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

doi.org/10.51891/rease.v11i5.19434

AS DIFICULDADES DA PRODUÇÃO DE PROVAS E INVESTIGAÇÃO DOS CRIMES SISTEMÁTICOS VIRTUAIS DO CYBERBULLY

THE DIFFICULTIES OF PRODUCING EVIDENCE AND INVESTIGATING SYSTEMATIC VIRTUAL CRIMES BY CYBERBULLY

Átala de Freitas Braga[1]
Kerolaine Melgueiro da Silva[2]
Thainá Ferreira dos Santos[3]
Marcelo Augusto Rebouças Leite[4]

RESUMO: Este artigo aborda os desafios enfrentados na investigação e produção de provas em crimes de cyberbullying, uma prática crescente no ambiente virtual, que atinge principalmente crianças e adolescentes. Apesar do avanço legislativo com normas como a Lei nº 14.811/2024 e o Marco Civil da Internet, ainda há sérias dificuldades técnicas e jurídicas que comprometem a responsabilização penal dos agressores. O problema central da pesquisa consiste na dificuldade de coleta de provas digitais, agravada pelo uso de tecnologias de anonimização, criptografia, servidores estrangeiros e pelas restrições impostas pela Lei Geral de Proteção de Dados (LGPD). O objetivo geral do estudo foi analisar as limitações jurídicas e técnicas que afetam a efetividade das investigações, com foco nos entraves à produção de provas. Como objetivos específicos, destacam-se: compreender o impacto da LGPD, investigar os efeitos das tecnologias na coleta de dados e exemplificar essas dificuldades por meio do caso do King Discord. A metodologia adotada foi qualitativa, com base em revisão bibliográfica, análise documental e estudo de caso. Os resultados evidenciam que a legislação brasileira, embora tenha evoluído, ainda carece deinstrumentos adequados à realidade tecnológica. A investigação digital requer rapidez, conhecimento técnico especializado e maior cooperação entre Estado, plataformas digitais e comunidade internacional. O estudo demonstrou que a carência de capacitação, a morosidade judicial e a proteção de dados, embora fundamentais, acabam dificultando o acesso a informações cruciais. Por fim, a conclusão aponta para a necessidade de atualização normativa, investimentos em perícia digital e ações preventivas, buscando o equilíbrio entre privacidade e segurança pública no enfrentamento ao cyberbullying.

Palavras-chave: Cyberbullying. Provas digitais. LGPD. Investigação criminal. Anonimato virtual.

[1]Discente do Curso de Direito do Centro Universitário do Norte – UNINORTE.
[2]Discente do Curso de Direito do Centro Universitário do Norte – UNINORTE.
[3]Discente do Curso de Direito do Centro Universitário do Norte – UNINORTE.
[4]Professor Orientador, Marcelo Augusto Rebouças Leite, advogado, especialista em docência do ensino superior e professor do curso de direito do Centro Universitário do Norte – UNINORTE.

ABSTRACT: This article addresses the challenges faced in the investigation and production of evidence in cyberbullying crimes, a growing practice in the virtual environment, which mainly affects children and adolescents. Despite legislative advances with standards such as Law No. 14,811/2024 and the Internet Civil Rights Framework, there are still serious technical and legal difficulties that compromise the criminal liability of aggressors. The central problem of the research is the difficulty in collecting digital evidence, aggravated by the use of anonymization technologies, encryption, foreign servers and restrictions imposed by the General Data Protection Law (LGPD). The general objective of the study was to analyze the legal and technical limitations that affect the effectiveness of investigations, focusing on obstacles to the production of evidence. The specific objectives include: understanding the impact of the LGPD, investigating the effects of technologies on data collection and exemplifying these difficulties through the case of King Discord. The methodology adopted was qualitative, based on a bibliographic review, document analysis and case study. The results show that Brazilian legislation, although it has evolved, still lacks instruments that are appropriate to the technological reality. Digital investigation requires speed, specialized technical knowledge and greater cooperation between the State, digital platforms and the international community. The study demonstrated that the lack of training, judicial delays and data protection, although fundamental, end up hindering access to crucial information. Finally, the conclusion points to the need for regulatory updates, investments in digital expertise and preventive actions, seeking a balance between privacy and public safety in combating cyberbullying.

Keywords: Cyberbullying. Digital evidence. LGPD. Criminal investigation. Virtual anonymity.

