (2023) observou que, sem um mecanismo eficaz de responsabilização penal, o anonimato deixou de ser apenas um desafio técnico para tornar-se um catalisador da criminalidade moderna. Nunes (2022) complementou que, nesse contexto, o Direito Penal precisou ser repensado, de modo a incorporar instrumentos tecnológicos e normativos capazes de reverter essa lógica de impunidade.

3. A LEI 14.811/2024 E A PREVENÇÃO DE CRIMES VIRTUAIS: AVANÇOS E LIMITES

3.1 HISTÓRICO E OBJETIVOS DA LEI Nº 14.811/2024

A promulgação da Lei nº 14.811/2024 representou um marco na legislação brasileira voltada à proteção de crianças e adolescentes, especialmente no contexto da violência escolar e dos crimes praticados em ambientes digitais. Essa norma introduziu alterações relevantes no Código Penal, no Estatuto da Criança e do Adolescente (ECA) e na Lei de Diretrizes e Bases da Educação Nacional (LDB), com o intuito de fortalecer o enfrentamento à violência infantojuvenil (Imprensa Nacional, 2024).

Conforme exposto por Dos Santos e Taporosky Filho (2024), a criação da lei respondeu a uma crescente demanda social por instrumentos mais eficazes de combate ao bullying e ao cyberbullying, ambos fenômenos em franca ascensão no Brasil e no mundo. Os autores destacaram que a legislação surgiu em um contexto de urgência, após sucessivos casos de ataques em escolas e de exposição digital de crianças e adolescentes, o que pressionou o legislador a agir.

O principal objetivo da nova legislação consistiu em reconhecer penalmente práticas que, até então, eram tratadas no campo da moralidade ou da responsabilidade civil, conferindo maior segurança jurídica às vítimas e atribuindo responsabilidade objetiva aos agressores. Segundo Cristiny, Correia e Queiroz (2025), a lei também se alinhou às diretrizes internacionais de proteção dos direitos da infância, especialmente no que diz respeito à proteção no ambiente digital.

Adicionalmente, a lei buscou reforçar o papel das instituições escolares, exigindo o desenvolvimento de políticas de prevenção à violência, protocolos de atuação diante de ameaças e integração com os órgãos de segurança pública. Essa abordagem multidisciplinar e preventiva foi apontada por Junior e Taporosky Filho (2024) como um avanço significativo em relação às normativas anteriores, que tratavam o bullying de forma fragmentada.

3.2 ARTIGO 146-A DO CÓDIGO PENAL E SUAS IMPLICAÇÕES PENAIS

A principal inovação trazida pela Lei nº 14.811/2024 foi a inclusão do artigo 146-A no Código Penal, que passou a tipificar os crimes de bullying e cyberbullying. O tipo penal definiu o bullying como "intimidar sistematicamente, individualmente ou em grupo, mediante violência física ou psicológica, uma ou mais pessoas, de modo intencional e repetitivo, sem

motivação evidente" (Brasil, 2024). Já o cyberbullying, previsto no parágrafo único, trata da mesma conduta quando realizada em ambiente virtual.

Segundo Junior e Taporosky Filho (2024), essa tipificação representou um avanço jurídico ao consolidar condutas recorrentes, mas de difícil enquadramento penal, em um artigo próprio. Antes da promulgação, tais comportamentos eram tratados com base em tipos penais genéricos, como injúria, ameaça ou difamação, o que gerava lacunas na proteção das vítimas e na punição dos agressores.

O parágrafo único do artigo 146-A previu pena de reclusão de dois a quatro anos e multa para o cyberbullying, tornando mais rígida a repressão a essa conduta no meio digital. Cristiny, Correia e Queiroz (2025) salientaram que a criação dessa figura penal buscou desestimular o uso da internet como espaço de violência e impunidade, estabelecendo parâmetros claros para a responsabilização penal, inclusive quando a ação for praticada sob anonimato.

Além disso, a nova lei permitiu aumento de pena quando o crime for cometido contra crianças ou adolescentes, ou quando houver divulgação de conteúdo ofensivo em larga escala, o que é comum nas redes sociais. Segundo Dos Santos e Taporosky Filho (2024), essa medida buscou combater a viralização de ataques pessoais e preservar a dignidade das vítimas em um contexto de hipervisibilidade digital.

3.3 APLICAÇÃO PRÁTICA DA LEI EM CASOS DE CYBERBULLYING E CRIMES CONTRA MENORES

No campo prático, a aplicação da Lei nº 14.811/2024 ainda enfrentou desafios estruturais, embora tenha representado um passo importante no combate à violência virtual. Desde sua entrada em vigor, órgãos de segurança pública e promotorias passaram a utilizar o novo tipo penal em denúncias que antes não encontravam tipificação adequada no Código Penal (Brasil, 2024).

