

Responsabilidade civil e criminal quanto à prática do *cyberstalking*

Civil and Criminal Liability in Cases of Cyberstalking

DÁYNE KÉTTLEN SILVEIRA GONÇALVES

Discente de Direito (UNIPAM)
daynekettlen@unipam.edu.br

RODRIGO LUIZ DA SILVA VERSIANI

Professor orientador (UNIPAM)
rodrigoversiani@unipam.edu.br

ELINE DÉBORA TEIXEIRA

Professora coorientadora (UNIPAM)
elinedebora@unipam.edu.br

Resumo: O presente artigo analisa a responsabilidade civil e criminal decorrente da prática do *cyberstalking*, compreendido como forma contemporânea de perseguição reiterada realizada por meio de tecnologias digitais, capaz de violar direitos fundamentais da vítima, especialmente a liberdade, a privacidade, a dignidade da pessoa humana e a integridade psíquica. O problema central da pesquisa consiste em verificar se o ordenamento jurídico brasileiro, após a tipificação do crime de perseguição pelo art. 147-A do Código Penal (Lei nº 14.132/2021), é suficiente para assegurar a responsabilização efetiva dos agressores e a reparação integral dos danos sofridos pelas vítimas no ambiente digital. Para tanto, adota-se metodologia qualitativa, com abordagem dogmático-jurídica e método dedutivo, desenvolvida por meio de pesquisa bibliográfica, documental e jurisprudencial, com análise da legislação penal, civil e constitucional, bem como de decisões dos tribunais superiores. Os resultados evidenciam que, embora haja avanço legislativo na criminalização do *cyberstalking* e no agravamento de crimes cibernéticos, persistem lacunas normativas e dificuldades práticas relacionadas à produção e preservação de provas digitais, à identificação dos agressores e à integração entre as esferas civil e penal. Conclui-se que a tutela jurídica adequada das vítimas de *cyberstalking* exige uma abordagem normativa integrada, aliada ao fortalecimento das investigações digitais, à responsabilização civil eficaz e à adoção de políticas públicas preventivas, como forma de garantir a efetividade dos direitos fundamentais no ambiente virtual.

Palavras-chave: *cyberstalking*; responsabilidade civil; responsabilidade penal; direitos fundamentais; violência digital.

Abstract: This article analyzes the civil and criminal liability arising from the practice of *cyberstalking*, understood as a contemporary form of repeated harassment carried out through digital technologies, capable of violating the victim's fundamental rights, particularly freedom, privacy, human dignity, and psychological integrity. The central research problem consists of determining whether the Brazilian legal system, following the criminalization of stalking under Article 147-A of the Penal Code (Law No. 14,132/2021), is sufficient to ensure the effective

accountability of perpetrators and the full compensation of damages suffered by victims in the digital environment. To this end, a qualitative methodology was adopted, based on a doctrinal legal approach and deductive method, developed through bibliographic, documentary, and case law research, including analysis of criminal, civil, and constitutional legislation, as well as decisions of higher courts. The findings indicate that, although there has been legislative progress in the criminalization of cyberstalking and the strengthening of cybercrime provisions, normative gaps and practical challenges remain, particularly concerning the production and preservation of digital evidence, the identification of perpetrators, and the coordination between civil and criminal spheres. It is concluded that the adequate legal protection of cyberstalking victims requires an integrated normative approach, combined with the strengthening of digital investigations, effective civil liability mechanisms, and the implementation of preventive public policies, in order to ensure the effective protection of fundamental rights in the virtual environment.

Keywords: cyberstalking; civil liability; criminal liability; fundamental rights; digital violence.

1 INTRODUÇÃO

O avanço das tecnologias digitais e a consolidação da internet como espaço central das interações sociais transformaram profundamente a forma como as relações humanas se desenvolvem. Se, por um lado, esses avanços ampliaram as possibilidades de comunicação e acesso à informação, por outro, também criaram um ambiente propício à emergência de novas modalidades de violência, especialmente aquelas praticadas de forma reiterada e invisibilizada no meio virtual. Nesse contexto, destaca-se o *cyberstalking*, caracterizado pelo assédio persistente, obsessivo e não consentido, realizado por meios digitais, capaz de violar direitos fundamentais da vítima, como a liberdade, a privacidade, a dignidade e a integridade psíquica (Wermuth; Callegari, 2021).

Embora a perseguição virtual se manifeste inicialmente no ambiente digital, seus efeitos frequentemente extrapolam essa esfera, atingindo de forma concreta a vida cotidiana da vítima. A vigilância constante, o controle de rotinas, as ameaças e a exposição indevida em redes sociais produzem impactos psicológicos e sociais profundos, gerando medo, insegurança e restrições à autodeterminação pessoal (Almeida da Silva, 2022). Trata-se, portanto, de uma forma de violência que não pode ser compreendida como mero dissabor ou conflito interpessoal, mas como violação grave à dignidade da pessoa humana.

A tipificação do crime de perseguição no ordenamento jurídico brasileiro, por meio da Lei nº 14.132/2021, que introduziu o art. 147-A no Código Penal, representou um avanço relevante ao reconhecer juridicamente a gravidade dessas condutas. No entanto, a criminalização isolada não se mostrou suficiente para assegurar proteção integral às vítimas, sobretudo diante das peculiaridades do ambiente digital, marcado pelo anonimato, pela volatilidade das provas e pela dificuldade de identificação dos agressores (Cunha, 2022).

Nesse cenário, evidencia-se um problema jurídico central: apesar da recente tipificação penal do *cyberstalking*, o sistema jurídico brasileiro ainda enfrenta dificuldades estruturais e interpretativas para responsabilizar de forma eficaz os

agressores e assegurar a reparação integral dos danos sofridos pelas vítimas, especialmente no âmbito digital. A atuação fragmentada entre as esferas penal e civil, aliada à ausência de protocolos claros de preservação de provas digitais e à limitação da responsabilização institucional, compromete a efetividade da tutela jurídica (Moraes, 2007).

Diante dessa problemática, o presente artigo tem como objetivo analisar criticamente a responsabilidade civil e criminal decorrente da prática do *cyberstalking* no ordenamento jurídico brasileiro, identificando lacunas normativas, fragilidades na aplicação das normas vigentes e desafios relacionados à investigação e à persecução penal. Parte-se da hipótese de que a proteção adequada das vítimas de *cyberstalking* exige uma abordagem integrada entre as esferas civil e penal, bem como uma interpretação constitucionalmente orientada das normas tradicionais à luz da realidade da sociedade digital contemporânea.

A presente pesquisa adota uma abordagem qualitativa, partindo de princípios gerais do ordenamento jurídico, notadamente a dignidade da pessoa humana, a proteção dos direitos da personalidade e a liberdade individual, para a análise específica da responsabilização civil e criminal no contexto do *cyberstalking*. Trata-se de um estudo de natureza dogmático-jurídica e analítico-crítica, voltado à compreensão dos limites e das possibilidades da tutela jurídica frente às novas formas de violência digital.

