LUMEN ET VIRTUS
ISSN: 2177-2789

CIBERCRIMINALIDADE: A EFICÁCIA DA LEI Nº 14.132/2021 NA PROTEÇÃO DAS VÍTIMAS DE STALKING VIRTUAL NO BRASIL

CYBERCRIME: THE EFFECTIVENESS OF LAW NO. 14,132/2021 IN PROTECTING VICTIMS OF ONLINE STALKING IN BRAZIL

CIBERCRIMEN: LA EFICACIA DE LA LEY N.° 14.132/2021 EN LA PROTECCIÓN DE LAS VÍCTIMAS DE ACOSO EN LÍNEA EN BRASIL

https://doi.org/10.56238/levv16n55-035

Data de submissão: 05/11/2025 **Data de publicação:** 05/12/2025

Eduardo Figueiredo da Silva
Graduando em Direito
Instituição: Faculdade de Teologia, Filosofia e Ciências Humanas Gamaliel – FATEFIG
E-mail: eduf5040@gmail.com

Claudia Araujo Costa
Professora Orientadora
Instituição: Faculdade de Teologia, Filosofia e Ciências Humanas Gamaliel – FATEFIG

RESUMO

O presente trabalho tem como objetivo analisar a eficácia da Lei nº 14.132/2021 na proteção das vítimas de perseguição virtual (stalking digital) no Brasil, examinando sua praticidade, abordando os obstáculos legais, tecnológicos e sociais que o cibercrime gera. A perspectiva doutrinária e jurisprudencial revela que a Lei nº 14.132/2021 é um avanço na proteção da liberdade pessoal, integridade psicológica e privacidade das vítimas de perseguição virtual. No entanto, a eficácia dependerá de fatores complementares como o treinamento técnico das autoridades, o fortalecimento da cooperação entre a plataforma digital e as autoridades públicas, políticas públicas externas à educação digital e apoio psicológico e jurídico às vítimas. Embora a legislação seja importante em termos de proteção contra delitos de assédio virtual, sua implementação permanece sujeita a restrições estruturais, além disso, continua a necessitar de reformas legislativas e, mais importante, de intervenções multidisciplinares para ter sucesso na proteção das vítimas e na prevenção do cibercrime. O artigo tem como metodologia a pesquisa bibliográfica e explicativa, por meio de uma abordagem qualitativa, com fundamento em livros jurídicos, artigos de lei e artigos publicados na rede mundial de computadores

Palavras-chave: Cibercrime. Perseguição Virtual. Proteção às Vítimas. Direito Penal Digital.

ABSTRACT

This paper aims to analyze the effectiveness of Law No. 14.132/2021 in protecting victims of online harassment (digital stalking) in Brazil, examining its practicality and addressing the legal, technological, and social obstacles generated by cybercrime. The doctrinal and jurisprudential perspective reveals that Law No. 14.132/2021 represents progress in protecting the personal freedom, psychological integrity, and privacy of victims of online harassment. However, its effectiveness will depend on complementary factors such as technical training for authorities, strengthening cooperation

between digital platforms and public authorities, public policies external to digital education, and psychological and legal support for victims. Although the legislation is important in terms of protection against online harassment offenses, its implementation remains subject to structural constraints; furthermore, it continues to require legislative reforms and, more importantly, multidisciplinary interventions to succeed in protecting victims and preventing cybercrime. This article employs bibliographic and explanatory research methodology, using a qualitative approach based on legal books, articles of law, and articles published on the World Wide Web.

Keywords: Cybercrime. Virtual Stalking. Victim Protection. Digital Criminal Law.

RESUMEN

Este artículo tiene como objetivo analizar la eficacia de la Ley n.º 14.132/2021 en la protección de las víctimas de acoso en línea (acecho digital) en Brasil, examinando su viabilidad y abordando los obstáculos legales, tecnológicos y sociales que genera el ciberdelito. La perspectiva doctrinal y jurisprudencial revela que la Ley n.º 14.132/2021 representa un avance en la protección de la libertad personal, la integridad psicológica y la privacidad de las víctimas de acoso en línea. Sin embargo, su eficacia dependerá de factores complementarios como la capacitación técnica de las autoridades, el fortalecimiento de la cooperación entre la plataforma digital y las autoridades públicas, las políticas públicas externas a la educación digital y el apoyo psicológico y jurídico a las víctimas. Si bien la legislación es importante en términos de protección contra los delitos de acoso en línea, su implementación sigue sujeta a limitaciones estructurales; además, sigue requiriendo reformas legislativas y, aún más importante, intervenciones multidisciplinarias para lograr la protección de las víctimas y la prevención del ciberdelito. Este artículo emplea una metodología de investigación bibliográfica y explicativa, con un enfoque cualitativo basado en libros de derecho, artículos jurídicos y artículos publicados en la World Wide Web.