Cristiny, Correia e Queiroz (2025) analisaram os primeiros meses de vigência da norma e apontaram que o artigo 146-A foi aplicado, sobretudo, em casos envolvendo crianças e adolescentes que sofreram ataques sistemáticos por meio de redes sociais, grupos escolares online e aplicativos de mensagens instantâneas. Contudo, a efetividade da norma ainda esbarrou em dificuldades técnicas relacionadas à identificação dos autores, especialmente em contextos de anonimato digital.

Junior e Taporosky Filho (2024) reforçaram que, apesar da clareza do novo tipo penal, a atuação das instituições de ensino continuou sendo um fator determinante para a prevenção e notificação de casos. Muitos colégios ainda não contavam com canais estruturados para receber denúncias de bullying ou com equipes capacitadas para atuar em situações de conflito digital, o que limitou a implementação plena da legislação.

Além disso, Dos Santos e Taporosky Filho (2024) alertaram que a investigação desses crimes exigia cooperação técnica com as plataformas digitais, o que nem sempre ocorria de forma célere. O sucesso das apurações dependia da preservação imediata de provas digitais e do fornecimento ágil de registros, muitas vezes sediados em servidores estrangeiros. Essa situação revelou a importância de acordos internacionais e de normas complementares que dessem suporte operacional à nova legislação.

3.4 LIMITES DA ATUAÇÃO ESTATAL MESMO COM NOVA TIPIFICAÇÃO PENAL

Apesar dos avanços trazidos pela Lei nº 14.811/2024, a atuação estatal no combate aos crimes virtuais ainda se mostrou limitada diante da complexidade tecnológica envolvida. A criminalização do bullying e do cyberbullying não resolveu, por si só, a dificuldade em identificar autores anônimos nem garantiu a rápida responsabilização penal (Imprensa Nacional, 2024).

Conforme expuseram Dos Santos e Taporosky Filho (2024), a principal limitação residiu na dependência do aparato técnico e jurídico já existente. A lei ampliou o rol de condutas puníveis, mas não criou mecanismos específicos para agilizar a cooperação com plataformas ou para dotar as polícias civis de ferramentas forenses adequadas. Assim, persistiu a necessidade de investimentos públicos em infraestrutura e capacitação de agentes.

Cristiny, Correia e Queiroz (2025) destacaram que, sem estrutura investigativa eficaz, a nova tipificação penal poderia correr o risco de se tornar letra morta. A responsabilização dos agressores virtuais ainda dependia de elementos probatórios sólidos, cuja obtenção exigia rapidez e domínio técnico por parte das autoridades.

Outro ponto de atenção foi o uso indevido da nova tipificação penal em casos de menor gravidade, o que poderia resultar em criminalização excessiva de condutas escolares que deveriam, em primeiro momento, ser resolvidas no âmbito pedagógico. Junior e Taporosky Filho (2024) alertaram para a necessidade de um uso proporcional e criterioso da lei, com ênfase na mediação e na educação digital, antes da judicialização do conflito.

Em síntese, a Lei nº 14.811/2024 significou um avanço ao reconhecer a gravidade dos crimes praticados no ambiente virtual, sobretudo contra crianças e adolescentes. No entanto, sua efetividade plena dependia de ações complementares, como investimentos em tecnologia, capacitação de agentes públicos, parcerias com plataformas digitais e desenvolvimento de políticas públicas integradas.

4. OS LIMITES DA LEGISLAÇÃO BRASILEIRA NA INVESTIGAÇÃO DIGITAL: MARCO CIVIL, LGPD E CONSTITUIÇÃO

4.1 PROTEÇÃO DA PRIVACIDADE E DOS DADOS PESSOAIS NA INTERNET

A proteção da privacidade na internet representou um dos pilares da regulação brasileira do ambiente digital. Essa proteção foi consagrada pela Constituição Federal de 1988, que assegurou, em seu artigo 5º, inciso X, o direito à intimidade, à vida privada e à inviolabilidade das comunicações. Com a expansão das tecnologias digitais e o aumento da exposição de dados pessoais em redes sociais, plataformas e aplicativos, tornou-se urgente o desenvolvimento de uma legislação específica para disciplinar o tratamento dessas informações no meio virtual.

O Marco Civil da Internet (Lei nº 12.965/2014) foi o primeiro instrumento jurídico a regulamentar de forma ampla os direitos e deveres dos usuários, dos provedores de serviços e do Estado na esfera digital. Essa norma estabeleceu princípios como a neutralidade da rede, a inviolabilidade das comunicações e a proteção de dados pessoais como fundamentos essenciais do uso da internet no Brasil (Brasil, 2014). Segundo Cristiny, Correia e Queiroz (2025), o Marco Civil trouxe importantes garantias aos cidadãos, ao limitar o acesso estatal aos dados pessoais e exigir ordem judicial para sua obtenção, salvo nas hipóteses legalmente previstas.