Quanto aos procedimentos técnicos, realizou-se pesquisa bibliográfica, documental e jurisprudencial. A pesquisa bibliográfica fundamentou-se em doutrina nacional e estrangeira relevante, especialmente nas áreas do Direito Penal, Direito Civil, direitos fundamentais e violência digital, com destaque para autores que analisam o *cyberstalking* e a criminalização da perseguição virtual (Wermuth; Callegari, 2021; Brito, 2021; Silva, 2023). A pesquisa documental concentrou-se na análise da legislação brasileira vigente, incluindo a Constituição Federal de 1988, o Código Penal, o Código Civil, a Lei nº 14.132/2021, a Lei nº 14.155/2021, o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Maria da Penha (Lei nº 11.340/2006).

Complementarmente, foi realizada pesquisa jurisprudencial, com exame de decisões dos tribunais superiores e de tribunais estaduais, visando compreender como o Poder Judiciário tem aplicado as normas relativas ao *cyberstalking* e aos crimes digitais, especialmente no que se refere à produção de provas, à definição de competência e à responsabilização penal e civil dos agressores (Brasil, 2020).

A seleção das fontes priorizou obras e artigos científicos contemporâneos, com reconhecida relevância acadêmica, observando-se um recorte temporal concentrado no período posterior à tipificação do crime de perseguição no Brasil, sem prejuízo da utilização de referências anteriores indispensáveis à construção teórica e conceitual do tema. Por fim, a metodologia adotada buscou não apenas descrever o arcabouço normativo existente, mas promover uma análise crítica de sua efetividade prática, apontando limites, contradições e possibilidades de aprimoramento da tutela jurídica frente ao fenômeno do *cyberstalking*.

A relevância do estudo sobre o *cyberstalking* evidencia-se diante do crescimento expressivo dos casos de perseguição no Brasil, especialmente em contextos que envolvem o uso de tecnologias digitais. De acordo com o Anuário Brasileiro de Segurança Pública 2024, elaborado pelo Fórum Brasileiro de Segurança Pública (2024),

foram registrados 77.083 casos de stalking contra mulheres no ano de 2023, representando um aumento de 34,5% em relação ao ano anterior, o que equivale a uma ocorrência a cada 6 minutos e 48 segundos no país. Considerando-se que grande parte dessas condutas se manifesta ou se intensifica no ambiente virtual, por meio de redes sociais, aplicativos de mensagens e outros meios digitais, o dado revela a dimensão estrutural e crescente do problema, bem como seus impactos diretos sobre a liberdade, a privacidade e a saúde psicológica das vítimas. Nesse contexto, justifica-se a necessidade de aprofundamento acadêmico e jurídico sobre o *cyberstalking*, especialmente quanto à efetividade dos mecanismos de prevenção, responsabilização e tutela dos direitos fundamentais no ambiente digital.

2 A CRIMINALIDADE VIRTUAL E O CYBERSTALKING: UMA ANÁLISE DOS PRINCIPAIS TIPOS DE CIBERCRIME

Atualmente, a prática de crimes por meio de dispositivos conectados à internet tem recebido diversas denominações na doutrina e na literatura especializada. Termos como delitos digitais, infrações informáticas, crimes virtuais, ilícitos cibernéticos e fraudes tecnológicas são frequentemente utilizados. No presente trabalho, adota-se a expressão “cibercrimes” como padrão terminológico, em razão de sua abrangência e aceitação crescente no meio jurídico.

O conceito de cibercrime pode ser compreendido como todo comportamento ilícito, não autorizado ou antiético que envolva tecnologias computacionais, seja pelo processamento de informações, seja pela transmissão de dados em rede. Pode ter como alvo indivíduos ou instituições, visando obter vantagem ilícita ou causar prejuízos à estrutura funcional ou à reputação das vítimas, sempre por meio de recursos tecnológicos.

A doutrina especializada costuma organizar os cibercrimes em duas categorias distintas: os cibercrimes próprios e os cibercrimes impróprios. Os cibercrimes próprios têm como alvo direto os sistemas tecnológicos e suas estruturas, de modo que o bem jurídico violado é a própria integridade da informação ou do sistema informático. Representam novas formas delituosas surgidas com o avanço da tecnologia, muitas das quais ainda enfrentam lacunas normativas, dificultando a atuação do poder punitivo estatal. Exemplos desse grupo incluem a invasão de contas eletrônicas, disseminação de malwares, sabotagem digital e pirataria de softwares.

Já os cibercrimes impróprios referem-se àqueles em que o agente utiliza a tecnologia como meio para praticar crimes convencionais. São infrações já previstas em leis penais anteriores, mas que passaram a ser executadas com o auxílio de dispositivos eletrônicos e redes digitais. O uso da internet como ferramenta para aplicar golpes é um exemplo claro dessa categoria, como no caso do estelionato digital, uma adaptação contemporânea do crime previsto no artigo 171 do Código Penal.

Entre os cibercrimes, destaca-se o *cyberstalking* ou perseguição virtual, caracterizado por condutas repetitivas e obsessivas de vigilância, monitoramento, ameaças e constrangimentos virtuais. O agressor recorre a redes sociais, e-mails, aplicativos de mensagens e até geolocalização para invadir a privacidade da vítima. Mais

do que um simples incômodo, trata-se de uma prática persistente que cria um ambiente de medo diário, afetando a liberdade e a dignidade da pessoa, podendo gerar sérios prejuízos emocionais e exigir medidas protetivas e ações judiciais urgentes, já que pode evoluir para perseguição física, agressões e até violência letal.

A perseguição digital, além de configurar infração penal autônoma com base na Lei nº 14.132/2021, que inseriu o artigo 147-A no Código Penal, também pode ofender direitos fundamentais garantidos constitucionalmente, como o previsto no art. 5º, inciso X, da Constituição Federal: “São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (Brasil, 1988, art. 5º, inciso X).

É um preceito que guia a proteção da dignidade da pessoa humana e tem por função resguardar o indivíduo contra qualquer forma de violência, abuso ou humilhação que comprometa sua integridade física, moral e psicológica. No âmbito penal, a vedação a tratamentos desumanos e degradantes ultrapassa a proibição física de agressões e torturas abrangendo também formas sutis de violência, aquelas impetradas no meio virtual.

O reconhecimento do *cyberstalking* como um comportamento passível de ser enquadrado na proteção do art. 5º, X requer que o ordenamento jurídico contemple as agressões não apenas físicas, mas também psicológicas. A interpretação constitucional deve ser ampla e atualizada, considerando o contexto da sociedade digital em que as agressões imateriais causam danos reais e profundos.

3 ESPÉCIES DE CYBERSTALKING

As diferentes espécies de *cyberstalking* demonstram como a tecnologia pode ser usada para práticas abusivas, como comunicações insistentes, invasão de dispositivos, exposição de imagens ou rastreamento por geolocalização. Essas condutas configuram violência psicológica e digital, causando sérios danos às vítimas e já encontram respaldo na legislação brasileira, refletindo a crescente preocupação jurídica e social com a proteção das vítimas em ambientes virtuais.