Palabras clave: Ciberdelincuencia. Acoso Virtual. Protección de Víctimas. Derecho Penal Digital.

1 INTRODUÇÃO

As relações humanas, a comunicação e a vida social contemporânea foram profundamente alteradas pelo progresso tecnológico e pela expansão da internet. No entanto, com os benefícios da era digital, surgiram novas formas de atividades ilegais, chamadas de cibercrimes, que desafiam o sistema jurídico convencional.

Dentre essas práticas, sobressai-se a perseguição virtual, também conhecida como stalking virtual um fenômeno que, apesar de ter sido inicialmente marginalizado, ganhou importância progressiva devido aos seus efeitos psicológicos e sociais nas vítimas.

A promulgação da Lei n.º 14.132/2021 foi um marco importante no ordenamento jurídico brasileiro, pois introduziu o artigo 147-A no Código Penal, que define o crime de perseguição. Essa lei é uma resposta à demanda por proteger a integridade física, psicológica e liberdade das pessoas frente a comportamentos constantes de assédio e intimidação, principalmente no ambiente virtual.

No entanto, para avaliar a eficácia da norma, é necessário realizar uma análise mais abrangente que considere não apenas sua dimensão penal, mas também suas implicações tecnológicas, institucionais e sociais.

Além disso, o estudo sugere uma reflexão sobre o papel das autoridades, das plataformas digitais e da sociedade civil na proteção das vítimas e na criação de um ambiente digital mais seguro. Com uma perspectiva interdisciplinar, busca-se mostrar que a criminalização do stalking foi um progresso jurídico importante, porém sua eficácia prática depende de ações adicionais, como a educação digital, assistência psicológica e jurídica às vítimas e melhoria das ferramentas de investigação digital.

Portanto, a urgência em entender a aplicação prática da Lei n.º 14.132/2021 e seus limites em face do aumento das perseguições online justifica este estudo. O estudo destaca que o combate à cibercriminalidade não deve se limitar apenas à punição penal, mas requer uma colaboração entre o Estado, sistema de justiça e sociedade para garantir a dignidade humana, liberdade e segurança no ambiente digital.

Justifica-se a pesquisa tendo em vista que o stalking, ou perseguição, tem se tornado uma conduta cada vez mais comum, principalmente em razão dos avanços tecnológicos que facilitam comportamentos invasivos como o cyberstalking. As vítimas de stalking virtual frequentemente enfrentam sérios danos psicológicos, incluindo ansiedade, depressão e transtornos de estresse, que podem evoluir para situações de agressões físicas e, em casos extremos, homicídios.

O stalking representa uma forma insidiosa de violência que ocasiona impactos profundos e duradouros na vida das vítimas. Além de comprometer a saúde mental das pessoas, provocando depressão, ansiedade e outros transtornos psicológicos, essas práticas também ameaçam sua segurança

emocional e física. O constante temor e a sensação de estar sendo vigiado ou perseguido podem levar a um estado de hipervigilância e isolamento social, deteriorando o bem-estar geral das vítimas.

O objetivo do presente trabalho é analisar a eficácia da Lei nº 14.132/2021 na proteção das vítimas de perseguição virtual (stalking) no Brasil, examinando sua praticidade, abordando os obstáculos legais, tecnológicos e sociais que o cibercrime gera. Os objetivos específicos são: avaliar os impactos psicológicos e sociais do stalking nas vítimas, destacando a gravidade da violência perpetrada através de meios digitais e suas consequências para o bem-estar emocional e físico; investigar os principais desafios enfrentados na aplicação da Lei nº 14.132/2021 no contexto do stalking e identificar boas práticas e possíveis ajustes legislativos para fortalecer a proteção das vítimas e a efetividade das medidas punitivas.

Sendo assim, a problemática do artigo será: Quais são os desafios e as oportunidades na criminalização do stalking no Brasil e como o Direito Penal pode ser aprimorado para oferecer uma proteção mais eficaz às vítimas?

O artigo tem como metodologia a pesquisa bibliográfica e explicativa, por meio de uma abordagem qualitativa, com fundamento em livros jurídicos, artigos de lei e artigos publicados na rede mundial de computadores

2 CONCEITO E EVOLUÇÃO HISTÓRICA DA CIBERCRIMINALIDADE

A cibercriminalidade, com ênfase no crime de stalking, emergiu como uma preocupação significativa no contexto digital, dessa forma, o stalking, caracterizado pela perseguição insistente e indesejada que causa medo e angústia à vítima, encontrou no ambiente virtual um terreno fértil para sua proliferação.

