CRIMES CIBERNÉTICOS E OS DESAFIOS LEGAIS PARA A PROTEÇÃO DO *STALKING*

Kawany G. Fernandes[1] (Unisecal)
Carlos A. N. Gross[2] (Unisecal)

Resumo: O presente artigo, analisa o fenômeno do *stalking* cibernético e os desafios enfrentados pelo ordenamento jurídico brasileiro na proteção das vítimas dessa prática. Com o avanço das tecnologias e a intensificação do uso das redes sociais, novas formas de perseguição surgiram, muitas vezes dificultando a identificação do agressor e a responsabilização penal. A pesquisa explora a caracterização do *cyberstalking*, os principais obstáculos legais e institucionais para seu enfrentamento, e propõe reflexões sobre a necessidade de políticas públicas, educação digital e atualização legislativa. Conclui-se que o combate eficaz ao *stalking* virtual exige uma abordagem multidisciplinar, com integração entre Direito, tecnologia e sociedade.

Palavras-chave: crimes cibernéticos, *stalking* digital, legislação, proteção de dados, desafios legais.

CYBERCRIMES AND LEGAL CHALLENGES FOR PROTECTION AGAINST STALKING

Abstract: This article, which is a final project for the course, analyzes the phenomenon of *cyberstalking* and the challenges faced by the Brazilian legal system in protecting victims of this practice. With the advancement of technology and the increased use of social media, new forms of *stalking* have emerged, often making it difficult to identify the aggressor and hold him or her criminally liable. The research explores the characterization of *cyberstalking*, the main legal and institutional obstacles to combating it, and proposes reflections on the need for public policies, digital education, and legislative updates. It is concluded that effectively combating *cyberstalking* requires a multidisciplinary approach, with integration between law, technology, and society.

***Keywords**: cybercrimes, cyberstalking, legislation, data protection, legal challenges.*

1 INTRODUÇÃO

Com o avanço acelerado das tecnologias digitais e a expansão do uso da internet, surgem novos desafios jurídicos relacionados à proteção da privacidade e da integridade dos indivíduos no ambiente virtual. Dentre os diversos delitos que se adaptaram ao ciberespaço, destaca-se o *stalking* digital, uma prática persistente de

1 Acadêmica do 9º período do curso de Bacharelado em Direito pelo Centro Universitário Santa Amélia (Unisecal). E-mail: kawanygfernandes@gmail.com
2 Orientador. Mestre em Ciências Sociais Aplicadas pela Universidade Estadual de Ponta Grossa – UEPG. Bacharel em Direito pela Universidade Estadual de Ponta Grossa – UEPG. Professor do curso de Bacharelado em Direito no Centro Universitário Santa Amélia (Unisecal).

perseguição, vigilância e assédio realizada por meios eletrônicos, que causa temor, instabilidade emocional e violação da intimidade das vítimas.

Este artigo tem como objetivo analisar a crescente relevância dos crimes cibernéticos, com ênfase no *stalking* digital, destacando sua evolução no contexto jurídico-penal e os impactos diretos sobre os direitos fundamentais, especialmente no que diz respeito à privacidade, liberdade individual e segurança pessoal. Apesar dos avanços legislativos, como a inclusão do art. 147-A no Código Penal, ainda se observam lacunas significativas nas políticas públicas e nos mecanismos jurídicos existentes, que se mostram, por vezes, ineficazes para conter ou punir de forma adequada esse tipo de violência.

A escolha do tema surgiu a partir da experiência adquirida durante o estágio na 13.ª Delegacia de Polícia de Ponta Grossa, onde foi possível constatar a recorrência de casos envolvendo perseguição virtual, revelando a urgência de uma abordagem mais eficaz e sensível por parte do sistema de justiça criminal

A presente pesquisa é instigada pela necessidade de reflexão crítica sobre a efetividade dos instrumentos legais atuais e a responsabilização penal do agente perseguidor, frente a um cenário cada vez mais digitalizado. Para isso, serão abordadas não apenas as previsões legislativas, mas também os obstáculos práticos enfrentados pelas vítimas, a atuação do Estado e a necessidade de construção de estratégias de prevenção e repressão mais eficazes.

Dessa forma, a problemática central que orienta este estudo consiste em responder: Quais medidas podem ser implantadas em relação ao crime de *stalking* para uma responsabilização efetiva do agressor e maior proteção das vítimas no ambiente digital?