Complementando esse marco normativo, foi promulgada a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), com o objetivo de regulamentar o uso, o armazenamento e o compartilhamento de dados pessoais no Brasil. A LGPD estabeleceu bases legais para o tratamento dessas informações, inclusive por parte do poder público, e impôs o princípio da minimização dos dados, exigindo que somente fossem coletados os estritamente necessários para a finalidade específica (Brasil, 2018). Assim, criou-se uma rede protetiva robusta, mas que também impôs limites consideráveis às investigações criminais.

4.2 IMPLICAÇÕES DO MARCO CIVIL DA INTERNET NAS INVESTIGAÇÕES CRIMINAIS

Embora o Marco Civil da Internet tenha representado um avanço na proteção dos usuários, ele também estabeleceu barreiras importantes para a atuação das autoridades no rastreamento de crimes digitais. De acordo com o artigo 10 da referida lei, qualquer acesso a registros de conexão ou de acesso a aplicações de internet depende de autorização judicial, o que tornou o processo investigativo mais burocrático e moroso (Brasil, 2014).

Araújo (2024) observou que, na prática, muitos inquéritos foram prejudicados pela dificuldade em obter dados cadastrais ou registros de IP a tempo de realizar diligências eficazes. A exigência de ordem judicial prévia, embora fundamental para resguardar os direitos dos usuários, tornou-se um desafio em investigações que exigiam agilidade, como nos casos de ameaças, incitação à violência ou exposição de imagens íntimas.

Outro entrave identificado foi a responsabilidade limitada dos provedores de aplicações. Conforme o artigo 19 do Marco Civil, os provedores somente poderiam ser responsabilizados civilmente se, após ordem judicial específica, não removessem conteúdo considerado ilícito. Essa regra, embora importante para evitar censura prévia, dificultou a responsabilização das plataformas em casos de omissão diante de crimes evidentes, como o cyberbullying contra menores (Cristiny; Correia; Queiroz, 2025).

Apesar disso, o Marco Civil manteve-se como uma das legislações mais equilibradas no cenário internacional, ao buscar harmonizar os interesses de liberdade de expressão e de proteção da privacidade com a necessidade de repressão aos delitos digitais. Todavia, sua aplicação revelou a necessidade de adaptações e interpretações que levassem em conta a celeridade e a gravidade de certos crimes cometidos sob anonimato.

4.3 BARREIRAS IMPOSTAS PELA LGPD E PELOS DIREITOS CONSTITUCIONAIS

A Lei Geral de Proteção de Dados Pessoais aprofundou as restrições ao uso de dados pessoais nas investigações, ao estabelecer, em seu artigo 7º, que o tratamento de dados só pode ocorrer nas hipóteses legais expressamente previstas. Entre elas, está o consentimento do titular, o cumprimento de obrigação legal, ou o exercício regular de direitos em processos judiciais, administrativos ou arbitrais (Brasil, 2018). Para Araújo (2024), essas condições legais, embora justificadas pela necessidade de proteção dos direitos fundamentais, tornaram ainda mais difícil o acesso das autoridades a informações sensíveis, mesmo em contextos de flagrante delito digital.

Outro fator complicador foi a ausência de regulamentação clara sobre como os dados devem ser compartilhados entre empresas e o Estado em investigações penais. Em muitos casos, provedores se recusaram a fornecer informações alegando falta de respaldo legal, mesmo quando solicitadas por autoridades públicas em caráter de urgência. Segundo Cristiny, Correia e Queiroz (2025), essa insegurança jurídica gerou impasses e atrasos em processos investigativos, resultando na perda de provas e na frustração de medidas cautelares.

A Constituição Federal também estabeleceu limites expressivos à atuação do Estado, ao garantir, no artigo 5º, inciso XII, o sigilo das comunicações telefônicas e de dados, salvo por ordem judicial. Assim, qualquer atuação investigativa que envolvesse interceptação de dados ou violação de sigilo exigia autorização do Judiciário, o que, embora garantisse o devido processo legal, nem sempre se mostrou compatível com a urgência de certas investigações, especialmente em crimes cometidos por meio de perfis anônimos (Brasil, 1988).

Essa tensão entre a efetividade das investigações e a proteção da privacidade foi um dos principais pontos de discussão na doutrina contemporânea, que buscou propor modelos de equilíbrio jurídico. Como destacou Araújo (2024), não se tratava de relativizar direitos, mas de buscar meios normativos e operacionais que permitissem a responsabilização penal, sem comprometer os pilares do Estado Democrático de Direito.