Com o uso massivo das redes sociais, aplicativos de mensagens e outras plataformas digitais, os stalkers podem monitorar e assediar suas vítimas com facilidade e anonimato (Gilaberte, 2021).

Destaca-se que, cibercrime ou crime cibernético é qualquer ato em que um computador ou meios de tecnologia da informação é utilizado para cometer um ato criminoso ou em que o computador ou outros meios de tecnologia da informação são o foco de um delito. (Junior, 2019).

O cibercrime está ligado ao fenômeno da criminalidade informacional, que envolve comportamentos que violam direitos fundamentais, tanto por meio da aplicação da informática na prática criminosa ou como componente de tipo legal de delito.

De forma abrangente, a criminalidade informática abarca todas as atividades ilícitas executadas por computadores ou tecnologias da informação. No sentido estrito, a criminalidade da informação abrange crimes, conforme Simas (2014, p. 12) afirma, “quem que o meio informático emerge como componente essencial do tipo legal, ainda que o bem jurídico protegido não seja digital.”

Nos últimos anos, com o desenvolvimento da tecnologia e a proliferação da internet, novas formas de interação social, comunicação e atividades econômicas foram integradas, mas também se desenvolveram novos métodos de comportamento ilícito.

Dessa forma, os crimes cibernéticos (ou crimes informáticos) são uma das questões centrais do Direito Penal moderno, pois desestruturam as formas convencionais de investigação, proteção e prevenção. Nesse novo ambiente, há a necessidade de estabelecer um sistema de leis que preveja a proteção de bens jurídicos públicos no ambiente virtual.

A legislação referente aos crimes cibernéticos no Brasil surgiu gradualmente a partir da década de 2010, e foi desenvolvida de forma mais consistente com a promulgação da Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que caracterizou comportamentos como a invasão de dispositivos informáticos.

Posteriormente, foi lançada a Lei nº 12.965/2014, que é o Marco Civil da Internet, que distribuiu princípios, garantias e direitos para o uso da rede mundial de computadores, assegurando a proteção de dados e a responsabilização dos agentes. Em complemento, a Lei Geral de Proteção de Dados (LGPD) Lei nº 13.709/2018, também trouxe maior rigor à proteção da privacidade e ao gerenciamento de informações pessoais no ambiente digital. Mais recentemente, foi emitida a Lei nº 14.132/2021 que definiu o crime de perseguição, dando grandes passos em direção à redução legal do assédio e ameaças repetidas (também feitas virtualmente).

Assim, pode-se ver que o sistema jurídico brasileiro tem lentamente aprendido as novas realidades sociais da era digital, tentando conciliar direitos humanos como a liberdade de expressão, a privacidade e a segurança dos cidadãos no ciberespaço.

O exame da legislação voltada para os crimes cibernéticos no Brasil é essencial para compreender os desafios impostos pela tecnologia à prestação do Direito, salvaguardando direitos básicos e servindo eficazmente os infratores no ambiente virtual.

A Lei nº 12.965, de 23 de abril de 2014, o Marco Civil da Internet foi um divisor de águas na regulamentação legal do ambiente digital no Brasil. Ressalta-se que o Marco Civil não foi criado para criminalizar condutas em primeira instância; ao contrário, foi concebido para fornecer os princípios, direitos e deveres para o uso da internet, tornando-se um estatuto legal adequado para a rede, em oposição às leis repressivas. Observa-se que é uma norma de natureza essencialmente civil e regulatória, cujo propósito é equilibrar a liberdade de expressão, a privacidade, a neutralidade da rede e a responsabilidade dos provedores de serviço.

O Marco Civil da Internet foi precedido por uma ampla discussão social por estudiosos do direito e agências públicas, bem como organizações civis e profissionais técnicos. O processo de legislação começou em 2009 com consultas públicas online facilitadas pelo Ministério da Justiça e pela Secretaria de Assuntos Legislativos, levando a uma lei nova e amplamente democrática.

Patrícia Peck (2021) também observa que o Marco Civil "inaugura uma nova era de governança digital participativa no Brasil, onde os cidadãos se tornam protagonistas na construção das normas que regem o ciberespaço."

O Marco Civil é composto por 32 artigos divididos em cinco capítulos, e seu artigo 2º lista os princípios fundamentais que orientam o uso da internet no país, entre os quais se destacam: a liberdade de expressão, a proteção da privacidade, neutralidade da rede, a preservação da estabilidade e funcionalidade da internet, a responsabilidade proporcional dos agentes e a liberdade de modelos de negócios. (Brasil, 2014).