2 CRIMES CIBERNÉTICOS: CONCEITOS E CLASSIFICAÇÃO

Os crimes cibernéticos são todos e quaisquer crimes que geralmente se dão de forma virtual, referindo-se a atividades ilícitas que se utilizam da tecnologia digital como meio ou como alvo. Com o avanço da sociedade, o meio tecnológico, de certa forma, se tornou mais hábil e comum para a prática dos crimes. Nessa senda, crimes cibernéticos “[...] são aqueles que podem ser praticados da forma tradicional ou por intermédio de computadores, ou seja, o computador é apenas um meio para a prática

do crime, que também poderia ser cometido sem o uso dele" (WENDT; JORGE, 2013, p.19).

Tais crimes cresceram exponencialmente com o aumento do uso da internet e das redes sociais, afetando principalmente a segurança de dados pessoais e envolvendo ataques a sistemas informáticos, redes e dispositivos, prejudicando diretamente a sociedade.

> A evolução operada nas novas tecnologias, projetou-se sobre o fenômeno criminal, pois se atendermos às suas duas vertentes, por um lado, a tecnologia poder, ela mesma, objeto de prática de crimes e por outro lado, suscita e potência novas formas criminais ou novas formas de práticas antigos crimes (SIMAS, 2014, p. 14)

A internet desempenha um papel significativo na sociedade, em todo tipo de relação, seja ela comercial, cultural ou social, e, com a crescente dependência da sociedade em relação à tecnologia da informação, os crimes cibernéticos têm se tornado um fenômeno cada vez mais comum e global, sendo utilizados por criminosos para violar direitos fundamentais.

Quando falamos sobre crimes cibernéticos, é importante entender que eles se dividem em duas categorias principais. Como explicam Jesus e Milagre (2016, p. 49), existem os chamados crimes informáticos próprios e os impróprios. Os crimes cibernéticos próprios são aqueles que só podem ser cometidos no ambiente virtual, ou seja, o bem jurídico atingido é justamente a tecnologia da informação. Um ponto interessante que os autores destacam é que, nesses casos, a legislação penal tradicional muitas vezes se mostra insuficiente, já que certas condutas simplesmente não estavam previstas na lei.

Já os crimes informáticos impróprios são caracterizados pelo fato de a internet funcionar apenas como um meio para a prática do crime, mas o bem jurídico protegido já existe no Código Penal. Um exemplo clássico é o acesso indevido a uma conta bancária. Nesse tipo de situação, como os autores pontuam, a legislação penal brasileira já oferece os mecanismos necessários para punir esse tipo de conduta, pois ela se encaixa em tipos penais já existentes.

Essa diferenciação evidencia a necessidade de constante adaptação da legislação vigente, referente aos avanços tecnológicos, de modo a garantir a repressão dos crimes cibernéticos.

O avanço da tecnologia e o acesso facilitado à internet trouxeram inúmeros benefícios à sociedade, mas também impulsionaram o crescimento de crimes cibernéticos, entre eles o *cyberstalking*.

O *cyberstalking* se caracteriza pela perseguição reiterada por meio digital, causando danos emocionais, psicológicos e, em alguns casos, físicos, à vítima. Segundo Valério de Oliveira Mazzuoli (2021), o *stalking* virtual intensifica os impactos do crime, pois o agressor pode se valer do anonimato e do amplo alcance das redes sociais para monitorar, ameaçar e intimidar a vítima de forma constante.

O crime de *stalking* foi incluído no Código Penal em seu novo artigo 147-A, por meio da Lei nº 14.132/2021. Entretanto, quando praticado no ambiente digital, pode estar associado a outros crimes cibernéticos previstos na legislação brasileira. Um deles é a invasão de dispositivos informáticos, prevista no artigo 154-A do Código Penal pela Lei Carolina Dieckmann (Lei nº 12.737/2012). Nessa prática, o agressor acessa indevidamente e-mails, redes sociais ou até mesmo câmeras da vítima para obter informações privadas e utilizá-las para controle, chantagem ou exposição pública.

Outro crime frequentemente relacionado ao *cyberstalking* é a divulgação não autorizada de imagens íntimas, prevista no artigo 218-C do Código Penal. Conhecido popularmente como *revenge porn*, esse crime ocorre quando o agressor expõe ou compartilha fotos e vídeos íntimos da vítima sem consentimento, com o objetivo de humilhá-la ou exercer poder sobre ela.

Além disso, há casos em que os *cyberstalkers* utilizam perfis falsos para perseguir, difamar ou enganar a vítima, configurando o crime de falsa identidade, tipificado no artigo 307 do Código Penal. Essas contas fictícias podem ser usadas para assediar a vítima, difamar sua reputação ou induzir terceiros a cometerem novos atos contra ela.

