RGe
ISSN: 2177-3246

STALKING DIGITAL: UMA ANÁLISE DA LEI MARIA DA PENHA PARA À LUZ DA LEI 14.132/2021

DIGITAL STALKING: AN ANALYSIS OF THE MARIA DA PENHA LAW IN LIGHT OF LAW NO. 14.132/2021

ACOSO DIGITAL: UN ANÁLISIS DE LA LEY MARIA DA PENHA A LA LUZ DE LA LEY 14.132/2021

10.56238/revgeov17n4-115

Rackel Cunha de Santana e Santana
Bacharelanda em Direito
Instituição: Instituto de Ensino Superior do Sul do Maranhão (IESMA/Unisulma)
E-mail: cunharackel@gmail.com.br

Lucas Lucena Oliveira
Professor Orientador
Doutor em Direito
Instituição: Unidade de Ensino Superior do Sul do Maranhão (UNISULMA)
E-mail: lucas.lucena@unisulma.edu.br

Luziane Lucena Souza Oliveira
Professora Coorientadora
Juíza de Paz
Instituição: Tribunal de Justiça do Maranhão, Unidade de Ensino Superior do Sul do Maranhão (UNISULMA)
E-mail: npj@unisulma.edu.br

RESUMO

Este estudo examina o fenômeno do *stalking* digital e as restrições da Lei Maria da Penha no enfrentamento de delitos cometidos no ambiente virtual. A investigação revela que, apesar de a referida lei constituir um avanço na salvaguarda das mulheres frente à violência doméstica e familiar, sua aplicação no espaço digital apresenta deficiências relevantes, sobretudo diante da perseguição virtual que envolve violação de privacidade, assédio psicológico e vigilância contínua. Nesse cenário, sobressai a Lei nº 14.132/2021, que incrimina a perseguição (*stalking*) no direito brasileiro, ampliando a proteção das vítimas ao reconhecer condutas reiteradas que ameaçam a liberdade e a intimidade, inclusive por meios digitais. Não obstante, o trabalho demonstra que as medidas protetivas convencionais, concebidas para o âmbito físico, têm eficácia limitada no ciberespaço, onde o agressor consegue exercer contato e controle à distância. A pesquisa adotou metodologia qualitativa, incluindo revisão bibliográfica e análise documental e jurisprudencial. Conclui-se pela necessidade de aprimoramento legislativo, com medidas protetivas digitais específicas e maior capacitação técnica, a fim de garantir a segurança das mulheres no ambiente virtual.

Palavras-chave: *Stalking* Digital. Lei Maria da Penha. Crimes Virtuais. Violência Contra a Mulher. Proteção Jurídica.

ABSTRACT
This study examines the phenomenon of digital stalking and the constraints of the Maria da Penha Law in addressing offenses committed in the virtual environment. The investigation reveals that, although this law represents a significant advancement in safeguarding women against domestic and family violence, its application in the digital sphere presents relevant shortcomings, particularly in the face of virtual persecution involving violations of privacy, psychological harassment, and continuous surveillance. In this context, Law No. 14,132/2021 stands out, as it criminalizes stalking within the Brazilian legal system, broadening victim protection by recognizing repeated conduct that threatens freedom and privacy, including through digital means. Nevertheless, the study demonstrates that traditional protective measures, designed for the physical realm, have limited effectiveness in cyberspace, where the aggressor can maintain contact and exert control remotely. The research adopts a qualitative methodology, including a literature review as well as documentary and jurisprudential analysis. It concludes that legislative improvement is necessary, with the development of specific digital protective measures and enhanced technical training, in order to ensure the safety of women in the virtual environment.

Keywords: Digital *Stalking.* Maria da Penha Law. Virtual Crimes. Violence Against Women. Legal Protection.

RESUMEN
Este estudio examina el fenómeno del acoso digital y las limitaciones de la Ley Maria da Penha para abordar los delitos cometidos en el entorno virtual. La investigación revela que, si bien la mencionada ley constituye un avance en la protección de las mujeres contra la violencia doméstica y familiar, su aplicación en el espacio digital presenta deficiencias significativas, especialmente en lo que respecta al acoso virtual que implica violación de la privacidad, acoso psicológico y vigilancia continua. En este contexto, destaca la Ley N° 14.132/2021, que penaliza el acoso en la legislación brasileña y amplía la protección de las víctimas al reconocer conductas reiteradas que amenazan la libertad y la intimidad, incluso a través de medios digitales. Sin embargo, el trabajo demuestra que las medidas de protección convencionales, diseñadas para el ámbito físico, tienen una eficacia limitada en el ciberespacio, donde el agresor puede ejercer contacto y control de forma remota. La investigación adoptó una metodología cualitativa, que incluyó revisión bibliográfica y análisis documental y jurisprudencial. Concluye que es necesario mejorar la legislación, con medidas específicas de protección digital y mayor capacitación técnica, para garantizar la seguridad de las mujeres en el entorno virtual.