Além disso, o artigo 3º complementa esses princípios afirmando que a disciplina do uso da internet é baseada no respeito à liberdade de expressão, aos direitos humanos e ao exercício da cidadania digital, reconhecendo o acesso à internet como uma ferramenta essencial para o desenvolvimento humano e social. (Brasil, 2014).

Os dados pessoais são outro eixo central do Marco Civil, conforme o artigo 7º que garante ao usuário uma série de direitos fundamentais, como a inviolabilidade da privacidade, proteção contra a coleta, uso e armazenamento indevidos de dados, bem como a exigência de consentimento expresso para o tratamento de informações pessoais. (Brasil, 2014).

Salienta-se que as disposições supramencionadas serviram como base legal para a criação subsequente da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que aprofundou ainda mais a regulamentação sobre o tema da privacidade digital.

Greco (2022) observa que "o Marco Civil da Internet atua como a Constituição da Internet brasileira, estabelecendo diretrizes gerais de conduta que buscam harmonizar o direito à liberdade de comunicação com o dever de proteger a privacidade e a segurança da informação."

Para os cibercriminosos, o regime de responsabilidade civil que o Marco Civil define é um dos mais relevantes, conforme o artigo 18 ao mencionar que “os provedores de serviços de internet não são civilmente responsáveis por danos decorrentes de conteúdo gerado por terceiros” e o artigo 19 ao estabelecer que “as aplicações de Internet (redes sociais, sites, plataformas) só se tornarão responsáveis após serem ordenadas por um tribunal a remover o material ofensivo.” (Brasil, 2014).

A Lei nº 14.132, de 31 de março de 2021 marcou uma grande mudança no sistema jurídico brasileiro na especificação do crime de assédio repetido, também conhecido como stalking em inglês. Ressalta-se que essa lei alterou o Código Penal (Decreto-Lei nº 2.848/1940) ao incorporar o artigo 147-A para revogar o antigo artigo 65 da Lei de Contravenções Penais (Decreto-Lei nº 3.688/1941), que tratava da contravenção de perturbação da paz. Assim, o legislador tentou dar mais efeito penal à repressão de comportamentos recorrentes que envolviam assédio, ameaças e vigilância em particular, em um contexto digital.

Na prática, o papel relevante da Lei nº 14.132/2021 reside na proteção da saúde psicológica das vítimas, da liberdade e privacidade da vítima, especialmente em casos de perseguição cibernética.

Antes da implementação, o comportamento contínuo de perseguição era limitado a contravenções penais, com pouco apoio legal disponível, e geralmente era realizado com poucos obstáculos. Assim, a nova lei expandiu o sistema de justiça criminal, dando uma resposta muito mais apropriada a esse tipo de violência.

A Lei nº 14.132/2021 incorpora o artigo 147-A ao Código Penal Brasileiro e define o crime de perseguição, popularmente conhecido como stalking. Essa inovação legislativa representou um avanço importante no sistema jurídico nacional, especialmente à luz das novas dinâmicas de interação social mediadas por tecnologias digitais. No ciberespaço, a interação de perseguição virtual tornou-se cada vez mais comum, exigindo instrumentos específicos de direito penal para coibir práticas de perseguição repetida, invasão de privacidade e assédio psicológico realizados por meios eletrônicos.

No stalking virtual, o assédio ocorre por meios eletrônicos, como redes sociais, aplicativos de mensagens, e-mails, chamadas, fóruns e similares. O comportamento típico envolve monitoramento constante, envio de mensagens persistentes, criação de perfis falsos, divulgação de informações pessoais da vítima sem consentimento, ou até mesmo ameaças e difamação online.

A repetição é um aspecto importante para diferenciar o stalking de atos isolados de perturbação digital, onde o stalking deve ser contínuo, persistente e capaz de induzir medo, ansiedade ou restrição da liberdade de ação e interação social da vítima (Greco, 2022).

Tal conduta habitual deve ser provada para o estabelecimento do próprio delito, assim no cenário online, pode-se prová-la usando capturas de tela, registros de conversas, e-mails, postagens em redes sociais e relatórios de perícia digital, que mostram a repetição e a intenção de perturbar a vítima.

Além disso, a Lei nº 14.132/2021 prevê uma pena aumentada quando a vítima é mulher, criança, adolescente ou idoso, refletindo a preocupação do legislador com grupos socialmente mais vulneráveis. Esta disposição está diretamente alinhada com a Lei Maria da Penha (Lei nº 11.340/2006) e o conceito de violência psicológica, agora reconhecida como uma das formas de violência doméstica e familiar.