Mensagens ameaçadoras também são comuns no contexto do *cyberstalking*, podendo ser enquadradas nos crimes de ameaça (artigo 147 do Código Penal) e coação (artigo 146 do Código Penal). O agressor pode enviar e-mails, mensagens em redes sociais ou utilizar aplicativos para intimidar a vítima e fazê-la ceder às suas exigências. Nesse sentido:

> (…) Além da exposição e constrangimento sofridos quando da divulgação de sua imagem, os danos à honra sofridos são imperiosamente maiores que aqueles sofridos pelos homens, pois o olhar cultural da sociedade tende a

> culpar a vítima que compartilha suas imagens, protegendo o agressor e impedindo a sua punição (CAVALCANTI, 2016, s/p).

Por fim, outra prática amplamente utilizada pelos *cyberstalkers* é o *doxxing*, que consiste na “divulgação pública intencional na Internet de informações pessoais sobre um indivíduo por terceiros” (DOUGLAS, 2016, p. 199). Essa prática incentiva o assédio por parte de terceiros e pode ser analisada à luz da Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), que protege a privacidade dos indivíduos no ambiente digital.

O *cyberstalking* representa uma nova forma de assédio que demanda uma atualização contínua das leis para assegurar a proteção dos afetados. Com o aumento das interações online, é fundamental reforçar as legislações e as diretrizes de segurança na web para prevenir esse tipo de comportamento e penalizar os culpados.

3 O *STALKING* E SUAS IMPLICAÇÕES LEGAIS

A palavra *Stalking* vem de origem inglesa e pode ser traduzida como "vigiar, espiar, ficar à espreita". É uma forma de violência psicológica que causa sérios danos à saúde emocional e mental da pessoa atingida. A prática envolve táticas como mensagens incessantes, ligações e até o aparecimento inesperado da pessoa em locais estratégicos, tudo com o intuito de controlar e intimidar. Nesse sentido:

> [...] Os efeitos potenciais de *stalking* atingem a saúde mental e emocional da vítima infligindo lhe uma negação ou dúvida, ou seja, a vítima não acredita o que lhe está acontecendo. Em seguida, ao perceber a gravidade do fato, a vítima é tomada de uma frustração, culpa, vergonha, baixa autoestima, insegurança, choque e confusão, irritabilidade, medo e ansiedade, depressão, raiva, isolamento, perda de interesse. (ADEMIR DA VEIGA, 2011, P.2)

Embora a legislação brasileira esteja avançando, com a tipificação do crime de *stalking*, ainda é necessário aprimorar os instrumentos legais e as políticas públicas para garantir a proteção efetiva das vítimas. A implementação de medidas protetivas e o oferecimento de suporte psicológico são essenciais, tanto para a punição do agressor quanto para o amparo à vítima. Dessa forma, é crucial que o sistema legal esteja cada vez mais capacitado para lidar com o *stalking* de maneira eficaz, proporcionando segurança e recuperação emocional para quem sofre com essa violência.

O *stalking* é definido como a perseguição reiterada que ameaça a integridade psicológica, emocional ou física da vítima, restringindo sua liberdade ou causando temor. No Brasil, essa conduta foi tipificada pelo artigo 147-A do Código Penal, introduzido pela Lei nº 14.132/2021. Segundo a norma:

> Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a
> integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de
> qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade.
> Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.
> § 1º A pena é aumentada de metade se o crime é cometido:
> I – contra criança, adolescente ou idoso;
> II – contra mulher por razões da condição de sexo feminino, nos termos do § 2º-A do
> art. 121 deste Código;
> III – mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma.
> § 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes à violência.
> § 3º Somente se procede mediante representação. (BRASIL, 2021)

A pena prevista é de reclusão de seis meses a dois anos e multa, podendo ser aumentada caso o crime seja cometido contra mulheres, crianças, idosos ou pessoas com deficiência.

De acordo com Valério de Oliveira Mazzuoli (2021), o *stalking* se diferencia do assédio moral ou da ameaça isolada por sua continuidade e pelo impacto psicológico duradouro que causa à vítima. O autor destaca que, no ambiente digital, o *cyberstalking* amplia o alcance da perseguição, tornando a vítima vulnerável a ataques constantes, mesmo em sua vida privada.

O Supremo Tribunal Federal (STF, 2021) e o Superior Tribunal de Justiça (STJ, 2021) têm reconhecido a gravidade do *stalking,* especialmente quando praticado em contexto de violência de gênero. Em diversos julgados, os tribunais ressaltam que a perseguição reiterada pode configurar violência psicológica contra a mulher, conforme previsto no art. 7º, inciso II da Lei Maria da Penha (Lei nº 11.340/2006).