INTRODUÇÃO

Com o crescimento exponencial da internet e das redes sociais, o fenômeno do cyberbullying tornou-se uma das principais formas de violência no ambiente virtual, afetando principalmente crianças e adolescentes. Segundo Brito (2021), o Brasil é o segundo país no ranking mundial em tempo de permanência nas redes sociais, o que potencializa a exposição dos usuários a riscos como ofensas, humilhações e ataques sistemáticos.

Apesar dos avanços legislativos, como a promulgação da Lei nº 14.811/2024 — que incluiu o crime de cyberbullying no Código Penal por meio do artigo 146-A — e a instituição do Marco Civil da Internet (Lei nº 12.965/2014), a apuração dessas infrações ainda enfrenta significativos entraves técnicos e jurídicos, especialmente no que se refere à produção de provas. Como observa Lima (2024), a investigação criminal no ciberespaço é marcada por uma complexidade crescente, agravada pelo uso de tecnologias de anonimização, criptografia e pela descentralização dos dados, muitas vezes armazenados em servidores localizados fora do país. Além disso, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) impõe restrições

importantes ao acesso a informações que seriam cruciais para a identificação dos responsáveis por crimes virtuais.

A partir disso, o problema da pesquisa concentra-se nas dificuldades de coleta e produção de provas nos crimes de cyberbullying, considerando o avanço tecnológico e os desafios jurídicos que comprometem a efetividade das investigações. Esta lacuna tem como consequência o aumento da sensação de impunidade e a perpetuação das agressões, com sérios impactos psicológicos sobre as vítimas, como depressão, ansiedade e ideação suicida, conforme exemplificado por Santos et al. (2024).

Logo, a relevância da pesquisa está em contribuir para o debate jurídico sobre a necessidade de aprimorar os mecanismos legais e investigativos frente ao aumento dos crimes sistemáticos virtuais. Dados do estudo de Muzakir et al. (2022) revelam que a Indonésia ocupa a terceira posição global em casos de cyberbullying, logo após o Japão e a Coreia do Sul, com o Brasil se aproximando desse cenário alarmante.

Desta maneira, duas hipóteses norteiam a pesquisa: a primeira, de que a legislação brasileira, embora avance na criminalização do cyberbullying, ainda é insuficiente para enfrentar os desafios da produção de provas digitais; a segunda, de que a LGPD, ao garantir a proteção dos dados pessoais, acaba por dificultar o acesso a informações essenciais para a investigação criminal, criando um conflito entre privacidade e segurança pública.

Para isso, o objetivo geral consiste em analisar as principais dificuldades enfrentadas pelos operadores do direito na produção de provas e investigação dos crimes de cyberbullying. Como objetivos específicos: 1) Explicar o impacto da LGPD e do Marco Civil da Internet na persecução penal dos crimes virtuais; 2) Demonstrar como a tecnologia, como a criptografia e o uso de servidores internacionais, interfere na coleta de provas; 3) Compreender casos emblemáticos, como o caso do King do Discord, para exemplificar os obstáculos e as possíveis soluções jurídicas.

A metodologia adotada é qualitativa, com base em revisão bibliográfica e análise documental de leis, artigos acadêmicos e estudos de caso, como o apresentado por Santos et al. (2024) e Severo Queiroz (2024). Além disso, serão analisadas experiências internacionais como a Convenção de Budapeste e as práticas investigativas relacionadas à infiltração virtual de agentes, descritas por Santos (2021), para subsidiar a pesquisa.

Por último, o artigo será dividido nas seguintes seções: a primeira apresentará o conceito de cyberbullying e os impactos jurídicos e sociais desta prática; a segunda abordará o papel da

legislação, especialmente o Marco Civil da Internet e a LGPD, na limitação ou facilitação das investigações; a terceira seção analisa os desafios técnicos na produção de provas, incluindo o uso de criptografia e anonimato; a quarta trará o estudo de caso do King do Discord, evidenciando as dificuldades enfrentadas pelas autoridades; e, por fim, a conclusão proporá alternativas legislativas e investigativas para aprimorar a responsabilização penal.

2 Cyberbullying: Definição e Impacto no Mundo Jurídico

O avanço das tecnologias digitais, aliado à crescente inserção de crianças e adolescentes no ciberespaço, ampliou a complexidade das relações sociais e, consequentemente, dos conflitos, entre eles o cyberbullying. Esta prática consiste na utilização de meios virtuais para humilhar, difamar, perseguir ou expor alguém de forma sistemática e repetitiva, causando danos às vítimas (Santos et al., 2024).