Nesse contexto, a criminalização do stalking virtual representa um avanço significativo na proteção dos direitos fundamentais à liberdade e à privacidade, alinhando o sistema jurídico brasileiro com novas formas de crime digital. No entanto, sua aplicação efetiva depende do treinamento técnico das autoridades, de uma melhor cooperação internacional em questões cibernéticas e da educação digital da população, para que o ambiente virtual seja de fato um espaço seguro, livre de perseguições e intimidações.

Embora não haja disposições concretas sobre medidas protetivas na Lei nº 14.132/2021, a aplicação da Lei nº 11.340/2006 (a Lei Maria da Penha) é reconhecida pela doutrina e pela jurisdição,

nos casos em que é aplicada com base na condição de gênero feminino. Algumas medidas protetivas (por exemplo, proibição de aproximação, limitação de contato por qualquer meio de comunicação, afastamento do agressor do local de trabalho ou residência da vítima, suspensão de perfis ou contas usadas em perseguição virtual).

Fora do ambiente judicial, a proteção das vítimas de perseguição virtual deve incluir políticas públicas que ofereçam apoio psicológico, orientação jurídica e suporte tecnológico, especialmente na forma de unidades especializadas em crimes cibernéticos e serviços de apoio às mulheres (DEAMs), tais iniciativas são essenciais para reduzir a subnotificação de casos e encorajar as vítimas a buscar ajuda.

Outra questão preocupante é a educação digital e a conscientização social, como aponta Greco (2022), a criminalização da perseguição "é apenas um passo para combater a perseguição sistemática é necessário criar uma cultura de respeito à privacidade, autonomia e segurança no ambiente virtual."

3 OS DESAFIOS NA PERSECUÇÃO PENAL DOS CRIMES CIBERNÉTICOS

A investigação digital constitui uma das fases mais complexas da acusação criminal no âmbito dos crimes cibernéticos, desse modo, operando em sistemas distribuídos e globais, o ambiente virtual oferece aos perpetradores maneiras de ocultar sua identidade, disfarçar rastros e dificultar a coleta de provas.

Por isso, aspectos como anonimato, criptografia e o uso da chamada dark web claramente representam alguns dos principais obstáculos para as agências de aplicação da lei e o Judiciário, de modo que, o anonimato por meios digitais é um dos problemas mais sérios para a polícia ao investigar crimes cibernéticos.

Ao criar perfis falsos, e-mails adicionais e com redes privadas virtuais (VPNs), é mais fácil até mesmo para criminosos disfarçar redes pessoais para mascarar endereços IP enquanto obscurecem o local do crime.

Apesar de o Marco Civil da Internet (Lei nº 12.965/2014) exigir que os provedores mantenham registros de conexão e acesso a aplicações, a identificação adequada do agente depende de quão bem-sucedida pode ser a cooperação das plataformas e a rapidez da ação judicial para preservar os dados e essa informação nem sempre é coletada prontamente.

A criptografia é outro grande obstáculo que protege a privacidade da própria comunicação, utilizando o meio de transmissão de informações. Embora seja importante para a privacidade e segurança da informação, seu uso por crimes digitais gera o fenômeno conhecido como "criptografia de ponta a ponta", o que significa que na comunicação através de aplicativos criptografados, ninguém (incluindo o provedor desses aplicativos) pode acessar os dados quando eles se comunicam.

Isso resulta no chamado "apagão de evidências", onde, apesar de fortes acusações de atividade criminosa, não é possível acessar o conteúdo necessário para processos criminais, levando a um impasse entre o direito à privacidade e o dever do Estado de investigar e punir crimes.

Ainda mais difícil é combater atividades ilegais na dark web, uma camada oculta da internet que não é indexada por motores de busca regulares e requer o uso de navegadores específicos, como o Tor, para ser acessada.

Assim, em tal cenário, mercados ilícitos de drogas, armas, pornografia infantil, dados pessoais e serviços prestados por organizações de hackers são abundantes – e as transações são comumente realizadas usando criptomoedas, que proporcionam um imenso ocultamento financeiro. Operações nesta área necessitam de treinamento especializado, supervisão constante e cooperação internacional, já que servidores e usuários estão frequentemente localizados em diferentes países, complicando a aplicação da lei penal brasileira devido aos limites da jurisdição territorial.

A evidência digital é uma das ferramentas mais relevantes e também das mais complicadas na acusação criminal de crimes cibernéticos. À medida que as interações humanas e o comportamento criminoso continuam a evoluir para meios digitais, a produção, preservação e análise de evidências eletrônicas tornaram-se aspectos fundamentais na elucidação dos fatos e no estabelecimento da certeza judicial.