3.1 ASSÉDIO POR COMUNICAÇÃO DIRETA

Trata-se de uma conduta em que o agressor busca contato frequente com a vítima, utilizando canais como e-mail, aplicativos de mensagens instantâneas, redes sociais ou mensagens de texto. São utilizados também perfis falsos para dificultar sua identificação, embora podendo agir com sua identidade real.

Como mencionado no livro *Stalking*, o *cyberstalking* conta com três vantagens: a possibilidade de se comunicar a distância; a possibilidade de entrar em contato também com pessoas desconhecidas; e a garantia do anonimato (Amiky, 2014). Pelos dados trazidos por Mazzola, o *stalking* cometido por e-mail já soma 80% dos casos (*apud* Amiky, 2014).

Esse tipo de perseguição se caracteriza pela insistência e abusividade de contato, os quais podem evoluir para conteúdos agressivos, ameaçadores, de cunho

sexual ou intimidador. A vítima com o passar do tempo pode sofrer abalos psicológicos, sem meios eficazes de se proteger, com as mensagens muitas vezes sendo direcionadas a familiares, amigos e parceiros, ampliando o dano social e emocional.

3.2 ASSÉDIO POR INVASÃO INFORMÁTICA

Uma das formas avançadas de *cyberstalking* envolve a invasão dos dispositivos eletrônicos da vítima, como computadores, celulares ou outros meios digitais. O agressor pode monitorar mensagens, capturar arquivos, acompanhar a localização em tempo real e, em casos mais graves, se passar pela vítima para enganar terceiros e obter informações adicionais.

A Lei nº 14.155/2021, que altera o Código Penal para tratar da invasão de dispositivos informáticos, representa um avanço significativo nesse contexto. Segundo essa norma, acessar indevidamente equipamentos eletrônicos alheios, com o objetivo de obter, adulterar ou destruir dados, ou instalar vulnerabilidades para vantagem ilícita, é punível com reclusão de 1 (um) a 4 (quatro) anos, com aumento da pena caso haja prejuízo econômico à vítima.

Nos termos do art. 154-A do Código Penal:

Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita. (Brasil, 2021, art.154-A do CP).

A eficácia dessa norma depende da capacidade investigativa e da coleta de provas digitais, ainda limitadas por obstáculos técnicos e jurídicos no Brasil. Apesar do avanço legislativo, permanece urgente a necessidade de aprimorar a cooperação entre autoridades, investir em perícia especializada e aumentar a conscientização social sobre os riscos à privacidade no ambiente virtual.

3.3 ASSÉDIO POR EXPOSIÇÃO PÚBLICA E MANIPULAÇÃO DE IMAGEM

Outra vertente do *cyberstalking* diz respeito à exposição pública. Trata-se da utilização de fotos, vídeos ou áudios, muitas vezes obtidos sem consentimento, com o objetivo de difamar, chantagear ou ridicularizar a vítima perante sua rede de contatos ou o público em geral.

Essa prática pode incluir desde a divulgação de conteúdos íntimos, muitas vezes associada à chamada “pornografia de vingança”, até a adulteração de imagens por meio de inteligência artificial, com a finalidade de criar informações falsas que denigram a reputação da vítima. Os efeitos são especialmente prejudiciais para mulheres, reforçando estereótipos de gênero e perpetuando violências psicológicas.

Diferentemente de mensagens privadas, postagens públicas ofensivas ou falsas em redes sociais podem expor a vítima a um linchamento virtual, atingindo sua honra, imagem e reputação em um espaço de ampla visibilidade e de difícil controle. Mesmo

após decisões judiciais, a remoção completa desse conteúdo pode ser dificultada. Consequentemente, a vítima passa a conviver com vigilância constante e sensação de desamparo, o que pode levar ao isolamento social e à deterioração da saúde mental.

3.4 ASSÉDIO COM USO DE TECNOLOGIAS DE GEOLOCALIZAÇÃO

A tecnologia de geolocalização para fins de perseguição representa uma evolução preocupante, aplicativos de localização em tempo real, sistemas de rastreamento por *Global Positioning System* (GPS) e dispositivos de monitoramento instalados clandestinamente em veículos ou objetos pessoais permitem que o agressor acompanhe os deslocamentos da vítima com alta precisão.

Esse tipo de assédio compromete não apenas a privacidade, mas também a integridade física da pessoa perseguida, pois permite ao autor do crime prever rotinas e horários, facilitando abordagens presenciais ou ataques mais diretos. É comum que esse controle seja exercido em contextos de relações abusivas, nas quais o agressor deseja manter domínio sobre todos os aspectos da vida da vítima, inclusive após o rompimento do vínculo afetivo.

A utilização de tecnologias de localização se tornou um mecanismo recorrente de vigilância e coerção no contexto de violência doméstica e familiar, a Lei Maria da Penha (Lei nº 11.340/2006), embora focada na violência contra a mulher, tem sido interpretada de forma extensiva para incluir casos de *cyberstalking* com base em geolocalização, especialmente quando presentes os elementos de controle, ameaça e sofrimento psicológico. Além disso, o PL 3.890/2020 (Estatuto da Vítima), visa ampliar a proteção legal às vítimas de violência digital, incluindo explicitamente práticas de rastreamento como forma de assédio criminalizável. Essa compreensão é respaldada pela Lei nº 13.772/2018, que, em seu artigo 7º, inciso II, define a violência psicológica como:

A violência psicológica, entendida como qualquer conduta que lhe cause dano emocional e diminuição da autoestima ou que lhe prejudique e perturbe o pleno desenvolvimento ou que vise degradar ou controlar suas ações, comportamentos, crenças e decisões, mediante ameaça, constrangimento, humilhação, manipulação, isolamento, vigilância constante, perseguição contumaz, insulto, chantagem, violação de sua intimidade, ridicularização, exploração e limitação do direito de ir e vir ou qualquer outro meio que lhe cause prejuízo à saúde psicológica e à autodeterminação [...] (Brasil, 2018 , art. 7º , inciso II, Redação dada pela Lei nº 13.772/2018).

A tipificação da violência psicológica, prevista no artigo 7º, inciso II, da Lei Maria da Penha, ganha especial relevância, pois abrange com precisão as condutas típicas do perseguidor digital, que utiliza recursos tecnológicos para controlar, intimidar, vigiar e desestabilizar emocionalmente a vítima. Assim, o *cyberstalking* pode ser compreendido não apenas como um crime informático, mas também como uma modalidade insidiosa de violência psicológica.

4 IMPACTOS PSICOLÓGICOS DO CYBERSTALKING: VÍTIMAS E AGRESSORES

As vítimas de *cyberstalking* sofrem com ansiedade, depressão e prejuízos nas relações pessoais, enquanto os agressores costumam apresentar traços obsessivos, impulsivos ou antissociais, motivados por controle, vingança ou satisfação pessoal. A compreensão desses impactos é essencial para orientar medidas preventivas, oferecer suporte psicológico e fundamentar estratégias jurídicas que assegurem proteção efetiva no ambiente virtual.