4.4 O DILEMA ENTRE SEGURANÇA PÚBLICA E LIBERDADES FUNDAMENTAIS

A partir da promulgação do Marco Civil da Internet e da LGPD, consolidou-se um dilema jurídico-constitucional no Brasil: como garantir a segurança pública e a efetividade da persecução penal sem violar as liberdades civis e os direitos fundamentais dos usuários da internet? Essa tensão foi amplamente discutida na literatura especializada e nos tribunais superiores, refletindo um desafio comum a diversas democracias contemporâneas.

Cristiny, Correia e Queiroz (2025) defenderam que o Estado brasileiro precisava encontrar soluções legislativas e operacionais que compatibilizassem os dois polos desse dilema. Isso incluía, por exemplo, a criação de protocolos técnicos padronizados para coleta e preservação de dados, bem como a ampliação das parcerias internacionais para obtenção de provas armazenadas no exterior.

Outro ponto essencial foi o fortalecimento institucional das autoridades encarregadas da investigação criminal, como as polícias civis e o Ministério Público, que demandavam capacitação técnica constante para lidar com crimes cibernéticos complexos. Araújo (2024)

ressaltou que a formação de núcleos especializados em crimes digitais representava um passo importante para mitigar os efeitos das limitações legais, sem violar garantias constitucionais.

Por fim, o reconhecimento da necessidade de educação digital e cidadania online foi destacado como medida preventiva complementar. Ao promover o uso consciente das tecnologias e o respeito aos direitos dos outros no ambiente virtual, seria possível reduzir a incidência de condutas delituosas e, consequentemente, a dependência de intervenções penais, muitas vezes ineficazes diante do anonimato (Cristiny; Correia; Queiroz, 2025).

5. PROVAS DIGITAIS E BARREIRAS TÉCNICAS: O PAPEL DAS AUTORIDADES E DAS PLATAFORMAS

5.1 PRODUÇÃO E VALIDAÇÃO DE PROVAS DIGITAIS: REQUISITOS LEGAIS

A produção e a validação de provas digitais tornaram-se elementos centrais para a responsabilização penal no ambiente virtual. A jurisprudência brasileira, especialmente a partir de decisões do Superior Tribunal de Justiça, passou a exigir rigor na obtenção e preservação desses elementos probatórios. Conforme Soares (2023), a prova digital precisa atender aos mesmos critérios de qualquer outra prova penal: legalidade, autenticidade, cadeia de custódia e pertinência com o fato investigado.

No entanto, diferentemente das provas físicas, as digitais são voláteis, de fácil modificação ou exclusão, o que torna a atuação imediata das autoridades essencial. Santos e Braz (2024) apontaram que, em casos de incitação à violência em escolas, a demora na extração de dados em redes sociais resultou na perda de informações cruciais, prejudicando a persecução penal. A integridade dos dados, portanto, depende de procedimentos técnicos específicos, como a realização de cópias forenses e a certificação digital das capturas de tela ou registros.

Além disso, os requisitos legais para a utilização das provas digitais em juízo impuseram desafios adicionais. Como destacou Araújo (2024), a obtenção de dados sem autorização judicial prévia ou sem observância da cadeia de custódia pode levar à invalidação da prova. Esse entendimento foi reiterado pela doutrina e pelos tribunais, especialmente no que diz respeito à privacidade e ao sigilo das comunicações, previstos no artigo 5º, inciso XII, da Constituição Federal.

5.2 CADEIA DE CUSTÓDIA E AUTENTICIDADE DAS EVIDÊNCIAS VIRTUAIS

A cadeia de custódia é um dos elementos mais relevantes na produção de provas digitais, pois garante a origem, integridade e confiabilidade das evidências coletadas. De acordo com Soares (2023), a ausência de documentação adequada sobre as etapas da coleta e armazenamento dos dados digitais pode invalidar a prova e comprometer o processo judicial. Por isso, a atuação pericial tornou-se indispensável, especialmente quando envolvia elementos como logs de acesso, e-mails, conversas de aplicativos e arquivos armazenados em nuvem.

No âmbito da responsabilização de agressores virtuais, a manutenção da cadeia de custódia é ainda mais sensível. Conforme observaram Fernandez e Corrêa (2024), em casos de ataques virtuais a crianças e adolescentes, a preservação imediata das mensagens e dos conteúdos ofensivos foi fundamental para a identificação dos responsáveis e para a prevenção de novas violências. A autenticidade das provas era frequentemente questionada quando obtidas de forma informal por vítimas ou familiares, sem a devida perícia técnica.