4. COLETA DE PROVAS NO *STALKING*

A reunião de evidências no delito de *stalking* é essencial para identificar a repetição das ações de perseguição e para a responsabilização do infrator. Dado que frequentemente esses atos ocorrem no ambiente digital, a documentação se torna

uma peça-chave nesse processo, especialmente para fins de responsabilização do agressor.

Conforme ensina Greco (2023), a prova no *stalking* pode ser dividida em três categorias principais:

4.1. PROVAS DIGITAIS

- Capturas de tela de mensagens, e-mails, comentários em redes sociais e ligações;
- Registros de conversas em aplicativos de mensagens, como WhatsApp e Telegram;
- Mensagens eletrônicas recebidas contendo ameaças ou informações intrusivas;
- Gravação ambiental clandestina utilizada para proteção dos direitos da vítima.

4.2. PROVAS TESTEMUNHAIS E INFORMANTES

- Relatos de amigos, parentes ou companheiros de trabalho que tenham observado a situação de assédio.
- Relatos de terceiros que tenham sido contatados pelo agressor na tentativa de atingir a vítima.

4.3. PROVAS TÉCNICAS E PERICIAIS

- Laudos de perícia digital para verificar a autenticidade das mensagens e identificar o autor dos atos;
- Registros de endereços IP e monitoramento dos aparelhos utilizados pelo ofensor.
- Laudos psicológicos que comprovem os impactos emocionais resultantes do assédio.
- crimes cibernéticos, *stalking* digital, legislação, proteção de dados, políticas públicas.

A ausência de provas pode comprometer todo o processo, uma vez que o sistema penal exige a demonstração clara da materialidade e da autoria do fato para a aplicação da punição. Por isso, é essencial que a vítima seja orientada, desde o início, a preservar mensagens, registrar *prints*, salvar áudios e manter o histórico das

interações. Mesmo que a vítima não tenha certeza se está sendo perseguida, qualquer elemento guardado pode futuramente servir de apoio à investigação.

Além disso, as provas não servem apenas para responsabilizar o agressor, mas também são fundamentais para a concessão de medidas protetivas urgentes. Quando a vítima apresenta evidências do comportamento ameaçador, o juiz pode agir com mais segurança ao determinar o afastamento do perseguidor ou a proibição de contato. Ou seja, as provas têm um efeito prático e direto na segurança da pessoa que sofre o crime.

Outro ponto fundamental é que, no caso do *stalking*, não basta provar uma ação isolada. É necessário demonstrar a repetição e a continuidade da conduta. Por isso, cada captura de tela, cada áudio e cada testemunho ganha um peso especial na hora de formar um conjunto probatório consistente. Muitas vezes, uma única captura de tela pode parecer irrelevante, mas, quando analisado junto com outras provas, mostra o padrão de perseguição.

Por fim, vale lembrar que o uso de provas digitais no processo penal exige cuidados técnicos. Para garantir sua validade, é importante que elas sejam preservadas de maneira íntegra e, sempre que possível, acompanhadas de metadados, endereços de IP ou laudos que atestem sua autenticidade.

Metadados são dados sobre dados, isto é, informações acerca de determinado dado existente no mundo digital, como quando, onde e por quem foi criado, por exemplo, enquanto o endereço de IP permite identificar, por exemplo, de qual máquina se originou determinada mensagem (POSTEL, 1981; GONZALEZ-PEREZ, 2025). A atuação de peritos e especialistas em tecnologia da informação se torna essencial nesse momento, já que pode evitar a alegação de provas adulteradas ou inválidas.

Portanto, em casos de *stalking*, especialmente no ambiente online, a prova não é apenas um detalhe do processo ela é a base sobre a qual se constrói toda a proteção da vítima e a responsabilização do agressor. Sua correta coleta, preservação e apresentação pode ser o diferencial entre a impunidade e a justiça.

O STJ já decidiu, no HC 598.051/SP, que, em casos de crimes cibernéticos, a coleta de provas deve ser conduzida com rigor técnico, garantindo a autenticidade e a integridade dos registros digitais (STJ, 2020). A vítima deve reunir todas as

evidências possíveis antes de denunciar, pois a falta de provas pode dificultar a responsabilização do agressor.

A Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) também pode ser utilizada para solicitar a remoção de conteúdos ofensivos publicados sem consentimento, além de ajudar na identificação do perseguidor por meio do compartilhamento de dados com autoridades.