4.1 CONSEQUÊNCIAS PSICOLÓGICAS PARA AS VÍTIMAS

O *cyberstalking* provoca impactos psicológicos graves e duradouros, afetando a saúde mental e o funcionamento diário das vítimas. Frequentemente, elas desenvolvem ansiedade, depressão e transtorno de estresse pós-traumático, prejudicando suas relações sociais, trabalho e rotina. A sensação constante de vulnerabilidade e o medo de novas agressões aumentam esses efeitos, podendo levar ao isolamento e à baixa autoestima.

É essencial destacar que as respostas ao trauma podem variar de pessoa para pessoa. Assim como a gravidade do trauma emocional pode ser influenciada por fatores como o nível de resiliência da pessoa, o suporte social e as circunstâncias específicas em que o trauma ocorreu.

Um impacto comum nas vítimas é o Transtorno de Estresse Pós-traumático (TEPT), que surge após experiências traumáticas. As vítimas revivem o trauma por meio de memórias intrusivas, pesadelos e flashbacks, o que dificulta o cotidiano. Esses sintomas podem incluir ansiedade intensa e evasão de lugares ou situações associadas ao trauma, comprometendo a vida normal.

O TEPT, ou Perturbação de Estresse Pós-traumático (PSPT), é o distúrbio de ansiedade que se manifesta por meio de uma variedade de sintomas físicos, psicológicos e emocionais. Essa condição ocorre em pessoas que foram vítimas ou testemunhas de eventos violentos ou experiências traumáticas. Entre os sintomas mais comuns, estão o distanciamento emocional, os pesadelos e *flashbacks* involuntários de memórias traumáticas.

As vítimas podem desenvolver depressão intensa em decorrência do trauma, manifestada por sentimentos persistentes de tristeza, desesperança e perda de interesse por atividades antes prazerosas. Esse quadro frequentemente leva ao isolamento social, dificultando a recuperação emocional, especialmente na ausência de apoio adequado.

O *cyberstalking* também impacta significativamente as relações interpessoais. O medo e a insegurança podem comprometer a confiança nos outros, fragilizando vínculos familiares e de amizade e criando um ciclo de retraimento social que intensifica o sofrimento psicológico.

Além disso, muitas vítimas desenvolvem uma percepção distorcida de si mesmas e do mundo, sentimento de culpa, vergonha e impressão de responsabilidade pelo ocorrido, mesmo sem qualquer controle sobre a situação. Esses fatores intensificam o sofrimento emocional e podem desencadear comportamentos autodestrutivos, como o

uso de álcool, drogas ou autoagressão, estratégias equivocadas para lidar com a dor psicológica.

O impacto do *cyberstalking* também se estende ao ambiente profissional. A necessidade de afastamento para tratamento ou alterações no comportamento podem gerar dificuldades no trabalho, incluindo a perda de emprego.

É importante destacar que a intensidade dos efeitos varia conforme fatores individuais. Indivíduos com experiências traumáticas prévias podem reagir de forma mais intensa a novos traumas, enquanto outros podem se beneficiar de sua experiência para fortalecer sua recuperação.

Além das consequências psicológicas, o trauma pode gerar impactos físicos, incluindo dores crônicas, fadiga e distúrbios gastrointestinais, evidenciando a relação entre saúde mental e física. O tratamento especializado é fundamental, podendo envolver terapia cognitivo-comportamental, terapia de exposição e grupos de apoio, oferecendo à vítima um espaço seguro para processar a experiência e desenvolver estratégias de enfrentamento.

Os profissionais de saúde mental devem estar capacitados para lidar com diferentes tipos de trauma, aplicando técnicas específicas e sensibilidade cultural. Paralelamente, a criação de redes de apoio comunitárias contribui para reduzir o estigma e favorecer a recuperação emocional. Além disso, é essencial que as vítimas tenham conhecimento sobre seus direitos legais, considerando que a liberdade de expressão não é ilimitada, e que o Código Penal Brasileiro prevê sanções para crimes digitais, incluindo a Lei Carolina Dieckmann, que tipifica a invasão de dispositivos eletrônicos e a divulgação indevida de dados pessoais.

4.2 PERFIL PSICOLÓGICO DOS AGRESSORES DE CYBERSTALKING

Embora a maior parte da literatura sobre *cyberstalking* concentre-se nas vítimas, compreender o perfil psicológico dos agressores é essencial para prevenção e reabilitação. Estudos indicam que os indivíduos que praticam *cyberstalking* frequentemente apresentam traços de personalidades obsessivas, são impulsivos e de baixa empatia, associados a uma necessidade de controle e domínio sobre a vítima.

Em muitos casos, esses agressores exibem comportamentos compatíveis com traços de narcisismo, maquiavelismo e psicopatia, utilizando o ambiente virtual como um meio de perseguição que lhes garante anonimato e reduz a percepção de consequências legais. Essa sensação de impunidade reforça a repetição do comportamento e dificulta a autorreflexão sobre os danos causados.

As motivações podem variar, incluindo vingança, ciúme, desejo de controle e satisfação pessoal como a busca por poder, frequentemente acompanhadas da dificuldade em reconhecer ou se importar com o sofrimento da vítima. Além disso, alguns agressores possuem histórico de traumas ou experiências sociais problemáticas que contribuem para a adoção de condutas agressivas.

Compreender esses padrões psicológicos é fundamental não apenas para a atuação judicial, mas também para a elaboração de políticas de prevenção, programas educativos e estratégias de reabilitação, podendo incluir acompanhamento psicológico,

medidas restritivas e ações de conscientização sobre os limites éticos do comportamento online.

5 RESPONSABILIDADES JURÍDICA E PREVENÇÃO

É fundamental analisar a responsabilização jurídica dos agressores e das plataformas digitais envolvidas. Essa responsabilização se desdobra em esferas civil e criminal, visando à reparação dos danos sofridos pelas vítimas e à punição dos infratores. Além disso, a prevenção assume papel central, integrando medidas jurídicas, tecnológicas e educativas que protejam os indivíduos e reduzam a reincidência de tais condutas.

5.1 RESPONSABILIDADE CIVIL NO CYBERSTALKING

É inegável que a ordem jurídica brasileira contemple diversas condutas consideradas ilícitas, contudo nem todo ato ilícito configura um crime. O ordenamento jurídico abrange uma ampla variedade de comportamentos ilícitos presentes nas esferas administrativa, tributária, trabalhista, civil, entre outras.

Embora o *cyberstalking* não seja tipificado em todas as suas formas, essas práticas são igualmente condenáveis, pois violam direitos fundamentais assegurados pela Constituição Federal de 1988. Tais atos atentam contra o princípio da dignidade da pessoa humana, comprometendo a autodeterminação das vítimas e ameaçando seu bem-estar, provocando medo, inquietação e transtornos psicológicos. Ao ferir direitos essenciais, como a liberdade e a privacidade, o assediador, por meios físicos ou digitais, torna-se passível de responsabilização na esfera civil.

Conforme dispõe o artigo 186 do Código Civil, “aquele que, por ação ou omissão voluntária, negligência ou imprudência, viola direito e causa danos a outrem, ainda que exclusivamente moral, comete ato ilícito” (Brasil, 2002).