Cristiny, Correia e Queiroz (2025) ressaltaram que a cadeia de custódia, além de ser uma exigência legal, é uma ferramenta de proteção tanto da vítima quanto do acusado. Garante que a prova apresentada ao juiz seja exatamente aquela capturada no momento do fato, sem alterações, cortes ou edições. Essa preocupação é central para o equilíbrio do processo penal e evita a instrumentalização de conteúdos digitais manipulados.

Em termos normativos, o Código de Processo Penal passou a exigir a documentação minuciosa da cadeia de custódia desde a edição da Lei nº 13.964/2019. Embora essa norma não tenha sido criada especificamente para o contexto digital, sua aplicação tornou-se essencial diante da fragilidade e da natureza efêmera das provas obtidas em ambiente virtual (Soares, 2023).

5.3 COLABORAÇÃO DAS PLATAFORMAS DIGITAIS NAS INVESTIGAÇÕES

A colaboração das plataformas digitais com as autoridades públicas é indispensável para o sucesso das investigações criminais no meio digital. A atuação dessas empresas, no entanto, tem variado bastante, dependendo de fatores como sede jurídica, políticas internas de privacidade e capacidade técnica. Segundo Santos e Braz (2024), em casos de ataques virtuais com ameaças a instituições escolares, a obtenção de informações por parte das plataformas foi determinante para evitar tragédias, embora nem sempre ocorresse de forma célere.

Fernandez e Corrêa (2024) apontaram que muitas plataformas estrangeiras apresentaram resistência ao fornecimento de dados cadastrais ou registros de IP, mesmo diante de ordens judiciais brasileiras. Tal resistência era justificada pela ausência de acordos de cooperação internacional e pelas diferenças entre as legislações de proteção de dados. Essa lacuna normativa dificultou o trabalho da polícia judiciária e do Ministério Público, que dependiam de tais informações para prosseguir com as investigações.

Araújo (2024) enfatizou que a responsabilização das plataformas também é objeto de debates no âmbito civil, especialmente nos casos em que há omissão reiterada diante de condutas ilegais. A responsabilização por danos decorrentes de cyberbullying, por exemplo, pode atingir as empresas quando elas deixam de agir mesmo após serem notificadas formalmente sobre conteúdos ofensivos.

Cristiny, Correia e Queiroz (2025) defenderam a necessidade de protocolos institucionais padronizados de cooperação entre plataformas e autoridades. Tais mecanismos poderiam garantir prazos de resposta mais rápidos, critérios técnicos uniformes e meios seguros para a transmissão de dados, respeitando ao mesmo tempo os direitos fundamentais dos usuários.

5.4 OBSTÁCULOS TÉCNICOS E INSTITUCIONAIS ENFRENTADOS PELAS AUTORIDADES

As autoridades brasileiras enfrentaram diversos obstáculos técnicos e institucionais na investigação de crimes virtuais, especialmente no que tange à coleta e análise de provas digitais. Soares (2023) destacou que, em muitas unidades policiais, a ausência de profissionais especializados em tecnologia da informação comprometeu a efetividade da atuação estatal. Esse déficit estrutural dificultou a condução de perícias forenses, a preservação da cadeia de custódia e a decodificação de dados criptografados.

Santos e Braz (2024) observaram que, além da questão técnica, houve entraves burocráticos relevantes, como a necessidade de tramitação judicial para autorização de acesso a dados e a morosidade no cumprimento de decisões por parte de empresas de tecnologia. A lentidão institucional criou lacunas de tempo que favoreciam a exclusão ou modificação de provas essenciais à responsabilização penal.

Segundo Araújo (2024), outro entrave foi o desconhecimento, por parte de muitos operadores do direito, das dinâmicas específicas do ambiente digital. Muitos procedimentos

investigativos e decisões judiciais não estavam adequadamente atualizados para lidar com a volatilidade e complexidade das provas virtuais, o que reduziu a efetividade da persecução penal e aumentou a sensação de impunidade.

Fernandez e Corrêa (2024) ressaltaram ainda que os desafios institucionais estavam relacionados à falta de investimentos em tecnologia e em centros especializados de combate ao crime cibernético, o que contrastava com o crescente volume e sofisticação das ocorrências. A ausência de políticas públicas integradas também dificultou a articulação entre órgãos como a Polícia Federal, as polícias civis, o Ministério Público e o Judiciário.

Frente a esse cenário, Cristiny, Correia e Queiroz (2025) sugeriram a criação de núcleos especializados regionais e a celebração de convênios com universidades e empresas de tecnologia, como forma de superar as lacunas técnicas e aprimorar as respostas do Estado aos crimes digitais. A partir de uma atuação mais articulada, preventiva e qualificada, seria possível garantir maior proteção às vítimas e fortalecer a aplicação do Direito Penal no ciberespaço.