Além de tudo isso, é importante lembrar que a sociedade também tem um papel fundamental no combate ao *stalking.* Ainda falta informação sobre o assunto, o que faz com que muitas vítimas não saibam como agir ou tenham medo de denunciar. Por isso, é essencial que existam mais campanhas de conscientização, principalmente em escolas, faculdades e nas redes sociais, para que as pessoas entendam o que é *stalking* e saibam como buscar ajuda. Outro ponto importante é o preparo dos profissionais que lidam com esse tipo de situação, como psicólogos, policiais, advogados e outros, para que estejam prontos para acolher a vítima e lidar com o caso da melhor forma possível. É necessário que todas as áreas, segurança, justiça e saúde, trabalhem juntas para garantir não só a punição do agressor, mas também o cuidado com quem sofreu essa violência. Dessa forma, estudar o *stalking* vai além da parte jurídica e envolve também ações sociais e educativas que ajudam a prevenir e enfrentar esse crime.

5 A LEGISLAÇÃO BRASILEIRA SOBRE CRIMES CIBERNÉTICOS

A legislação brasileira referente a delitos cibernéticos está em fase de transformação, mas já conta com relevantes ferramentas jurídicas voltadas para a repressão de atividades ilegais no ambiente digital. Conforme afirmam Almeida e Oliveira (2022, p.4):

> A Lei nº 12.737/2012 –Lei dos Crimes Cibernéticos, ou, também conhecida como, a Lei “Caroline Dieckmann”, trouxe importantes alterações ao Decreto-Lei 2.848/40 –Código Penal brasileiro, ao passo que realizou a formalização e a tipificação de condutas delituosas no âmbito informático, constituindo os chamados “crimes cibernéticos.

Esta legislação pune a invasão de dispositivos, incluindo celulares, computadores e outras plataformas digitais, com vistas a acessar, alterar ou eliminar informações sem o consentimento do proprietário. Esse fato representa um progresso

na norma jurídica, em resposta ao aumento de delitos ocorrendo no espaço digital, como o furto de dados pessoais, fraudes e ataques virtuais.

A Lei nº 13.709/2018, que instituiu a Lei Geral de Proteção de Dados Pessoais (LGPD), também tem relevância, uma vez que assegura a privacidade dos dados pessoais e estabelece penalidades para o uso indevido de informações na internet. Embora a LGPD tenha um foco principal na proteção de dados, ela também contribui indiretamente para o combate a crimes cibernéticos ao estabelecer diretrizes rígidas para a coleta, tratamento e armazenamento de informações pessoais na rede.

Contudo, existe uma lacuna na capacitação técnica de agentes públicos para lidar com crimes virtuais. Muitos delegados, investigadores e peritos ainda não possuem formação especializada para coletar e analisar provas digitais, o que pode comprometer a eficácia das investigações. O mesmo acontece no Judiciário, onde muitos magistrados enfrentam dificuldade em compreender a dinâmica dos crimes cibernéticos e o funcionamento dos meios digitais utilizados para sua prática.

Por isso, cresce a importância da atuação de núcleos especializados em crimes cibernéticos nas polícias civis e nos Ministérios Públicos dos estados. Esses núcleos contam com profissionais treinados e ferramentas próprias para rastrear IPs, recuperar dados e identificar autores de delitos digitais, contribuindo para que a justiça seja mais ágil e eficaz nesse tipo de situação.

O Ministério Público do Rio Grande do Norte, por exemplo, iniciou um curso de capacitação em investigação cibernética para delegados e agentes da Polícia Civil potiguar. A promotora de Justiça Engrácia Monteiro destacou que "tornou-se imperativo os agentes da lei conhecerem as técnicas para identificação, preservação e coleta de provas no ciberespaço" (MPRN, 2023).

Igualmente relevante é o papel das plataformas digitais, como redes sociais e serviços de mensagens, na identificação e remoção de conteúdos criminosos. Embora já exista uma cooperação com autoridades em casos de crimes graves, muitas empresas ainda se recusam a fornecer dados ou dificultam o processo ao alegar proteção da privacidade do usuário. Isso mostra a necessidade de regulamentações mais claras e firmes que obriguem essas plataformas a colaborar com a Justiça brasileira, respeitando os limites legais, mas priorizando a proteção das vítimas.

O Congresso Nacional promulgou, em sessão solene, a Emenda Constitucional 115/2022, que eleva a proteção de dados pessoais à categoria de

direito fundamental na Constituição Brasileira. Essa medida visa adaptar a legislação nacional às novas realidades digitais, garantindo maior segurança jurídica aos cidadãos e alinhando o Brasil às práticas internacionais de proteção de dados pessoais

A proteção de dados pessoais, prevista na LGPD, ademais, deve ser pensada em conjunto com os direitos fundamentais à dignidade da pessoa humana, à intimidade e à liberdade. Isso significa que, em situações de conflito, deve haver um equilíbrio entre o direito do agressor ao sigilo e o direito da vítima à proteção. O Judiciário, nesse sentido, deve atuar com sensibilidade e agilidade, especialmente nos casos em que há risco iminente à integridade física ou psicológica da vítima.