Pode-se afirmar que tais condutas apresentam nexo causal com os dispositivos da legislação civil, na medida em que o dano decorre diretamente da ação do agente, tornando incontestável a responsabilidade civil e o dever de indenizar.

Além disso, a Constituição Federal, em seu art. 5º, inciso V, garante o direito à reparação de danos materiais e morais, o que representa não apenas a proteção contra o inadimplemento de obrigações, mas também a ampliação das hipóteses de responsabilização, em consonância com a evolução das demandas sociais. Nesse contexto, Moraes (2007) destaca que houve uma mudança significativa no enfoque da responsabilidade civil, que passou a privilegiar a proteção da vítima em vez da conduta do agente:

Com o advento da Constituição de 1988, fixou-se a prioridade à proteção da dignidade da pessoa humana e, em matéria de responsabilidade civil, tornou-se plenamente justificada a mudança de foco, que, em lugar da conduta (culposa ou dolosa) do agente, passou a enfatizar a proteção à vítima de dano injusto, daí o alargamento das

hipóteses de responsabilidade civil objetiva, que independe da culpa, isto é, da prática do ato ilícito (Moraes, 2007, p. 29).

Um aspecto que merece destaque é a equivalência entre as condutas praticadas no ambiente online e aquelas realizadas no mundo físico. Dessa forma, uma ação considerada ilícita fora do ambiente digital deverá ser igualmente reconhecida como ilícita quando realizada na internet. Essa igualdade simplifica a análise jurídica das condutas digitais, facilitando a determinação de sua licitude ou ilicitude.

Não há dúvidas de que a violação da tranquilidade causada pela ação injusta de um perseguidor, por si só, configura um dano. A sensação de ser vigiado, ofendido, atacado ou mesmo a necessidade de se abster do uso habitual da Internet, a fim de evitar a situação vivenciada, provoca abalo psicológico que vai além de um mero dissabor cotidiano.

Ao estudar o instituto da prescrição no direito penal, utiliza-se frequentemente a metáfora da espada de Dâmocles para justificar a inadmissibilidade de se manter a “Espada da Justiça” de forma indefinida sobre a cabeça do investigado. De maneira análoga, tal metáfora se aplica ao presente contexto: a ausência de responsabilização, ainda que na esfera civil, gera a sensação de que o perseguidor mantém constantemente sua “espada” sobre a vítima. O medo permanente sofrido pelo perseguido configura, por si, um dano capaz de ensejar o dever de indenizar.

Embora não seja imprescindível, o dano material também pode estar presente. Em decorrência das ações de um perseguidor, a vítima pode vir a perder o emprego, encerrar relações comerciais; em ambos os casos pode haver danos materiais na forma de lucros cessantes ou ainda despendar recursos financeiros para minimizar os prejuízos sofridos, configurando situações de danos emergentes, diante da existência de um dano, material ou moral, decorrente da quebra do direito à tranquilidade.

Independentemente do sistema de imputação, objetiva ou subjetiva, é fundamental demonstrar o nexo causal entre a conduta do *cyberstalking* e o prejuízo da vítima. Diferentemente de outras ciências que analisam efeitos para identificar causas, o Direito exige constatar o vínculo entre o ato ilícito e os danos dele decorrentes.

Para Marcelo Benacchio (2015, p. 210), “a relação de causalidade se mostra presente quando positivo o julgamento posterior de probabilidade de que aquele comportamento decorreu determinado dano”.

A verificação do nexo causal deve considerar as particularidades de cada caso concreto; no entanto, não se configura como um ponto controverso, visto que os danos típicos decorrentes do *cyberstalking* são, em regra, consequências diretas e apropriadas das condutas perpetradas pelo perseguidor. Dessa forma, há uma relação clara entre o comportamento abusivo e os prejuízos sofridos pela vítima.

Visando a análise dos três elementos estruturantes que configuram a responsabilidade civil no contexto do *cyberstalking*, os quais são a existência do ato ilícito, o dano sofrido pela vítima e o nexo causal que vincula diretamente a conduta lesiva ao resultado danoso torna-se fundamental direcionar o foco para o sistema de imputação mais adequado a ser aplicado nessas situações.

Esse aspecto é relevante porque influencia a forma de atribuição da responsabilidade ao agente e o grau de exigência na comprovação da culpa ou das

provas necessárias. O sistema de imputação adotado afeta a dinâmica do processo judicial e as possibilidades de tutela à vítima, determinando se será preciso demonstrar intenção ou negligência do agente ou se basta a ocorrência do dano em uma atividade de risco.

Dessa maneira, a aplicação correta desses selecionados revela-se essencial para garantir a justiça material e o equilíbrio na proteção dos direitos fundamentais no ambiente digital, configurando-se como um pilar para a efetividade da responsabilização civil frente às novas modalidades de violação, como o *cyberstalking*.

Embora as hipóteses de responsabilidade objetiva tenham ganhado espaço no ordenamento jurídico brasileiro, a regra geral continua a ser a responsabilização fundamentada na teoria da culpa. Conforme o parágrafo único do art. 927 do Código Civil, a responsabilidade objetiva aplica-se apenas nas hipóteses previstas em lei ou quando a atividade envolvida apresenta risco aos direitos de terceiros:

Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem (Brasil, 2002, art. 927, Código Civil, redação dada pela Lei nº 10.406/2002).

O princípio “*neminem laedere*”, herança do direito romano, estabelece que os direitos da personalidade são invioláveis e não podem ser afrontados. Consequentemente esse princípio impõe a obrigação primordial de não causar danos a terceiros, sendo a responsabilidade civil a obrigação secundária que visa à reposição desses danos, o objetivo desse dever de indenização.

Embora alguns autores defendam a aplicação da teoria do risco a condutas digitais, tal abordagem não é adequada. A responsabilidade objetiva, que prescinde de culpa, aplica-se apenas em leis específicas, como o Código de Defesa do Consumidor e a Política Nacional do Meio Ambiente, sendo restrita a situações legalmente previstas.

A aplicação da teoria do risco, no entanto, está condicionada à existência de uma atividade de risco, conceito previsto no parágrafo único do art. 927 do Código Civil de 2002. Uma interpretação sistemática desse dispositivo revela que “atividade” se refere à prática habitual e organizada com especificidade econômica.

Segundo Melo (2018, p. 1.278), “aqui, não se tem em conta a conduta individual, isolada, mas sim a atividade como conduta reiterada, habitualmente exercida, organizada de forma profissional ou empresarial, para realizar fins econômicos”.

De maneira geral, o comportamento do *cyberstalker* é movido por interesses individuais ou pela própria satisfação pessoal, não podendo ser considerado uma conduta decorrente de atividade de risco. Mesmo em situações excepcionais em que exista algum tipo de vínculo profissional entre o perseguidor e a vítima, a própria prática de perseguição não se enquadra nas definições legais de atividade de risco.

Diante desses elementos, embora haja divergências na doutrina, revela-se mais adequado aplicar ao *cyberstalking* o modelo de responsabilização fundamentado na

teoria da culpa, exigindo a demonstração de intenção, dolo ou negligência para que haja a responsabilização civil do agente.