6. CAMINHOS POSSÍVEIS: PROPOSTAS PARA O APRIMORAMENTO DA RESPONSABILIZAÇÃO PENAL EM AMBIENTES VIRTUAIS

6.1 REFORMAS LEGISLATIVAS E PROPOSTAS DE APRIMORAMENTO JURÍDICO

A constante evolução das tecnologias digitais exige uma legislação dinâmica, capaz de acompanhar os novos cenários de criminalidade cibernética. A Lei nº 14.811/2024 representou um avanço importante ao tipificar penalmente o bullying e o cyberbullying, mas, conforme destacaram Dos Santos e Taporosky Filho (2024), ainda há lacunas legais que dificultam a responsabilização efetiva de agentes que atuam sob anonimato. Nesse contexto, reformas legislativas se mostraram necessárias para fortalecer o arcabouço jurídico e garantir maior efetividade nas investigações digitais.

Uma das principais propostas nesse sentido consiste na criação de normativas complementares que definam prazos e protocolos para a cooperação entre plataformas digitais e autoridades. Cristiny, Correia e Queiroz (2025) enfatizaram que a ausência de diretrizes claras prejudica a celeridade das investigações e favorece a impunidade. Além disso, é fundamental que o ordenamento jurídico contemple medidas processuais específicas para provas digitais, como a simplificação dos pedidos de quebra de sigilo de dados em casos de flagrante virtual.

Araújo (2024) acrescentou que o Direito Penal precisa ser constantemente reinterpretado à luz da realidade digital. A tipificação de condutas, como a disseminação em massa de

conteúdos difamatórios por meio de robôs automatizados ou a criação de perfis falsos para o cometimento de crimes, ainda é incipiente. Assim, a atualização das categorias penais tradicionais é uma medida urgente para adaptar a legislação aos novos instrumentos de violação de direitos.

6.2 INVESTIMENTOS EM TECNOLOGIA FORENSE E COOPERAÇÃO INTERNACIONAL

Além das reformas legais, o aprimoramento da responsabilização penal em ambientes digitais depende de investimentos robustos em tecnologia forense e da ampliação da cooperação internacional. Dos Santos e Taporosky Filho (2024) destacaram que grande parte das provas digitais reside em servidores localizados no exterior, o que torna indispensável a existência de acordos bilaterais e multilaterais para compartilhamento de dados. Sem essa articulação, muitas investigações se tornam inviáveis, principalmente quando envolvem crimes transnacionais.

No Brasil, a escassez de ferramentas tecnológicas nas polícias civis e no Ministério Público comprometeu a análise pericial dos elementos digitais coletados. Conforme relatado por Fernandez e Corrêa (2024), muitos agentes públicos não dispõem de formação adequada para lidar com provas criptografadas, manipulação de metadados e rastreamento de conexões anônimas. Isso reforça a urgência de políticas públicas voltadas à capacitação de profissionais e à criação de laboratórios forenses especializados em crimes cibernéticos.

A cooperação internacional, por sua vez, deve ser fortalecida por meio da adesão do Brasil a tratados de auxílio mútuo jurídico e à atualização dos mecanismos de cooperação direta com empresas de tecnologia. Araújo (2024) apontou que, embora existam tratados multilaterais sobre crimes cibernéticos, como a Convenção de Budapeste, sua internalização e aplicação prática ainda enfrentam obstáculos, sobretudo no que tange ao compartilhamento ágil de dados em investigações de cyberbullying contra menores.

6.3 RESPONSABILIZAÇÃO DAS PLATAFORMAS E MEDIDAS PREVENTIVAS

A responsabilização das plataformas digitais, embora ainda envolta em debates jurídicos, tem se mostrado fundamental para o enfrentamento da criminalidade no ciberespaço. Cristiny, Correia e Queiroz (2025) argumentaram que as empresas que administram redes sociais, aplicativos de mensagens e fóruns online possuem papel ativo na prevenção e repressão de

delitos virtuais, especialmente quando têm conhecimento prévio sobre o uso indevido de seus serviços.

Nesse sentido, é imprescindível que as plataformas mantenham mecanismos de denúncia acessíveis, sistemas de moderação de conteúdo eficazes e políticas claras de cooperação com as autoridades públicas. Dos Santos e Taporosky Filho (2024) sugeriram que a legislação avance no sentido de estabelecer obrigações específicas às plataformas em casos de reincidência, omissão ou resistência injustificada ao fornecimento de dados essenciais à investigação criminal.