No entanto, como a natureza dos dados digitais é intangível, mutável e facilmente manipulável, requer rigor técnico e legal em sua aquisição, sob pena de comprometer sua validade processual.

A aquisição de provas digitais deve ser guiada por princípios constitucionais que regem suas atividades probatórias, particularmente o devido processo legal (art. 5º, LIV, CF), o direito à intimidade e à privacidade (art. 5º, X, CF) e a confidencialidade das comunicações (art. 5º, XII, CF). (Brasil, 1988).

Para informações mantidas em dispositivos eletrônicos, bem como em contas de e-mail, redes sociais e serviços de nuvem, geralmente é uma questão de autorização judicial, de acordo com a interpretação harmonizada do Supremo Tribunal Federal (STF) e do Superior Tribunal de Justiça (STJ).

Outro aspecto a ser considerado é a cadeia de custódia das provas digitais que é o conjunto de procedimentos documentados que garante a integridade, autenticidade e confiabilidade de evidências digitais. Essa formalização é crucial para garantir que os dados não sejam manipulados ou adulterados, garantindo a confiança probatória.

Quando se trata de evidências digitais, a preservação dos registros originais, a geração de códigos hash, o software forense, bem como os certificados, registrando todas as ações realizadas sobre o material, têm um papel vital na cadeia de custódia. Para quebrar a sequência de análise processual,

deve haver uma interrupção que cause nulidade processual; a confiabilidade das evidências digitais está ligada à integridade técnica delas.

A validade legal das evidências digitais é uma questão ainda mais sensível, pois está correlacionada com seu contexto, legalidade e relevância. Salienta-se o artigo 155 do Código de Processo Penal, que ressalta "o juiz formará sua convicção pela livre avaliação das provas, mas não pode basear-se apenas nas provas obtidas durante a investigação, exceto as provas cautelares e antecipadas."

Portanto, para que as evidências digitais sejam válidas, elas devem ser adquiridas por meio de um processo legal, sujeitas a procedimentos contraditórios e acompanhadas por uma perícia técnica competente.

Em essência, o Código Penal Brasileiro não só pode proteger o direito do indivíduo de proteger sua liberdade, mas também a integridade de seu bem-estar psicológico, e, portanto, essas medidas em referência ao crime de perseguição podem ser abordadas com a aplicação da Lei nº 14.132/2021.

No entanto, o desenvolvimento do crime eletrônico e o ritmo acelerado do desenvolvimento tecnológico representam uma ameaça persistente à implementação prática dessa regulamentação. Portanto, o diálogo de visões e sugestões de melhoria torna-se necessário para o aprimoramento da política criminal brasileira no que diz respeito à perseguição virtual e outros crimes cibernéticos.

Em primeiro lugar, é importante aprimorar os frameworks de investigação digital. A conduta virtual é tecnicamente complicada e exige treinamento rotineiro de especialistas e agentes públicos à medida que aplicam análise forense digital, rastreamento de IP, criptografia e questões de segurança da informação.

O investimento em laboratórios cibernéticos e assistência técnica de parceiros internacionais aumentará a eficácia da persecução penal e diminuirá a impunidade. Segundo Souza (2022), a escassez de recursos humanos e tecnológicos especializados é uma das principais restrições na aplicação da Lei nº 14.132/2021.

O cibercrime é tanto difuso quanto dinâmico e não pode ser combatido apenas por meios repressivos. Esses efeitos adversos só podem ser totalmente enfrentados por meio de intervenções preventivas colaborativas que englobem educação digital, alfabetização tecnológica e formação ética dos usuários da internet.

A educação digital, portanto, é vista como um instrumento chave para a política pública e pode reduzir vulnerabilidades, incentivar o uso responsável das tecnologias modernas e fortalecer a cidadania no ciberespaço.

Nesse sentido, o processo de ensino e aprendizagem para adquirir uma compreensão crítica, ética e segura do uso das tecnologias de informação e comunicação (TICs). Isso requer habilidades

que permitam às pessoas identificar ameaças, proteger informações pessoais, considerar atos abusivos e agir conscientemente nas redes.

Ferreira (2023) argumenta que a prevenção do cibercrime tem como primeiro passo o treinamento do usuário, observando que "a melhor defesa contra o cibercrime é o conhecimento disseminado e um senso de responsabilidade digital."

Além da educação formal, campanhas de conscientização social devem ser incentivadas pelo Estado com a cooperação de empresas de tecnologia, ONGs e agências públicas para combater o stalking virtual, o cyberbullying, a exposição inadequada de imagens e as fake news.