6 MEDIDAS DE PROTEÇÃO ÁS VÍTIMAS DE *STALKING* CIBERNÉTICO

No âmbito das pessoas afetadas por *stalking*, a legislação pátria conta com várias ferramentas de proteção. Uma das mais importantes é a possibilidade de solicitar medidas protetivas emergenciais, conforme a Lei nº 11.340/2006 (Lei Maria da Penha), em situações de violência doméstica ou ameaça. Tais medidas podem englobar o afastamento do agressor do domicílio e a restrição de aproximação ou contato com a vítima.

Além disso, a Lei nº 13.968/2019, que modificou o Código Penal, implementou novas normas para garantir a proteção das vítimas de crimes cibernéticos. Isso possibilita, por exemplo, o bloqueio de contas fraudulentas em plataformas sociais e a remoção ágil de conteúdos prejudiciais. Essas iniciativas se tornam ainda mais essenciais no contexto do *stalking*, uma vez que asseguram uma resposta eficaz da Justiça diante da ameaça imediata de prejuízos à vítima. Conforme explica Lima Viana (2023, p.81):

> [...] é fundamental que a sociedade trabalhe na prevenção do crime de *stalking*, promovendo a educação sobre o tema e incentivando as pessoas a denunciar situações de perseguição e assédio. Somente dessa forma, será possível garantir a segurança e a tranquilidade das pessoas e construir uma sociedade mais justa e igualitária.

A sensibilização acerca das ações de proteção durante o *stalking* é vital para assegurar a proteção das vítimas e o cumprimento eficaz da lei. As ações legais devem ser amplamente divulgadas para que as vítimas possam reagir e procurar

ajuda. A sensibilização deve abranger não só as vítimas desse tipo de violência, mas também os especialistas em direito, segurança pública e saúde, para que todos estejam aptos a reconhecer e intervir de maneira eficiente, acolhendo adequadamente a vítima. Ademais, campanhas de conscientização são essenciais para desmistificar o procedimento e assegurar que as vítimas se sintam protegidas ao reportar e procurar auxílio.

As medidas de proteção legal, como o afastamento do agressor e a restrição de contato, são fundamentais, mas muitas vezes não são suficientes, especialmente no ambiente digital. Na internet, o agressor pode continuar a perseguição por meio de perfis falsos, e-mails anônimos, aplicativos com criptografia ou até mesmo fóruns escondidos. Por isso, além das medidas judiciais, é importante que a vítima receba orientação técnica sobre como proteger suas redes sociais, e-mails e dispositivos eletrônicos.

De acordo com Lima Viana (2023, p. 80), o crime de *stalking* apresenta sérias dificuldades para identificação e punição do agressor, especialmente quando os atos de perseguição ocorrem por meios virtuais, como redes sociais e aplicativos de mensagens. Nesses casos, o agressor costuma utilizar perfis falsos ou contas anônimas para continuar assediando a vítima, mesmo após bloqueios anteriores, o que compromete o sucesso das investigações policiais. O autor também destaca: envolvem também o desenvolvimento de transtornos emocionais como ansiedade e depressão, além de prejuízos na vida social, profissional e na confiança interpessoal. Ainda segundo o autor, o *stalking* pode evoluir para situações de extrema gravidade, incluindo agressões físicas e, em alguns casos, até homicídios. Ademais, a sociedade da informação intensifica esse cenário, pois o uso cotidiano das mídias sociais facilita o acesso a dados pessoais da vítima, permitindo que o agressor acompanhe seus movimentos e mantenha contato, mesmo após tentativas de bloqueio.

A atuação de profissionais da área da tecnologia, como analistas de segurança da informação e peritos forenses digitais, pode fazer toda a diferença na proteção da vítima. Eles podem auxiliar na identificação de tentativas de invasão, orientar sobre o uso de autenticação em duas etapas, senhas seguras e outros mecanismos de defesa digital. Em muitos casos, é possível mapear o comportamento do agressor e prevenir futuras investidas.

Outra medida essencial é a criação de redes de apoio psicológico e emocional. A vítima de *stalking*, especialmente o cibernético, tende a se sentir isolada, insegura e, muitas vezes, culpada. O atendimento psicológico pode ajudá-la a retomar sua rotina, recuperar a autoestima e enfrentar o medo causado pelas ameaças constantes. As universidades, organizações não governamentais e centros de atendimento à mulher têm papel importante nesse acolhimento.