Além da responsabilização jurídica, as plataformas devem ser incentivadas a adotar medidas preventivas, como o uso de inteligência artificial para detectar automaticamente conteúdos violentos, ameaças e discursos de ódio. Fernandez e Corrêa (2024) relataram que, em casos envolvendo crianças e adolescentes, a atuação preventiva das plataformas foi crucial para evitar danos maiores, especialmente em situações de exposição indevida ou perseguição virtual.

Araújo (2024) também mencionou que o ambiente digital não pode ser concebido como uma zona neutra de responsabilidade. A ausência de ação das plataformas diante de violações evidentes configura, em certos contextos, coautoria omissiva. Por isso, é urgente que o Direito Civil, o Penal e o Administrativo dialoguem na construção de um regime jurídico moderno de responsabilização digital.

6.4 EDUCAÇÃO DIGITAL, CIDADANIA E MEDIAÇÃO DE CONFLITOS ONLINE

Por fim, um dos caminhos mais eficazes para a promoção da responsabilização penal em ambientes virtuais é a educação digital e a promoção da cidadania online. Taborda e Sippert (2024) destacaram que a prevenção ao cyberbullying e a outras formas de violência virtual passa, necessariamente, pela formação ética dos usuários, especialmente das crianças e adolescentes. A escola, nesse cenário, torna-se espaço estratégico para o desenvolvimento de competências digitais e socioemocionais.

A educação digital não deve se limitar ao uso técnico das tecnologias, mas envolver discussões sobre respeito, empatia, privacidade e consequências legais das condutas no ambiente online. Fernandez e Corrêa (2024) ressaltaram que muitos jovens desconhecem os limites legais das interações digitais, o que contribui para a banalização de comportamentos ofensivos. A integração entre família, escola e Estado é essencial para mudar essa realidade.

Além da educação formal, a mediação de conflitos virtuais tem sido apontada como alternativa eficaz para a resolução de situações de cyberbullying sem necessidade de judicialização. Taborda e Sippert (2024) relataram experiências exitosas de mediação em ambiente escolar, nas quais a escuta ativa, o acolhimento e o diálogo restaurativo foram capazes de reverter quadros de agressão e reestabelecer vínculos afetivos.

Dos Santos e Taporosky Filho (2024) reforçaram que o Direito Penal deve ser acionado como última instância, após esgotadas as tentativas de solução extrajudicial. Nesse sentido, é recomendável a criação de programas institucionais de mediação digital, especialmente em instituições de ensino, em parceria com defensores públicos, psicólogos e conselhos tutelares.

Cristiny, Correia e Queiroz (2025) concluíram que, ao aliar medidas repressivas, reformas legislativas, atuação institucional integrada e educação para a cidadania digital, é possível criar um ecossistema jurídico e social mais justo, seguro e eficaz no enfrentamento da violência e da impunidade no ciberespaço.

7. CONSIDERAÇÕES FINAIS

A presente pesquisa teve como objetivo analisar os principais desafios impostos pelo anonimato digital à responsabilização penal dos autores de crimes cibernéticos e avaliar de que forma a Lei nº 14.811/2024 contribuiu para enfrentá-los. A partir da revisão normativa e doutrinária realizada, foi possível constatar que, embora o ordenamento jurídico brasileiro tenha evoluído no combate às práticas ilícitas no ambiente virtual, ainda existem entraves consideráveis que limitam a eficácia das medidas punitivas.

O anonimato digital revelou-se um dos maiores obstáculos à persecução penal contemporânea, especialmente em um contexto marcado pela volatilidade das informações e pela facilidade de ocultação da identidade do agente. As ferramentas tecnológicas disponíveis para a prática de crimes virtuais evoluíram mais rapidamente do que os mecanismos legais e institucionais de combate a essas condutas, o que gerou uma lacuna entre a legislação vigente e as necessidades práticas da investigação criminal.

A Lei nº 14.811/2024 trouxe importantes avanços ao tipificar penalmente o bullying e o cyberbullying, especialmente quando praticados contra crianças e adolescentes. A criação do artigo 146-A do Código Penal representou um esforço legislativo relevante para dar visibilidade jurídica a condutas antes negligenciadas. No entanto, sua efetividade plena depende de fatores

que extrapolam o texto legal, como a estrutura das instituições de segurança pública, a cooperação com plataformas digitais e a capacitação técnica dos profissionais envolvidos.

Os limites impostos pelo Marco Civil da Internet, pela LGPD e pela própria Constituição Federal quanto ao acesso a dados pessoais e à privacidade dos usuários impõem um dilema jurídico entre a proteção de direitos fundamentais e a garantia da segurança pública. Nesse sentido, o equilíbrio entre esses dois polos deve ser constantemente buscado, por meio de interpretações harmônicas e propostas legislativas que compatibilizem os interesses em jogo.