De acordo com Leal (2024), o Brasil tem evoluído legislativamente para combater esse crime, especialmente com a promulgação da Lei nº 14.811/2024, que incluiu a intimidação sistemática no Código Penal, prevista no artigo 146-A da referida lei:

> **Art. 146-A.** Intimidar sistematicamente, individualmente ou em grupo, mediante violência física ou psicológica, uma ou mais pessoas, de modo intencional e repetitivo, sem motivação evidente, por meio de atos de intimidação, de humilhação ou de discriminação ou de ações verbais, morais, sexuais, sociais, psicológicas, físicas, materiais ou virtuais:
> Pena - multa, se a conduta não constituir crime mais grave.
> **Parágrafo único.** Se a conduta é realizada por meio da rede de computadores, de rede social, de aplicativos, de jogos on-line ou por qualquer outro meio ou ambiente digital, ou transmitida em tempo real:
> Pena - reclusão, de 2 (dois) anos a 4 (quatro) anos, e multa, se a conduta não constituir crime mais grave.

Entretanto, segundo Leal (2024), o desafio maior está na efetividade da aplicação dessa lei, considerando o princípio da ultima ratio do direito penal. Visto que a legislação, embora necessária, encontra dificuldades na delimitação de condutas, já que o ambiente digital, dinâmico e em constante mutação, favorece o anonimato e a impunidade.

Por outro lado, as consequências para as vítimas são devastadoras e vão além do mero constrangimento virtual. Conforme apontam Santos et al. (2024), o cyberbullying provoca transtornos psicológicos graves como depressão, ansiedade e, em casos extremos, pensamentos suicidas, especialmente entre adolescentes. Exemplo emblemático disso foi o caso de Lucas

Santos[5], que cometeu suicídio após sofrer ataques homofóbicos nas redes sociais, fato que escancarou a letalidade dessa forma de violência (Santos et al., 2024).

2.1 Atuação jurídica no enfrentamento ao Cyberbullying

Conforme Severo Queiroz (2024), a volatilidade da prova digital e o uso de tecnologias de anonimização dificultam a responsabilização penal dos agressores. A Convenção de Budapeste, incorporada recentemente ao ordenamento brasileiro, reforça a necessidade de preservação imediata de dados digitais para garantir a efetividade da investigação.

No campo jurídico, a responsabilidade das plataformas digitais também se impõe como desafio moderno. Tanes (2023) salienta que a responsabilização civil e penal das empresas por omissão ou facilitação da prática de cyberbullying precisa ser aprimorada no Brasil, principalmente no cenário dos e-sports, onde o fenômeno tem crescido de forma alarmante. Visto que, nesse sentido, o Marco Civil da Internet (Lei nº 12.965/2014), art. 18, dispõe: "O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros" (Brasil, 2014), o que impõe desafios à responsabilização direta das plataformas.

Portanto, é inegável que o combate ao cyberbullying exige um sistema jurídico penal robusto, mas também flexível e atualizado, capaz de responder à complexidade das relações no ciberespaço. No entanto, conforme Leal (2024), a mera criminalização não é suficiente, sendo necessário o fortalecimento das políticas públicas de prevenção e educação digital para mitigar o problema na raiz.

3 A Lei Geral de Proteção de Dados (LGPD) e Seus Efeitos na Investigação Criminal

O artigo 7º da LGPD, por exemplo, exige o consentimento do titular para o tratamento de dados, salvo exceções legais. No entanto, o §3º do mesmo artigo prevê que o tratamento poderá ocorrer sem consentimento quando necessário para atender aos interesses legítimos do controlador ou de terceiros, desde que não prevaleçam direitos e liberdades fundamentais do

[5]A Lei nº 14.811/2024, popularmente conhecida como Lei Lucas Santos, foi criada em homenagem ao adolescente Lucas Santos, que tirou a própria vida após sofrer ataques de cyberbullying nas redes sociais. A norma alterou o Código Penal brasileiro ao tipificar a prática de bullying e cyberbullying como crimes, inserindo o artigo 146-A. A lei também prevê agravantes quando a violência for praticada contra crianças e adolescentes, além de incluir novas condutas no rol dos crimes hediondos, reforçando a proteção legal à infância e juventude no ambiente físico e virtual.

titular. Já o artigo 11 da mesma lei, ao tratar dos dados sensíveis, impõe restrições ainda mais rigorosas. Tais exigências impactam diretamente as investigações, dificultando o acesso célere e eficaz a informações essenciais.