Além disso, afigurar-se-ia de relevo a criação de campanhas permanentes que incentivem a denúncia e expliquem os caminhos que a vítima pode seguir. Muitas pessoas ainda desconhecem que o *stalking* é crime, e acabam minimizando os sinais de perseguição. A educação é, portanto, uma forma de prevenção. Ensinar sobre limites, respeito e segurança digital deve fazer parte da formação desde o ensino fundamental.

Por fim, é necessário avançar na elaboração de políticas públicas específicas voltadas ao combate do *stalking* digital. Essas políticas podem incluir a criação de delegacias especializadas, linhas diretas de denúncia, parcerias com empresas de tecnologia e investimento em capacitação de profissionais da segurança pública e da justiça. Somente com um esforço conjunto, amplo e integrado será possível garantir a efetividade da lei e a segurança real das vítimas.

O crime de *cyberstalking* é também previsto na legislação outros países, como Estados Unidos, Reino Unido, Canadá e Austrália, demonstrando que se trata de uma conduta globalmente preocupante.

As consequências para a vítima são profundas e vão além do medo constante: envolvem também o desenvolvimento de transtornos emocionais como ansiedade e depressão, além de prejuízos na vida social, profissional e na confiança interpessoal. Ainda segundo o autor, o *stalking* pode evoluir para situações de extrema gravidade, incluindo agressões físicas e, em alguns casos, até homicídios. Ademais, a sociedade da informação intensifica esse cenário, pois o uso cotidiano das mídias sociais facilita o acesso a dados pessoais da vítima, permitindo que o agressor acompanhe seus movimentos e mantenha contato, mesmo após tentativas de bloqueio.

Dessa forma, é evidente que o *stalking*, especialmente no ambiente digital, representa uma grave ameaça tanto à integridade física como principalmente psicológica, sendo exigido medidas legais, eficazes de capacitação dos profissionais que atuam na rede de proteção as vítimas, sendo fundamental que campanhas

educativas sejam desenvolvidas, para prevenir a prática do crime, e orientar as vítimas quais as formas de proteção

7 CONSIDERAÇÕES FINAIS

A prática do *stalking* no ambiente virtual representa um fenômeno complexo e crescente, que desafia o sistema jurídico brasileiro a responder de maneira eficaz frente às novas formas de violência mediadas pela tecnologia. Apesar dos avanços no reconhecimento do problema, ainda há lacunas relevantes na legislação penal e na estrutura institucional do país, especialmente no que diz respeito à identificação dos agressores, à coleta de provas digitais e à proteção célere e eficaz das vítimas.

Ficou evidente que o enfrentamento do *cyberstalking* demanda não apenas o aprimoramento das normas jurídicas existentes, mas também a criação de políticas públicas integradas que promovam a educação digital, o fortalecimento das instituições de investigação e repressão aos crimes cibernéticos, bem como o apoio psicológico e jurídico às vítimas.

Além disso, é essencial que o ordenamento jurídico acompanhe o ritmo acelerado da evolução tecnológica, com a elaboração de mecanismos legais mais específicos e atualizados, capazes de lidar com as particularidades dos delitos virtuais, garantindo a efetivação dos direitos fundamentais à privacidade, liberdade e segurança dos indivíduos.

Portanto, proteger a sociedade dos impactos do *stalking* cibernético exige uma atuação conjunta entre o Poder Público, os operadores do Direito, as plataformas digitais e a sociedade civil. Somente por meio dessa articulação será possível oferecer respostas jurídicas mais eficazes, humanas e adaptadas à realidade digital que marca o nosso tempo.

REFERÊNCIAS

ALMEIDA, Haian de Assis Lopes de; OLIVEIRA, Tamar Ramos de. Crimes virtuais: o avanço dos crimes eletrônicos e a evolução das leis específicas no Brasil. **Revista Ibero-Americana de Humanidades**, **Ciências e Educação**, v. 8, n. 11, p. 277–294, 2022. Disponível em: https://periodicorease.pro.br/rease/article/view/7554. Acesso em: 18 mar. 2025.

BRASIL. Agência Brasil. **Proteção de dados pessoais passa a ser direito constitucional.** 10 fev. 2022. Disponível em: https://agenciabrasil.ebc.com.br/politica/noticia/2022-02/protecao-de-dados-pessoais-passa-ser-direito-constitucional. Acesso em: 15 maio 2025.