Iniciativas como a Semana Nacional de Segurança da Informação, conduzida pela Secretaria de Governo Digital, e os esforços educacionais da SaferNet Brasil são lembretes desses esforços embora esporádicos e descoordenados.

O Marco Civil da Internet (Lei nº 12.965/2014), com sua ênfase em princípios como a responsabilidade social pelo uso da rede e a garantia da liberdade de expressão com respeito aos direitos humanos. Essa orientação deve informar não apenas a aplicação do direito penal, mas também programas governamentais de longo prazo para educação digital e prevenção.

A parceria entre o Ministério da Justiça, o Ministério da Educação e o Comitê Gestor da Internet no Brasil (CGI.br) é fundamental para o estabelecimento de uma política nacional de cidadania digital, com foco em segurança, ética e inclusão.

Consequentemente, a educação digital e a prevenção como políticas públicas são parte integrante da política criminal contemporânea que busca não apenas a prosperidade, mas também a mudança cultural e social.

O combate ao cibercrime deve começar com o empoderamento informacional do cidadão, com o Estado assumindo um papel ativo na promoção de uma cultura de segurança, ética e responsabilidade digital, pilares indispensáveis para a convivência democrática no ciberespaço.

Embora a Lei nº 14.132/2021, que moderniza o crime de perseguição no sistema jurídico brasileiro, represente um passo bastante notável na proteção das liberdades pessoais e psicológicas das vítimas, a experiência prática revelou lacunas regulatórias e desafios de interpretação desde a sua implementação.

Assim, é necessário discutir possíveis mudanças na lei, de modo a torná-la mais eficaz e proporcional à forma como os crimes cibernéticos, como a perseguição virtual e outros, evoluíram em relação à nossa realidade tecnológica existente.

Para enfrentar esses desafios, seria difícil para o legislador inserir um parágrafo específico no artigo 147-A, prevendo formas prejudiciais de perseguição digital, com descrições detalhadas de comportamentos típicos e fatores agravantes. Essa mudança garantiria segurança jurídica e

uniformidade interpretativa, evitando que condutas graves sejam rebaixadas a delitos menores ou que meros atos de incivilidade sejam indevidamente criminalizados.

Uma proposta adicional relevante consiste em incluir mecanismos processuais complementares à Lei nº 14.132/2021, semelhantes à Lei Maria da Penha (Lei nº 11.340/2006). Poderiam ser previstas medidas protetivas específicas para o ambiente virtual, como o bloqueio judicial imediato de perfis falsos, a remoção rápida de conteúdo persecutório, a proibição de contato digital e a preservação obrigatória de provas eletrônicas pelos provedores.

Por último, as políticas públicas obrigatórias para a educação digital e prevenção baseadas em normas criminais são impedidas devido ao Artigo 205 da Constituição Federal (educação como meio de desenvolvimento pleno do cidadão) que prevê legislação para esse efeito.

A legislação criminal não pode ser considerada isoladamente: a eficácia da Lei nº 14.132/2021 depende da formação ética, tecnológica e emocional dos usuários da internet e do fortalecimento da função social e pedagógica do Direito Penal.

Por isso que essas recomendações para o aprimoramento legislativo abordam o desenvolvimento de um Direito Penal Digital mais dinâmico, garantidor e eficaz, cujo propósito é equilibrar a liberdade individual, a segurança da informação e a proteção da dignidade humana no ciberespaço.

O desafio para o legislador moderno hoje é conciliar a inovação tecnológica com o espírito dos nossos valores constitucionais, para garantir que o combate ao cibercrime seja feito em nome do Estado Democrático de Direito.

4 CONSIDERAÇÕES FINAIS

O objetivo deste trabalho foi trabalho é analisar a eficácia da Lei nº 14.132/2021 na proteção das vítimas de perseguição virtual (stalking) no Brasil, examinando sua praticidade, abordando os obstáculos legais, tecnológicos e sociais que o cibercrime gera.

Toda a pesquisa resultou nas conclusões de que a sociedade moderna, que se tornou mais dependente da tecnologia e da comunicação por meio virtual, trouxe novos tipos de crime onde intervenções legais rápidas, específicas e técnicas são os novos requisitos.

A verdade é que o aumento do cibercrime é realmente uma das maiores ameaças à segurança e à liberdade no século XXI. A perspectiva histórica forneceu evidências de que o crime digital mudou junto com os avanços tecnológicos, de nada mais do que intrusões e fraudes eletrônicas para comportamentos sofisticados que envolvem o uso de criptografia e anonimato na dark web.