Conforme destaca Freitas et al. (2023), a volatilidade das evidências digitais, a criptografia e o uso de redes anônimas tornam urgente o acesso a dados, o que colide com a morosidade imposta pela necessidade de autorização judicial e pela proteção de dados prevista na LGPD. Essa tensão entre o direito à privacidade e a segurança pública é latente quando se trata de crimes como o cyberbullying, onde a identificação do autor depende frequentemente da obtenção de dados de conexão, como o endereço IP.

Para mitigar essas barreiras, instrumentos legais como o artigo 10 da Lei nº 12.850/2013, que trata da infiltração de agentes em organizações criminosas, e o artigo 190-A do Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) autorizam, mediante autorização judicial, a atuação de agentes policiais infiltrados em ambiente virtual, principalmente para investigar crimes contra a dignidade sexual de crianças e adolescentes.

Santos (2021) observa que a infiltração virtual tem se mostrado um método eficaz para combater crimes digitais, mas destaca que, para sua validade, é imprescindível o cumprimento dos requisitos legais, como o fumus comissi delicti e o periculum in mora, além da autorização judicial. Ademais, o artigo 5º, inciso XII, da Constituição Federal garante o sigilo das comunicações, exceto por ordem judicial, o que reforça a necessidade de cautela nas investigações digitais.

Ainda, a complexidade se acentua em crimes como o cyberbullying, prática caracterizada pela violência sistemática no ambiente digital. A Lei nº 13.185/2015 define o bullying como "intimidação sistemática" e prevê a implementação de políticas públicas de prevenção no âmbito educacional. Já a recente Lei nº 14.811/2024 altera o Código Penal e acrescenta o artigo 146-A, tipificando o bullying e, em seu parágrafo único, o cyberbullying, com penas de até quatro anos de reclusão, além de multa, quando praticado por meio eletrônico.

Gonçalves e Oliveira (2020) apontam que a punição dos agressores de cyberbullying é muitas vezes inviabilizada pela dificuldade de identificação, causada tanto pela anonimização dos meios digitais quanto pelas restrições da LGPD. Essa situação exige um diálogo entre a proteção de dados e o interesse público na persecução penal.

No ambiente escolar, a responsabilidade se estende às instituições de ensino, conforme previsto no artigo 70 do Estatuto da Criança e do Adolescente, que estabelece o dever do Estado,

da família e da sociedade de proteger a criança de toda forma de violência (Brasil, 1990). Assim, omissões na prevenção e combate ao cyberbullying podem gerar responsabilização civil da escola e dos pais dos agressores, nos termos do artigo 932, I, do Código Civil.

Nesse cenário, é essencial a capacitação de agentes públicos para lidar com as novas ferramentas digitais e jurídicas. Além disso, é urgente que o Judiciário atue com maior celeridade na concessão de autorizações legais para medidas invasivas, como a quebra de sigilo telemático, prevista no artigo 1º da Lei nº 9.296/1996, a fim de viabilizar investigações eficazes.

4 Tecnologias de Comunicação e Desafios na Coleta de Provas

Segundo Severo Queiroz (2024), o avanço das Tecnologias da Informação e Comunicação (TICs) tem transformado profundamente a maneira como a sociedade interage e se comunica, ao mesmo tempo em que impõe novos desafios ao sistema jurídico, especialmente na coleta de provas digitais. A criptografia ponta a ponta e o uso de navegadores como o Tor Project representam ferramentas eficazes na proteção da privacidade dos usuários, mas também dificultam investigações criminais em ambientes virtuais. O crescimento de crimes cibernéticos, que utilizam essas tecnologias para camuflar práticas ilícitas, demanda um novo olhar jurídico sobre a admissibilidade e obtenção de provas.

A criptografia ponta a ponta tornou-se amplamente utilizada em aplicativos de mensagens como forma de garantir confidencialidade na comunicação entre usuários. Este modelo impede que terceiros – inclusive os próprios provedores de serviços – tenham acesso ao conteúdo transmitido. Esta característica, embora salutar do ponto de vista da proteção de dados e liberdades civis, representa um enorme obstáculo para as autoridades quando se trata da interceptação de comunicações suspeitas de envolvimento com atividades criminosas (Lima, 2024).

O Tor Project, por sua vez, é uma tecnologia de anonimização baseada em redes de sobreposição que permite aos usuários ocultarem seu endereço IP real, navegando de forma anônima pela internet, inclusive pela chamada Dark Web. Embora o anonimato digital esteja garantido como direito em sociedades democráticas, sua utilização como ferramenta de proteção para condutas ilícitas, como pedofilia, tráfico de drogas e crimes contra a honra, gera complexidade probatória para o sistema penal (Severo Queiroz, 2024).