5.2 RESPONSABILIDADE CRIMINAL NO *CYBERSTALKING*

No Brasil, havia uma lacuna legislativa, pois não existia um tipo penal específico que criminalizasse as condutas de *cyberstalking*, mas o país, ainda que de forma tardia, acompanhou os exemplos internacionais: elaborou o artigo 147-A no Código Penal, por meio da Lei nº 14.132/2021, representando um avanço significativo na tipificação e no combate a essas práticas persecutórias.

Antes da existência de uma legislação específica no Brasil, as práticas de *cyberstalking* eram combatidas por meio da aplicação de outras normas jurídicas. Era aplicado principalmente o artigo 65 da Lei das Contravenções Penais como base em casos que envolviam intimidação da vítima; em outros, aplicavam crimes de constrangimento ilegal e até mesmo contra a honra objetiva e subjetiva.

O primeiro projeto de lei apresentado foi o PL nº 5.419/2009, que tratou especificamente do crime de perseguição, apresentado pelo Deputado Federal Capitão Assunção, em resposta à ausência de legislação específica e ao aumento expressivo de casos no país.

No entanto, esse projeto acabou sendo arquivado na Câmara dos Deputados. Posteriormente, outras propostas foram apresentadas para criminalizar as condutas de *cyberstalking*. Em 2019, foi apresentado o PL 1.369/2019, originado na Câmara dos Deputados e relatado pela Deputada Leila Barros, que, após parecer favorável, foi alterado para PL 1.369-A/2019. Esse projeto foi aprovado no Legislativo e, em 31 de maio de 2021, tornou-se lei após sanção presidencial, entrando em vigor oficialmente para tipificar essas práticas criminosas.

Sobre o artigo 147-A do Código Penal, introduzido pela Lei 14.132/21, Cunha (2022, p. 246) analisa a específica e os efeitos da tipificação:

A Lei 14.132/21 inseriu no Código Penal o art. 147-A, denominado “crime de perseguição”. Sua finalidade é a tutela da liberdade individual, abalada por condutas que constroem alguém a ponto de invadir severamente sua privacidade e de impedir sua livre determinação e o exercício de liberdades básicas.

O fato ilícito tratado no artigo em questão está inserido no Código Penal, no capítulo referente aos delitos contra a liberdade individual. Dessa forma, o bem jurídico protegido por esse crime é justamente a liberdade, abrangendo a proteção dos direitos à privacidade, à livre locomoção, à saúde mental e, de maneira geral, à integridade da vítima, conforme previsto na Constituição Federal. Assim busca resguardar o direito fundamental de viver em tranquilidade, livre de perturbações ou perseguições indesejadas.

O elemento subjetivo previsto no tipo penal é o dolo, independentemente da existência de uma determinada finalidade. Dessa forma, o tipo penal exige apenas a intenção consciente de perseguir alguém, não admitindo a modalidade culposa.

O *cyberstalking* configura-se como crime impróprio, pois não se restringe ao uso do computador, sendo este apenas um dos meios previstos no artigo 147-A do Código Penal para a perseguição. Além desse delito, o agente pode responder por outros crimes correlatos, como o art. 216-B, que trata da divulgação não autorizada de cenas íntimas (pornografia de vingança), e o art. 154-A, relativo à invasão de dispositivos eletrônicos, bem como por condutas de *doxxing*, caracterizadas pela exposição de dados ou imagens privadas com o intuito de prejudicar a vítima.

O Superior Tribunal de Justiça (STJ) tem desempenhado papel relevante na construção da jurisprudência sobre crimes digitais, reconhecendo que os delitos cometidos pela internet não apenas se equiparam aos crimes tradicionais, mas também apresentam particularidades que exigem medidas investigativas modernas e apropriadas, cujo aresto segue abaixo citado:

É plenamente válida a utilização de provas obtidas por meio de interceptações telemáticas autorizadas judicialmente, inclusive em crimes cibernéticos, especialmente quando a atuação do agente é realizada em redes sociais e aplicativos de mensagens, cuja natureza pública ou semipública justifica a persecução penal (Brasil, 2020. STJ – HC 598.051/SP, Rel. Min. Ribeiro Dantas, Quinta Turma, julgado em 27/10/2020, DJe 03/11/2020).

A jurisprudência referente à Lei Carolina Dieckmann demonstra a importância de combater a criminalidade digital e a necessidade de atualização contínua das práticas judiciais, garantindo a proteção efetiva dos direitos fundamentais dos cidadãos na era digital.

A pena para o crime de *cyberstalking*, prevista no art. 147-A do Código Penal, varia de seis meses a dois anos de reclusão, além de multa. Esse dispositivo também prevê fatores que podem agravar a pena, reforçando a proteção às vítimas diante dessa violência digital.

Em relação às circunstâncias que determinam o aumento das penas previstas, veja-se o que consta do §1º do Artigo 147-A, do Código Penal, segundo Nucci (2022, p. 251):

O § 1.º do art. 147-A do Código Penal contempla causas de aumento de pena (ou majorantes), em patamar fixo, metade, a serem utilizadas na terceira fase da dosimetria da pena. Impõe-se uma elevação fixa, no montante de metade, para as hipóteses previstas nos incisos I a III do § 1º.

Prevê causas específicas de aumento de pena, aplicáveis na terceira fase da dosimetria, como a idade da vítima, a prática do delito contra mulher por motivação de gênero, o concurso de duas ou mais pessoas e o uso de armas.

O crime de perseguição é caracterizado como um crime formal, de consumação antecipada ou de resultado cortado, possuindo conduta e resultado naturalístico. Sua consumação independe da ocorrência efetiva do dano à integridade física ou psicológica

da vítima; basta que o agente pratique a perseguição de forma reiterada, por qualquer meio, com potencial de ameaça, mesmo que os efeitos não se concretizem.

Por se tratar de crime habitual, em regra não se admite tentativa, todavia é possível demonstrar situações em que o início da execução ocorreu, mas a consumação não se concretizou por circunstâncias alheias à vontade do agente.

5.3 RESPONSABILIDADE INSTITUCIONAL E INVESTIGAÇÃO DO CYBERSTALKING

A persecução penal no Direito Penal Brasileiro inicia-se com a investigação criminal, uma fase pré-processual de grande relevância para apurar a materialidade e a autoria do delito, buscando aproximar-se da verdade real dos fatos e identificar o agente causador do dano. Em relação ao conceito de inquérito policial, o doutrinador Távora (2013, p. 98) assim se expressa:

O inquérito policial vem a ser o procedimento administrativo, preliminar, presidido pelo delegado de polícia, no intuito de identificar o autor do ilícito e os elementos que atestem a sua materialidade (existência), contribuindo para a formação da opinião delitiva do titular da ação penal, ou seja, fornecendo elementos para convencer o titular da ação penal se o processo deve ou não ser deflagrado.