Outro aspecto crítico identificado foi a dificuldade na produção e validação de provas digitais. A ausência de cadeia de custódia adequada, a morosidade nos processos investigativos e a insuficiência de cooperação por parte das plataformas dificultam a responsabilização penal efetiva. Além disso, a atuação do Estado ainda encontra entraves técnicos e operacionais que precisam ser superados com investimentos em tecnologia, infraestrutura e especialização.

Como proposta de aprimoramento, destacaram-se a necessidade de reformas legislativas, o fortalecimento das parcerias internacionais, a responsabilização das plataformas digitais mediante regras mais claras e rigorosas, bem como a adoção de medidas preventivas, com foco na educação digital e na mediação de conflitos. A prevenção deve ser compreendida como eixo fundamental para a construção de uma cultura de respeito, ética e responsabilidade no uso das tecnologias.

Conclui-se, portanto, que o combate à criminalidade digital exige uma atuação articulada, interdisciplinar e adaptativa por parte do Estado, da sociedade e das instituições privadas. A responsabilização penal no ambiente virtual só será efetiva quando acompanhada de políticas públicas amplas, voltadas à proteção da dignidade humana, à preservação de direitos e à promoção de um ciberespaço mais seguro e justo para todos.

REFERÊNCIAS

ARAUJO, J. H. A. **Responsabilidade civil no âmbito do cyberbullying: desafios da era digital.** 2024. Disponível em: https://lume.ufrgs.br/handle/10183/283510. Acesso em: 23 abr. 2025.

ARAÚJO, T. F. M. **Os desafios do direito penal na proteção das crianças e adolescentes na era digital: uma análise da repressão dos crimes cibernéticos à luz da Lei 14.811/24.** 2024. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro. Disponível em: https://pantheon.ufrj.br/handle/11422/25324. Acesso em: 23 abr. 2025.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal.** Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 23 abr. 2025.

BRASIL. Imprensa Nacional. **Lei nº 14.811, de 12 de janeiro de 2024.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/lei/l14811.htm. Acesso em: 23 abr. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 23 abr. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 abr. 2025.

BRASIL. **Lei nº 14.811, de 12 de janeiro de 2024. Presidência da República**, 2024. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/lei/l14811.htm. Acesso em: 23 abr. 2025.

CRISTINY, A.; CORREIA, I.; QUEIROZ, C. Impactos da Lei 14.811/24 (Direito). **Repositório Institucional**, v. 3, n. 2, 2025. Disponível em: https://revistas.icesp.br/index.php/Real/article/view/6145. Acesso em: 23 abr. 2025.

FERNANDEZ, C. B.; CORRÊA, V. L. M. Crianças no ambiente virtual: entre riscos e proteção. **ARACÊ**, v. 6, n. 2, p. 2730-2745, 2024. Disponível em: https://periodicos.newsciencepubl.com/arace/article/view/836. Acesso em: 23 abr. 2025.

JUNIOR, J. Z.; TAPOROSKY FILHO, P. S. Artigo 146-A do Código Penal: uma análise dos novos crimes de bullying e cyberbullying. **Academia de Direito**, v. 6, p. 3835-3858, 2024. Disponível em: http://www.periodicos.unc.br/index.php/acaddir/article/view/5601. Acesso em: 23 abr. 2025.

NUNES, R. P. **Direito penal e crimes cibernéticos: fundamentos e aplicações práticas.** São Paulo: Editora Jurídica, 2022.

SANTOS, G. H. F.; TAPOROSKY FILHO, P. S. Desafios jurídicos e operacionais na implementação da Lei n. 14.811/24: um estudo sobre a proteção contra o cyberbullying no Brasil. **Academia de Direito**, v. 6, p. 3859-3877, 2024. Disponível em: http://www.periodicos.unc.br/index.php/acaddir/article/view/5602. Acesso em: 23 abr. 2025.

SANTOS, L. V. V. A.; BRAZ, L. C. F. S. Incitação on-line a ataques de violência nas escolas do Brasil: uma análise do fenômeno à luz da responsabilidade penal. 2024. Disponível em: https://ri.ucsal.br/items/206fcf59-7656-4cf1-b7fe-fbc537b4817e. Acesso em: 23 abr. 2025.

SOARES, F. **Investigação criminal na era digital: desafios e perspectivas.** Rio de Janeiro: Digital Jurídica, 2023.

TABORDA, A. B.; SIPPERT, E. L. A mediação como prática de valorização da escuta, do exercício de cidadania e da pacificação social nos casos de cyberbullying. **Anais do Seminário Internacional em Direitos Humanos e Sociedade**, v. 6, 2024. Disponível em: https://www.periodicos.unesc.net/ojs/index.php/AnaisDirH/article/view/9359. Acesso em: 23 abr. 2025.