A volatilidade das provas digitais – que podem ser rapidamente apagadas, alteradas ou criptografadas – exige atuação célere e tecnicamente especializada das autoridades, como

destacou Severo Queiroz (2024), ressaltando a necessidade de pedidos imediatos de preservação de dados aos provedores. Todavia, nem sempre a legislação vigente acompanha essa velocidade, e lacunas processuais impedem que provas obtidas em tempo sejam aceitas judicialmente, especialmente quando não respeitada a cadeia de custódia.

Ainda que a Lei nº 12.737/2012 (Lei Carolina Dieckmann) e o Marco Civil da Internet (Lei nº 12.965/2014) tenham representado avanços ao tratar de delitos cibernéticos e regras de fornecimento de dados por provedores, ambas carecem de especificidade para lidar com o uso de tecnologias como o Tor e a criptografia avançada (Mendonça, 2023). Em muitos casos, a ausência de provas robustas leva à impunidade, fortalecendo a percepção de que o ambiente virtual é “terra sem lei”.

Por outro lado, a criminalização e o controle excessivo dessas ferramentas tecnológicas podem colidir com princípios constitucionais como a liberdade de expressão, o direito à privacidade e o devido processo legal (Leonardi, 2012). Dessa forma, o desafio não reside apenas na criação de leis mais duras, mas no equilíbrio entre segurança e liberdade, como destaca, ao defender que o sistema jurídico precisa ser eficaz sem perder sua essência democrática.

A atuação das autoridades investigativas, portanto, deve estar baseada em conhecimento técnico, capacitação constante e uso de ferramentas forenses compatíveis com a complexidade dos crimes digitais (Severo Queiroz, 2024). Isso inclui, por exemplo, a adoção de estratégias de engenharia reversa, análise de metadados, cooperação internacional e práticas investigativas compatíveis com a Convenção de Budapeste, da qual o Brasil é signatário (Lima, 2024).

Em paralelo, a educação digital da população e a criação de políticas públicas preventivas devem caminhar lado a lado com a repressão penal. A responsabilização das plataformas, como previsto na LGPD (Lei nº 13.709/2018), deve ser fortalecida, especialmente no que se refere ao dever de colaborar com as investigações, sem violar garantias fundamentais (Mendonça, 2023).

A construção de um ambiente digital seguro, ético e juridicamente eficaz depende de ações multidisciplinares e de um sistema legal adaptado aos novos paradigmas tecnológicos. O aprimoramento das leis, a especialização das polícias, o investimento em perícia forense e a cooperação internacional são caminhos imprescindíveis para enfrentar o cenário atual. Como bem enfatiza Severo Queiroz (2024), "a investigação criminal do futuro já é realidade, e exige respostas urgentes".’

5 King do Discord e a Produção de Provas

No contexto brasileiro, a investigação dessas infrações enfrenta desafios significativos, sobretudo quando a coleta de provas digitais se depara com barreiras legais e técnicas. O chamado Caso do King do Discord foi um episódio no qual um usuário identificado como King do Discord se envolveu em práticas ilícitas em plataformas digitais, escancarou as limitações enfrentadas pelas autoridades diante do anonimato digital e da aplicação da Lei Geral de Proteção de Dados (LGPD), dificultando a persecução penal.

O caso ganhou notoriedade após a descoberta de que o King do Discord liderava servidores fechados na plataforma Discord, nos quais eram compartilhados conteúdos criminosos, especialmente relacionados à pornografia infantil, aliciamento de menores, discurso de ódio e incitação à violência. Utilizando identidades falsas, técnicas de criptografia, redes privadas virtuais (VPNs) e proxies, o indivíduo conseguia mascarar sua identidade e localização. Apesar de denúncias feitas por usuários e organizações civis, a resposta das autoridades foi limitada pela dificuldade técnica e jurídica de identificar o responsável e obter os dados armazenados fora do Brasil, onde os servidores do Discord estão sediados.

A dificuldade em rastrear os responsáveis por crimes no ambiente virtual deriva, em grande medida, do anonimato oferecido pelas redes. Como apontam Jesus e Milagre (2016), o Brasil passou a se preocupar com a criminalidade cibernética somente nas últimas duas décadas, o que contribui para a fragilidade das investigações. A ausência de mecanismos ágeis para identificação do autor e a exigência de decisões judiciais para quebra de sigilo dificultam a resposta do Estado aos delitos.