Palabras clave: Acoso Digital. Ley María da Penha. Ciberdelitos. Violencia Contra las Mujeres. Protección Jurídica.

1 INTRODUÇÃO

A Lei nº 11.340/2006, conhecida como Lei Maria da Penha, foi elaborada em um contexto em que a violência doméstica era predominantemente física e presencial. No entanto, a realidade contemporânea revela que o espaço digital é igualmente capaz de gerar danos profundos à liberdade, à privacidade e à dignidade das vítimas. O *stalking digital*[1] caracterizado pelo monitoramento constante, invasão de privacidade e intimidação psicológica, expõe lacunas jurídicas que dificultam a proteção efetiva das mulheres e de outros grupos vulneráveis.

Nesse cenário, a Lei nº 14.132/2021 representa um avanço ao tipificar o crime de perseguição (*stalking*) no ordenamento jurídico brasileiro, reconhecendo condutas reiteradas que atentam contra a liberdade e a intimidade da vítima, inclusive por meios digitais. Ainda assim, apesar de ampliar a proteção penal, persistem desafios na articulação entre essa legislação e as medidas protetivas da Lei Maria da Penha, especialmente no que se refere à eficácia das respostas jurídicas no ambiente virtual.

O presente trabalho aborda o fenômeno do *stalking* digital e a insuficiência da Lei Maria da Penha para lidar com crimes virtuais. A relevância do tema decorre da crescente digitalização das relações sociais e da consequente ampliação das formas de violência psicológica e perseguição que se manifestam no ambiente virtual. Redes sociais, aplicativos de mensagens e plataformas digitais tornaram-se espaços de interação, mas também de vulnerabilidade, onde práticas abusivas se multiplicam e desafiam os limites da legislação tradicional.

A escolha deste tema se justifica pela necessidade de avaliar se a legislação vigente é capaz de enfrentar os desafios impostos pela era digital e de propor alternativas que ampliem a segurança jurídica. Além da relevância social, o estudo busca contribuir para o debate acadêmico e legislativo sobre a modernização do ordenamento jurídico brasileiro, reconhecendo que o ambiente virtual não é separado da realidade cotidiana, mas uma extensão dela.

O problema central da pesquisa consiste em verificar se a Lei Maria da Penha é eficaz na proteção contra o *stalking digital* ou se sua aplicação se mostra inadequada diante das especificidades dos crimes virtuais. O objetivo geral é analisar a efetividade da lei nesse contexto e propor reformas legislativas que fortaleçam os mecanismos de proteção. Os objetivos específicos incluem: (i) Identificar as principais falhas da Lei Maria da Penha na prevenção e repressão ao stalking digital; (ii) Discutir os desafios probatórios relacionados à produção e à preservação de provas no ambiente virtual; (iii) Analisar os entraves institucionais, especialmente quanto à capacitação técnica e à atuação estatal

[1] O *stalker digital* é a pessoa que, valendo-se de recursos tecnológicos, redes sociais, aplicativos de mensagem, e-mail e demais ambientes virtuais, persegue, vigia ou hostiliza repetidamente outra pessoa. Tal comportamento abrange ações como vigilância contínua, envio persistente de mensagens, apropriação indevida de dados pessoais e invasão da esfera íntima, provocando medo, vexame ou transtorno psicológico à vítima. No Direito brasileiro, essas condutas podem ser tipificadas como crime de perseguição, nos termos da Lei nº 14.132/2021.

diante da violência digital; e (iv) Sugerir medidas protetivas digitais que assegurem maior efetividade na proteção das vítimas.

Para alcançar esses objetivos, a pesquisa adota uma abordagem qualitativa, fundamentada em revisão bibliográfica, análise documental com ênfase em suporte teórico em Barros; Oliveira (2025), Rivelli (2025), Casto; Sydow (2017); e estudo de jurisprudência, conforme já destacado no resumo do trabalho. O método permite examinar criticamente as lacunas legislativas e os desafios probatórios relacionados ao *stalking* digital, bem como avaliar a efetividade das medidas protetivas previstas na Lei Maria da Penha.