A investigação criminal tem início com a *notitia criminis*, momento em que a vítima informa o delito à autoridade competente, para dar início à persecução penal. O inquérito policial, enquanto procedimento administrativo investigatório conduzido, em regra, pela polícia judiciária, visa coletar informações sobre a materialidade e a autoria do fato delituoso, fornecendo elementos para que o titular da ação penal decida sobre o prosseguimento do processo.

No contexto do crime de *cyberstalking*, a responsabilidade institucional para processar e julgar é estritamente delimitada pelas normas constitucionais e processuais penais, refletindo a competência de cada esfera do Poder Judiciário e das autoridades investigativas.

A competência jurisdicional é o poder-dever do Estado-juiz de aplicar o direito ao caso concreto; assim, a competência define a área de atuação do juiz, sendo categorizada em três espécies principais, conforme o art.69 do Código de Processo Penal (CPP): em razão da matéria (*ratione materiae*), da pessoa (*ratione personae*) e do lugar (*ratione loci*).

A competência em razão da matéria (*ratione materiae*) refere-se à natureza do crime objeto da ação penal, conforme os art.69, inciso III, e 74 do CPP. Exemplos incluem a competência do Tribunal do Júri para crimes dolosos contra a vida e dos Juizados Especiais Criminais (JECrim) para infrações de menor potencial ofensivo.

Já a competência em razão da pessoa (*ratione personae*) está relacionada ao foro por prerrogativa de função, previsto nos art.69, inciso VII, e 84 a 87 do CPP. Nesse caso, autoridades com cargos de relevância pública, como o Presidente da República, têm seus

processos julgados pelo Supremo Tribunal Federal, enquanto prefeitos são julgados pelo Tribunal de Justiça da respectiva comarca.

Por fim, a competência em razão do lugar (*ratione loci*), estabelecida pelos artigos 69, inciso I, 70 e 71 do CPP, determina o foro competente com base no local da consumação da infração ou do último ato de execução, conforme disposto no artigo 70: “A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução”.

O ordenamento jurídico brasileiro adota a Teoria da Ubiquidade para definir o local do crime, conforme o art. 6º do Código Penal: “Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir o resultado”. Essa teoria é especialmente relevante para crimes cibernéticos, como o *cyberstalking*, devido à natureza transnacional da internet, que permite a prática delitiva a partir de qualquer lugar do mundo, utilizando dispositivos como computadores, celulares e tablets.

A competência para processar e julgar o *cyberstalking* é majoritariamente da justiça estadual, por se tratar de infrações de âmbito local, salvo quando o delito envolve bens jurídicos tutelados pela União ou apresenta caráter transnacional, casos em que passa à Justiça Federal, nos termos do art. 109, inciso IX, da CF, combinado com o art. 88 do CPP. A investigação criminal é conduzida pela Polícia Civil nos casos de competência estadual ou pela Polícia Federal quando o crime ultrapassa fronteiras estaduais ou internacionais, conforme reforçado pela Lei nº 14.155/2021, que introduziu agravantes para crimes cibernéticos no Código Penal.

Nos crimes cibernéticos, definir o foro competente é desafiador, pois o delito pode ser praticado remotamente, dificultando a identificação do local da consumação. Para crimes tentados ou consumados no Brasil, a jurisprudência dos tribunais superiores, com base no art. 70 do CPP, estabelece que o foro é o local da consumação, como o domicílio do provedor de internet em casos estaduais que não afetem bens da União. Nos crimes internacionais, que se iniciam no Brasil e se propagam no exterior ou atingem bens da União, a competência é da Justiça Federal.

A falta de legislação específica para crimes cibernéticos, dado que o Código Penal é de 1940, faz da jurisprudência dos tribunais superiores um guia fundamental para definir a competência. Assim, normas do CP e do CPP vêm sendo adaptadas às peculiaridades dos delitos virtuais, garantindo a persecução penal. A divisão de atribuições entre Justiça Estadual, Federal, Polícia Civil e Polícia Federal assegura a efetividade da investigação e do julgamento do *cyberstalking*, dentro dos limites legais e constitucionais.

5.4 PREVENÇÃO E COMBATE AO CYBERSTALKING

A prevenção e o combate ao *cyberstalking* exigem uma abordagem integrada que proteja a vítima e enfrente o agressor, garantindo a privacidade das vítimas durante investigações e processos judiciais, de forma que a coleta de evidências não exponha indivíduos fragilizados. Medidas de segurança digital, como o uso de senhas robustas, configuração adequada de privacidade em redes sociais e cautela no compartilhamento

de informações pessoais, contribuem para reduzir a vulnerabilidade das possíveis vítimas.

A prevenção eficaz exige compreender as motivações dos agressores e as formas de vitimização, considerando fatores sociais, estereótipos de gênero, exclusão e desigualdades de poder que incentivam abusos online, como assédio, racismo, homofobia e *bullying*. Políticas públicas, programas educativos e campanhas de conscientização digital são essenciais para orientar os usuários e estabelecer limites claros nas interações virtuais.

Além disso, a atuação coordenada entre sistema jurídico, órgãos de segurança, sociedade civil e plataformas digitais é essencial para responsabilizar agressores, proteger vítimas e criar um ambiente virtual mais seguro.

Serviços de apoio, como centros especializados, linhas diretas e redes de suporte emocional, fortalecem o acolhimento e incentivam a denúncia. Medidas legais, tecnológicas, educativas e psicológicas integradas constituem a base para prevenir o *cyberstalking* e mitigar seus impactos, promovendo segurança, dignidade e respeito no espaço digital.

6 CONCLUSÃO

O estudo demonstrou que o avanço das tecnologias digitais, embora facilite a comunicação, também criou um ambiente propício à perseguição virtual, potencializada pelo anonimato e pela exposição em redes sociais, com graves impactos psicológicos, sociais e emocionais. Constatou-se que, apesar da evolução legislativa com o art. 147-A do Código Penal (Lei nº 14.132/2021) e o agravamento de crimes cibernéticos pela Lei nº 14.155/2021, ainda persistem desafios para responsabilizar eficazmente os agressores.

Entre as lacunas normativas, destaca-se a ausência de regras específicas para preservação de provas digitais, como registros de *login*, fundamentais em crimes como o *cyberstalking* e a invasão de dispositivos (art. 154-A, CP). Além disso, normas como a Lei Maria da Penha (Lei nº 11.340/2006), a Lei nº 13.772/2018 e o art. 7º, II, da CF/88 carecem de integração clara ao ambiente virtual, enquanto a responsabilidade civil prevista nos arts. 186 e 927 do Código Civil enfrenta entraves na quantificação de danos imateriais online.

A Lei nº 14.155/2021 ampliou penas, mas não definiu protocolos detalhados para a colaboração de provedores, o que se agrava pela dimensão transnacional da internet.

Ferramentas de anonimato (VPNs) e a volatilidade dos dados dificultam a aplicação da Teoria da Ubiquidade (art. 6º, CP) e exigem modernização das investigações. O inquérito policial, definido por Távora (2013, p. 98) como “procedimento administrativo, preliminar, presidido pelo delegado de polícia, no intuito de identificar o autor do ilícito e os elementos que atestem a sua materialidade”, é conduzido pela Polícia Civil em casos locais ou pela Polícia Federal em crimes transnacionais (art. 109, CF/1988; art. 88, CPP), observando-se a competência definida no art. 69 do CPP e nos arts. 84 a 87 sobre prerrogativas de função.