As provas digitais, por sua natureza volátil e efêmera, exigem rapidez na coleta e preservação. Conforme destaca Santos (2021), a identificação do IP é uma etapa inicial crucial nas investigações, mas ela é frequentemente inviabilizada por ferramentas de mascaramento utilizadas por criminosos. Além disso, a LGPD impõe limites ao acesso de dados pessoais por órgãos de investigação, exigindo rigorosos critérios de proporcionalidade e legalidade. No caso em tela, a exigência de autorização judicial para requisição de dados à plataforma resultou em atrasos que comprometeram o rastreamento eficaz do suspeito.

Nesse sentido, a infiltração policial virtual desponta como alternativa viável, desde que amparada por autorização judicial, conforme preconiza a Lei 13.441/17 (Santos, 2021). Essa técnica tem sido empregada, sobretudo, em investigações relacionadas à pornografia infantil,

mas seu uso ainda encontra resistência e pouca regulamentação no que tange a crimes como os do King do Discord, que envolvem múltiplas modalidades ilícitas, combinando delitos sexuais, crimes contra a honra, fraudes e ameaças.

A atuação do Judiciário e dos órgãos de persecução penal ainda esbarra na carência de capacitação técnica. Investigações que envolvem ambientes como o Discord ou a deep web exigem conhecimentos específicos de engenharia reversa, rastreamento de metadados e linguagens de programação, o que está longe da realidade das polícias brasileiras (Lima, 2024).

Além disso, observa-se um descompasso entre o avanço legislativo e a dinâmica dos crimes digitais. A tipificação da invasão de dispositivo informático pelo art. 154-A do Código Penal, inserida pela Lei 12.737/12 (Lei Carolina Dieckmann), representou avanço importante, mas ainda insuficiente frente à complexidade das novas infrações. Muitos delitos não encontram previsão normativa clara, sendo enquadrados por analogia, o que compromete a segurança jurídica (Mendonça, 2023).

O caso também ilustra a necessidade de se repensar o papel das plataformas digitais na cooperação com o poder público. A relutância de empresas em fornecer dados, sob alegação de proteção à privacidade, tem se mostrado um entrave frequente. Nesse aspecto, a adesão do Brasil à Convenção de Budapeste é vista como medida estratégica para promover maior colaboração internacional no combate ao cibercrime (Silva, 2022).

CONCLUSÃO

A partir do exposto neste estudo, é possível afirmar que o fenômeno do cyberbullying revela um cenário desafiador e multifacetado, que exige respostas mais efetivas por parte do sistema jurídico, das autoridades investigativas e da sociedade como um todo. Ficou evidente que, embora o ordenamento jurídico brasileiro tenha avançado com a promulgação de normas como a Lei nº 14.811/2024 e com a adesão à Convenção de Budapeste, esses instrumentos ainda não são suficientes para enfrentar a complexidade das infrações digitais, sobretudo no que diz respeito à coleta e à preservação de provas.

A pesquisa revelou que a produção de provas em crimes de cyberbullying esbarra em obstáculos técnicos, como o uso de criptografia, anonimização e servidores internacionais, além de entraves jurídicos resultantes da aplicação da Lei Geral de Proteção de Dados. Este conflito entre a proteção da privacidade e a necessidade de garantir a segurança pública gera uma tensão

constante, dificultando a responsabilização penal dos agressores e, consequentemente, contribuindo para a perpetuação da violência digital.

Além disso, os casos emblemáticos, como o caso do King do Discord, reforçam esta realidade, ao escancarar as limitações das instituições diante da volatilidade das provas e da necessidade de atuação célere e tecnicamente preparada. A carência de investimentos em capacitação de agentes, a burocracia dos procedimentos legais e a resistência de algumas plataformas em colaborar com as investigações agravam ainda mais o problema.

Apesar disso, o estudo também aponta caminhos promissores. Medidas como a infiltração virtual, quando respeitados os limites legais, e o fortalecimento da cooperação internacional, surgem como ferramentas estratégicas no combate ao cyberbullying. Além disso, destaca-se a importância de políticas públicas que aliem repressão e prevenção, bem como o papel fundamental da educação digital na construção de uma cultura de respeito e segurança no ambiente virtual.

Conclui-se, portanto, que o enfrentamento ao cyberbullying requer uma abordagem integrada, que envolva aprimoramento legislativo, modernização dos meios investigativos, maior responsabilização das plataformas digitais e, sobretudo, um compromisso coletivo com a proteção das vítimas. Somente assim será possível transformar o espaço digital em um ambiente mais justo, seguro e humanizado.

REFERÊNCIAS

BRASIL. **Constituição (1988).** Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988.