Isso exigiu que o Estado reformasse sua ordem jurídica, na qual, através da história legislativa, aprovou, entre outras coisas, a Lei Carolina Dieckmann (Lei nº 12.737/2012), o Marco Civil da Internet

(Lei nº 12.965/2014) e, mais recentemente, a Lei nº 14.132/2021. A criminalização do stalking, e especialmente de sua versão virtual, tem sido uma das maiores conquistas do Direito Penal Brasileiro.

Ao reconhecer as características do artigo 147-A do Código Penal, a proteção à liberdade pessoal, à integridade psicológica e à privacidade das vítimas é resguardada, preenchendo o vazio atual no tratamento legal dado ao assédio repetido.

Mas a aplicação prática da norma permanece limitada por desafios de prova, subnotificação de casos e infraestrutura tecnológica e humana insuficiente para investigação digital. Foi mencionado posteriormente que a eficácia da Lei nº 14.132/2021 baseia-se principalmente na intervenção coesa dos órgãos do sistema de justiça criminal e das empresas de mídia social, juntamente com intervenções públicas de prevenção.

A criminalização da atividade por si só não é suficiente para resolver o problema; a educação digital deve ser reforçada, as autoridades devem ser treinadas; também é necessário proteger as vítimas.

Além disso, a assistência psicológica e jurídica auxilia na restauração dos danos e na restauração da sociedade das partes afetadas.

Portanto, a Lei nº 14.132/2021 é um marco significativo no combate à perseguição virtual através do desenvolvimento das disposições, mas toda a implementação da política deve ser constantemente atualizada por meio da lei, atualizações tecnológicas e iniciativas de mudança social.

A batalha contra o cibercrime também exige uma atitude multidimensional e humana que integra a defesa da dignidade humana com os princípios de liberdade e privacidade dos meios digitais. Nada pode ser alcançado a menos que essa solução holística seja implementada para que todos possamos habitar um ciberespaço seguro e mais respeitoso.

REFERÊNCIAS

ALEXANDRE JUNIOR, Julio Cesar. Cibercrime: um estudo acerca do conceito de crimes informáticos. Franca: Faculdade de Direito de Franca, 2019.

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

BRASIL. Lei nº 7.210, de 11 de julho de 1984. Institui a Lei de Execução Penal. Diário Oficial da União, Brasília, DF, 13 jul. 1984.

BRASIL. Lei nº 11.340, de 7 de agosto de 2006. Cria mecanismos para coibir a violência doméstica e familiar contra a mulher (Lei Maria da Penha). Diário Oficial da União, Brasília, DF, 8 ago. 2006.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos (Lei Carolina Dieckmann). Diário Oficial da União, Brasília, DF, 3 dez. 2012.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Diário Oficial da União, Brasília, DF, 24 abr. 2014.

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.

BRASIL. Lei nº 14.132, de 31 de março de 2021. Altera o Código Penal para incluir o crime de perseguição (stalking). Diário Oficial da União, Brasília, DF, 1º abr. 2021.

Comitê Gestor da Internet no Brasil. Relatório TIC Educação 2023. São Paulo: CGI.br, 2024.

CONSELHO DA EUROPA. Convenção de Budapeste sobre o Cibercrime. Budapeste, 23 nov. 2001.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 2. ed. Rio de Janeiro: Forense, 2021.

FERREIRA, Flávia. Stalking e Cibercriminalidade: o desafio da tutela penal no espaço virtual. São Paulo: Revista dos Tribunais, 2023.

GOMES, Luiz Flávio; CERVINI, Raúl. Criminalidade informática: aspectos penais e processuais. São Paulo: Revista dos Tribunais, 2021.

GRECO, Rogério. Crimes Cibernéticos: teoria e prática. Rio de Janeiro: Impetus, 2022.

MENDES, Gilmar Ferreira. Direitos Fundamentais e Internet: o equilíbrio entre liberdade e segurança. São Paulo: Saraiva, 2022.

Ministério da Justiça e Segurança Pública. Diretrizes Nacionais de Atendimento às Vítimas de Crimes. Brasília, 2022.

ONU. Declaração dos Princípios de Justiça para as Vítimas de Crimes e Abuso de Poder. Resolução nº 40/34, de 29 de novembro de 1985.

PIMENTA, Andréa; COSTA, Thaís. Psicologia e direito: atendimento a vítimas de crimes cibernéticos. Brasília: Conselho Federal de Psicologia, 2023.

SAFERNET BRASIL. Relatório anual de denúncias de crimes cibernéticos no Brasil. São Paulo, 2023.

SOUZA, Sérgio Ricardo de. Prova digital e investigação criminal: desafios da persecução penal na era tecnológica. Brasília: JusPodivm, 2022.

UNESCO. Education for Digital Citizenship in the 21st Century. Paris: UNESCO Publishing, 2021.