A eficácia, contudo, é limitada pela falta de capacitação em perícias digitais e pela ausência de normas sobre cooperação internacional, como a adesão à Convenção de

Budapeste. Para superar esses obstáculos, propõe-se: (i) criação de legislação específica para preservação de provas digitais, alinhada à Lei nº 14.155/2021; (ii) capacitação de policiais e peritos em análise forense; (iii) adesão a tratados internacionais para troca de informações; (iv) regulamentação da responsabilidade de plataformas digitais conforme o Marco Civil da Internet (Lei nº 12.965/2014); (v) ampliação da aplicação da Lei Maria da Penha e do art. 216-B do CP para casos de *cyberstalking* com violência de gênero; e (vi) promoção de campanhas educativas sobre segurança digital.

Conclui-se que a adaptação do sistema jurídico brasileiro ao *cyberstalking* exige integração normativa, uso de tecnologia avançada e medidas preventivas. A proteção dos direitos fundamentais e a responsabilização eficaz dos agressores dependem da combinação entre legislação, tecnologia e responsabilidade social, garantindo um ambiente virtual mais seguro e protetivo da dignidade humana.

REFERÊNCIAS

ALMEIDA DA SILVA, Mariana. A internet como ambiente facilitador à violência de gênero: cyberstalking, sextorsão e revenge porn. **Revista do Ministério Público do Estado do Rio de Janeiro**, n. 86, p. 109-122, 2022.

AMILKY, Luciana Gerbovic. **Stalking**. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2014.

BENACCHIO, Marcelo. Algumas considerações acerca da relação de causalidade na responsabilidade civil. In: GUERRA, Alexandre Dartanhan de Mello; BENACCHIO, Marcelo (Coords.). **Responsabilidade civil**. São Paulo: Escola Paulista de Magistratura, 2015.

BRASIL. Código Penal. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Alterado pela Lei nº 14.155, de 27 de maio de 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Diário Oficial da União, Brasília, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

BRASIL. Decreto-Lei n. 3.689, de 3 de outubro de 1941. Código de Processo Penal. **Diário Oficial da União**, Rio de Janeiro, 4 out. 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm.

BRASIL. Lei n. 10.406, de 10 de janeiro de 2002. Código Civil. **Diário Oficial da União**, Brasília, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm.

BRASIL. **Lei nº 11.340, de 7 de agosto de 2006.** Cria mecanismos para coibir a violência doméstica e familiar contra a mulher. Alterada pela Lei nº 13.772, de 19 de dezembro de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/111340.htm.

BRASIL. **Superior Tribunal de Justiça. Habeas Corpus nº 598.886/SC.** Relator: Min. Rogério Schietti Cruz. Julgado em 27 out. 2020. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/897212872/habeas-corpus-n-598886-sc>.

BRITO, Edilayne Silva de. **Cyberstalking:** uma análise do crime de perseguição contra mulheres na internet, sob o olhar do art. 147-A, CP inserido pela nova Lei 14.132/2021. Mossoró: UERN, 2021.

CENTRO UNIVERSITÁRIO DE PATOS DE MINAS. **Manual para normalização de trabalhos acadêmicos.** 6. ed. rev. ampl. Patos de Minas: FEPAM, 2025.

CUNHA, Rogério S. **Manual de direito penal:** parte especial (arts. 121 ao 361). 15. ed. rev., atual. e ampl. São Paulo: JusPODIVM, 2022.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário Brasileiro de Segurança Pública 2024:** *stalking* contra mulheres cresce 34,5% no Brasil em 2023. São Paulo: FBSP, 2024. Disponível em: <https://forumseguranca.org.br/wp-content/uploads/2024/07/anuario-2024.pdf>.

MELO, Diogo Leonardo Machado de. Responsabilidade civil. In: NANNI, Giovanni Ettore (Coord.). **Comentários ao Código Civil:** direito privado contemporâneo. São Paulo: Saraiva, 2018.

MOTA, Carlos Henrique de Espíndola. **Cyberstalking:** a necessidade de tipificação no Direito Penal Brasileiro. Recife: Faculdade Damas da Instrução Cristã, 2020.

MORAES, Maria Celina Bodin de. **Danos à pessoa humana:** uma leitura civil-constitucional dos danos morais. Rio de Janeiro: Renovar, 2007.

NETO, Luísa. Informação e liberdade de expressão na internet e violação de direitos fundamentais: um conflito de (im)possível resolução. In: PROCURADORIA-GERAL DA REPÚBLICA DE PORTUGAL. **Informação e liberdade de expressão na Internet e a violação de direitos fundamentais:** comentários em meios de comunicação online. Lisboa: Imprensa Nacional Casa da Moeda, 2014.

NUCCI, Guilherme S. **Curso de direito penal:** parte especial arts. 121 a 212 do código penal. 6. ed. Rio de Janeiro: Forense, 2022.

O PEROBAL – UEL. **Estudo identifica perfis recorrentes envolvidos em casos de cyberbullying.** 17 jan. 2024. Disponível em: <https://www.uel.br>.

PAESANI, Liliana Minardi. **Direito e Internet**: liberdade de informação, privacidade e responsabilidade civil. 4. ed. São Paulo: Atlas, 2008.

PSYMEET SOCIAL. **A psicologia do cyberbullying**. 6 mar. 2023. Disponível em: <https://www.psymeetsocial.com/blog/artigos/a-psicologia-do-cyberbullying>.

REVISTA FT. **Violência doméstica e o novo crime de cyberstalking**. 11 jun. 2024. Disponível em: <https://www.revistaf.com.br>. Acesso em: 22 ago. 2025.

SILVA, Isabella Moura da *et al.* **O crime de cyberstalking no ordenamento jurídico penal brasileiro**. UniSALESIANO, 2021.

SILVA, Jair Ilídio da. Stalking e *cyberstalking*: uma violação à privacidade e à intimidade. In: PINTO, Fernanda Miler Lima (org.). **Reflexões sobre Direito e sociedade**: fundamentos e práticas. Ponta Grossa: Aya, 2023. v. 7, p. 41-49.

SILVA, Júlia de Oliveira. **A inserção do crime de stalking no Código Penal Brasileiro**: do procedimento adotado em face à Lei nº 14.132/2021. Goiânia: PUC Goiás, 2022.

SIMAS, Diana Viveiros de. **O cibercrime**. Lisboa: Universidade Lusófona de Humanidades e Tecnologias, 2014.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal**: de acordo com a Lei nº 12.760/2012 que aumentou o rigor da “Lei Seca”. 8. ed. Bahia: JusPodvm, 2013.

WERMUTH, Maiquel Ângelo Dezordi; CALLEGARI, André Luís. *Stalking e cyberstalking*: considerações críticas sobre o delito tipificado no art. 147-A do Código Penal brasileiro. **Revista Brasileira de Ciências Criminais**, v. 186, p. 105-126, dez. 2021.