_____. **Lei nº 14.811, de 12 de janeiro de 2024.** Altera o Código Penal para dispor sobre os crimes de bullying e cyberbullying e dá outras providências. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/lei/L14811.htm. Acesso em: 25 mar. 2025.

_____. **Lei nº 8.069, de 13 de julho de 1990.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 16 jul. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 25 mar. 2025.

_____. **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). Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 25 mar. 2025.

_____. **Lei nº 13.185, de 6 de novembro de 2015.** Institui o Programa de Combate à Intimidação Sistemática (bullying). Diário Oficial da União: seção 1, Brasília, DF, 9 nov. 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm. Acesso em: 25 mar. 2025.

BRITO, Izabela Pacheco. **Cyberbullying:** os crimes contra honra no ambiente virtual. 2021. Monografia (Graduação em Direito) – Faculdade de Inhumas, Inhumas-GO, 2021.

CASTRO, José Ernane Barbosa de. Resenha do artigo intitulado: "A ineficácia da punibilidade do cyberbullying no Brasil". **Revista Processus Multidisciplinar**, v. 2, n. 4, jul./dez. 2021. ISSN: 2675-6595. Disponível em: https://doi.org/10.5281/zenodo.5525129. Acesso em: 15 abr. 2025.

FILHO, Antonio Cesar Correia et al. **Os crimes cibernéticos, a necessidade da Lei nº 14.155/21 e as dificuldades na investigação.** Carangola-MG: Faculdade Doctum, 2024.

FREITAS, Elison de Araújo; SILVA, Pedro Henrique Aguiar; SOUZA, Márcio Cabral de. **Crimes cibernéticos: desafios da investigação e preservação das provas. JNT - Facit Business and Technology Journal**, ed. 44, v. 1, p. 178-194, ago. 2023. ISSN: 2526-4281. Disponível em: http://revistas.faculdadefacit.edu.br. Acesso em: 15 abr. 2025.

GONÇALVES, Jonas Rodrigo; OLIVEIRA, Lívia Rebeca Gramajo. A ineficácia da punibilidade do cyberbullying no Brasil. **Revista Educar Mais**, Pelotas, v. 4, n. 2, p. 308–319, 2020. Disponível em: https://periodicos.ifsul.edu.br/index.php/educarmais/article/view/1819. Acesso em: 22 maio 2025.

HAMID, Supardi; SAKA, Octalya; RUSMAWAN, Teddy. **Cyberbullying: an analysis of the impact of crime phenomena in the digital era on the social life of society.** Riwayat: Educational Journal of History and Humanities, v. 6, n. 4, p. 2535-2542, out. 2023. Disponível em: https://doi.org/10.24815/jr.v6i4.34914. Acesso em: 15 abr. 2025.

JESUS, Damásio de. MILAGRE, José Antonio. **Manual de crimes informáticos**, São Paulo: Saraiva, 2016.

LEAL, Maria Eduarda. A criminalização do bullying e do cyberbullying: desafios e implicações legais no contexto brasileiro. 2024. **Artigo de Conclusão de Curso (Bacharelado em Direito)** – Universidade Federal de Santa Maria, Santa Maria, RS, 2024. Disponível em: https://www.ufsm.br. Acesso em: 25 mar. 2025.

LIMA, Douglas Magno Fernandes do Nascimento. **Os desafios da investigação nos crimes cibernéticos.** Santa Rita: Universidade Federal da Paraíba, 2024. Disponível em: https://www.ufpb.br. Acesso em: 25 mar. 2025.

LOBO, Milena Garcia de Souza; CORDEIRO, Taiana Levinne Carneiro. As consequências jurídicas do bullying e cyberbullying: responsabilidade civil e criminal nos espaços educacionais. **Revista Ibero-Americana de Humanidades, Ciências e Educação – REASE**, São Paulo, v. 10, n. 11, nov. 2024. Disponível em: https://doi.org/10.51891/rease.v10i11.16719. Acesso em: 15 abr. 2025.

MENDONÇA, Felipe Thiago Porfírio de. **Crimes cibernéticos – a perícia técnica (Lei Carolina Dieckmann).** 2023. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Pontifícia Universidade Católica de Goiás, Escola de Direito, Negócios e Comunicação, Goiânia, 2023. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/7361. Acesso em: 22 maio 2025.

MUZAKIR, Ari; SYAPUTRA, Hadi; PANJAITAN, Febriyanti. A **comparative analysis of classification algorithms for cyberbullying crime detection: an experimental study of Twitter social media in Indonesia.** Scientific Journal of Informatics, v. 9, n. 2, p. 133-137, nov. 2022. Disponível em: https://journal.unnes.ac.id/nju/index.php/sji/article/view/35149. Acesso em: 25 mar. 2025.