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

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

BRASIL. Código Penal Brasileiro. **Decreto-lei nº 2.848, de 7 de dezembro de 1940.** Art. 147 e art. 146. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm. Acesso em: 02 abr. 2025

BRASIL. **Lei nº 11.340, de 7 de agosto de 2006.** Lei Maria da Penha - Criação de mecanismos para coibir a violência doméstica e familiar contra a mulher. Diário Oficial da União, Brasília, DF, 8 ago. 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11340.htm. Acesso em: 12 nov. 2024.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Altera a Lei nº 9.610, de 19 de fevereiro de 1998, para tipificar os crimes informáticos. Diário Oficial da União: Brasília, DF, 30 nov. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm. Acesso em: 12 mar. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 nov. 2024.

BRASIL. **Lei nº 13.968, de 26 de dezembro de 2019**. Altera a Lei nº 9.099, de 26 de setembro de 1995, para dispor sobre o acordo de não persecução penal e a suspensão condicional do processo. Diário Oficial da União, Brasília, DF, 27 dez. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019 2022/2019/lei/l13968.htm. Acesso em: 12 nov. 2024

BRASIL**. Lei nº 14.132, de 31 de março de 2021**. Altera o Código Penal para incluir o crime de perseguição (*stalking*). Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14132.htm. Acesso em: 01 abr. 2025.

BRASIL. Ministério Público do Rio Grande do Norte. **MPRN promove curso de capacitação em crimes cibernéticos para policiais civis.** 10 fev. 2023. Disponível em: https://www.mprn.mp.br/noticias/mprn-promove-curso-de-capacitacao-em-crimes-ciberneticos-para-policiais-civis/. Acesso em: 15 maio 2025.

BRASIL. **Superior Tribunal de Justiça**. Gravação ambiental clandestina é válida se direito protegido tem valor superior à privacidade do autor do crime. 8 fev. 2024. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/08022024-Gravacao-ambiental-clandestina-e-valida-se-direito-protegido-tem-valor-superior-a-privacidade-do-autor-do-crime.aspx. Acesso em: 15 maio 2025.

CAMBRIDGE UNIVERSITY PRESS. *Stalking*. **Cambridge Dictionary**. Disponível em: https://dictionary.cambridge.org/pt/dicionario/ingles-portugues/*stalking*. Acesso em: 19 nov. 2024.

CAVALCANTE, Vivianne Albuquerque Pereira et al. Violência de gênero contemporâneo: Uma Nova Modalidade através da Pornografia da Vingança. **Interfaces Científicas-Direito**, v. 4, n. 3, p. 59-68, 2016. Disponível em: https://periodicos.set.edu.br/direito/article/view/3118/0. Acesso em: 4 junho. 2025

DOUGLAS, D. M. Doxing: a conceptual analysis. **Ethics and Information Technology**, v. 18, n. 3, p. 199–210. 2016. Disponível em: https://link.springer.com/article/10.1007/s10676-016-9406-0. Acesso em: 5 dez. 2023

GRECO, Rogério. **Código Penal Comentado**. 13. ed. São Paulo: Saraiva, 2023.

GONZALEZ-PEREZ, Cezar. **Information modelling for archaeology and anthropology:** software engineering principles for cultural heritage. Springer Cham. 1 Ed. 2018.

LIMA VIANA, Guilherme Manoel; ALBERTO, Nara Fernandes; JUNIOR, Irineu Francisco Barreto. Prevenção e combate à violência contra a mulher: Lei Maria da Penha e sua aplicação no crime de *stalking*. **Revista Eletrônica Leopoldianum**, v. 49, n. 138, p. 16-16, 2023. Disponível em:https://periodicos.unisantos.br/leopoldianum/article/view/1417/1187. Acesso em: 19 nov. 2024

LIMA, Wesley de. Apontamentos sobre o fenômeno do *stalking*: uma realidade emergente na sociedade contemporânea. **Âmbito Jurídico.** Disponível em: http://ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=9706&revista_caderno=3. Acesso em: 12 nov. 2024.

MAZZUOLI, Valerio de Oliveira. **Curso de Direitos Humanos**. 8. ed. Rio de Janeiro: Método, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530993320/. Acesso em: 02 abr. 2025.

POSTEL, Jon. **Internet Protocol**. Disponível em: https://www.rfc-editor.org/info/rfc791>. Acesso em: 03 jun. 2025.

SILVA, Patrícia Santos da. **Direito e crime cibernético**: análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015.

SIMAS, Diana Viveiros de**. O cibercrime**. 2014. 168f. Dissertação (Mestrado em Ciências Jurídico-Forenses) - Universidade Lusófona de Humanidades e Tecnologias, Lisboa, 2014.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **HC 598.051/SP**, Rel. Min. Reynaldo Soares da Fonseca, Quinta Turma, julgado em 15/12/2020.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira**. Crimes cibernéticos:** Ameaças e procedimentos de investigação. 2ª ed. Rio de Janeiro: Brasport, 2013.