OLIVEIRA, Geovana Xavier de. Crimes cibernéticos: direito digital e os novos paradigmas da investigação criminal. 2022. **Artigo Científico (Graduação em Direito)** – Pontifícia Universidade Católica de Goiás, Goiânia, 2022.

PINTO, Samara Silva. **Dos crimes virtuais, da obtenção das provas e as tendências jurídicas decorrentes da evolução tecnológica.** Brasília: Instituto Brasiliense de Direito Público – IDP, 2022. Disponível em: https://www.idp.edu.br. Acesso em: 15 abr. 2025.

QUEIROZ, Liv Ferreira Augusto Severo. Os crimes cibernéticos no ordenamento jurídico brasileiro: investigação criminal e desafios. **Revista do Conselho Nacional do Ministério Público** – CNMP, v. 12, p. 417-432, 2024. Disponível em: https://www.cnmp.mp.br/portal/publicacoes/revista-do-cnmp. Acesso em: 25 mar. 2025.

REZENDE SANTOS, Ana Paula Torres. A infiltração policial virtual como meio de investigação de crimes cibernéticos: os limites para a obtenção de provas válidas. 2021. **Monografia (Graduação em Direito)** – Centro Universitário de Brasília, Brasília, 2021.

SCHEEL, Fernanda et al. **Crimes virtuais e cyberbullying:** uma conversa com alunos da rede pública estadual da cidade de Londrina. V PRÓ-ENSINO: Mostra Anual de Atividades de Ensino da UEL, 10 nov. 2023. Universidade Estadual de Londrina.

SILVA, Dickson Carvalho Gonçalves da. Crimes cibernéticos: limites e desafios da investigação. 2022. **Monografia (Graduação em Direito)** – Centro Universitário UNDB, São Luís, 2022.

SOUSA, Luyd Nuan Pimentel Andrade de; SANTOS, Monalisa Davinci de Sousa; OLIVEIRA, Edjôfre Coelho de. Cyberbullying: responsabilidade civil e seus efeitos na sociedade. **Revista Ibero-Americana de Humanidades, Ciências e Educação – REASE**, São Paulo, v. 10, n. 5, maio 2024. Disponível em: https://doi.org/10.51891/rease.v10i5.14147. Acesso em: 15 abr. 2025.

SANTOS, Camilly Vitoria Moraes dos; SILVA, Gabrielly Vitória de Lima; GEROLA, Murilo; ALVES, Roseli Pedroso. **Desafios jurídicos na identificação e punição do cyberbullying.** Santa Bárbara D'Oeste: Etec Prof. Dr. José Dagnoni, 2024. Disponível em: https://www.etecjosedagnoni.com.br. Acesso em: 25 mar. 2025.

SANTOS, Ana Paula Torres Rezende. **A infiltração policial virtual como meio de investigação de crimes cibernéticos: os limites para a obtenção de provas válidas.** Brasília: Centro Universitário de Brasília – UniCEUB, 2021. Disponível em: https://www.uniceub.br. Acesso em: 25 mar. 2025.

SEVERO QUEIROZ, Liv Ferreira Augusto. Os crimes cibernéticos no ordenamento jurídico brasileiro: investigação criminal e desafios**. Revista do Conselho Nacional do Ministério Público – CNMP**, v. 12, p. 417-432, 2024. Disponível em: https://www.cnmp.mp.br/portal/publicacoes/revista-do-cnmp. Acesso em: 25 mar. 2025.

TANES, João Antônio de Oliveira. Crimes cibernéticos no e-sports, cyberbullying. 2023. **Trabalho de Conclusão de Curso (Bacharelado em Direito)** – Centro Universitário UNIFACIG, Manhuaçu, MG, 2023. Disponível em: https://www.unifacig.edu.br. Acesso em: 25 mar. 2025.

VICTOR DUARTE, Samuel; ALMEIDA, Tyciano Magno de Oliveira. **Coagindo crimes cibernéticos:** uma análise do arcabouço legal brasileiro para a segurança digital e comunicação. Altus Ciência, v. 18, ago./dez. 2023. Disponível em: https://doi.org/10.5281/zenodo.8144558. Acesso em: 15 abr. 2025.

ZACARIAS, Fabiana; FREIRE, Lucas Zacharias. **Crimes virtuais:** análise das dificuldades e limitações ao combate. Revista JurES, v. 16, n. 29, p. 29-61, jun. 2023. ISSN 2179-0167.