A investigação estrutura-se em etapas que incluem a delimitação do problema, a análise normativa e jurisprudencial e a proposição de medidas protetivas digitais, buscando oferecer uma compreensão abrangente da inadequação do ordenamento jurídico atual diante das dinâmicas tecnológicas contemporâneas. Nesse percurso, enfatiza-se a necessidade de constante atualização legislativa e interpretativa, de modo a assegurar que os instrumentos jurídicos acompanhem a velocidade das transformações digitais e garantam efetiva proteção aos direitos fundamentais.

2 A INSUFICIÊNCIA DA PROTEÇÃO JURÍDICA NO CENÁRIO DIGITAL

A falta de proteção legal no ambiente digital se torna clara ao analisarmos o rápido desenvolvimento das tecnologias e sua conexão com comportamentos como o *stalking* digital. A rapidez com que novas ferramentas aparecem contínua pressiona o sistema jurídico, que requer um tempo adequado para discussões, amadurecimento e análise de resultados antes de estabelecer regras.

Esse descompasso resulta em legislações recentes que rapidamente se tornam inadequadas, permitindo que crimes cibernéticos se espalhem e explorem brechas na legislação. A transformação das relações sociais para o meio virtual impõe novos desafios ao ordenamento. Nesse contexto, torna-se urgente a criação de políticas públicas e mecanismos jurídicos capazes de acompanhar a velocidade das inovações tecnológicas.

No que diz respeito ao *stalking* digital, a ineficácia da Lei Maria da Penha é bastante evidente. Embora criada para proteger mulheres que enfrentam violência doméstica e familiar, a lei não foi elaborada para abordar perseguições online, ameaças pela internet ou invasões de privacidade através de redes sociais e aplicativos. Conforme assevera Barbosa.

> A aparência do *stalking* ganhou contornos inéditos na sociedade contemporânea. Se antes a perseguição se manifestava por meio da presença física constante, telefonemas insistentes ou vigilância direta, hoje ela se expressa de maneira fragmentado, distribuído entre aplicações, redes sociais, geolocalização e comportamentos digitais repetitivos que produzem sensações permanentes de vigilância (Barbosa, 2025).

Apesar do Código Penal ter classificado o crime de perseguição, a integração dessa norma com a abordagem protetiva da Maria da Penha ainda é restrita, resultando em muitas vítimas em condições de vulnerabilidade. “A violência doméstica contra as mulheres é uma característica estrutural e multifacetada, que exige respostas efetivas do sistema jurídico e das políticas públicas para proteção das vítimas” (Barros; Oliveira 2025, p. 4369).

A insuficiência de uma tipificação analítica específica ao *cyberstalking*[2] no Código Penal mitiga a eficácia da norma, gerando lacunas que alimentam a insegurança jurídica. Quando a conduta delitiva se examina no ambiente virtual, através de algoritmos e perfis apócrifos, a subsunção do fato à norma torna-se complexa e subjetiva. Tal cenário dificulta a pronta intervenção estatal, retardando a proteção de agressores que valem do anonimato tecnológico para violar a privacidade alheia. Castro e Sydow afirmam que:

> O stalking, no ambiente virtual, ganha contornos de onipresença e perenidade, uma vez que a rede mundial de computadores permite ao agressor o monitoramento constante da vítima, suprimindo-lhe a paz de espírito e a liberdade de autodeterminação sem que haja, necessariamente, a proximidade física (Castro; Sydow, 2017, p. 38).

Essa barreira dogmática obstaculiza, sobretudo, a aplicação de medidas protetivas de urgência, pois a falta de clareza sobre os meios de execução impede o magistrado. Sem a visibilidade imediata do *periculum in mora*[3], a vítima permanece em estado de vulnerabilidade perante uma violência que, embora imaterial, é contumaz e devastadora. Assim, a proteção da autodeterminação individual exige que o Direito acompanhe a celeridade e a onipresença das interações digitais contemporâneas.

Essa lacuna normativa compromete a efetividade das medidas de proteção, deixando vítimas em situação de vulnerabilidade diante de práticas reiteradas de perseguição online. Além disso, a ausência de tipificação clara gera dificuldades interpretativas para operadores do direito, que precisam recorrer a analogias ou enquadramentos insuficientes em tipos penais tradicionais

Essa questão se torna ainda mais séria devido à natureza transnacional da internet. Um agressor pode estar localizado em outro país, enquanto a vítima enfrenta os efeitos no território brasileiro, o que levanta questões sobre qual legislação deve ser aplicada e como as autoridades de diferentes regiões podem colaborar. Tratados internacionais, como a Convenção de Budapeste[4], tentam facilitar essa

[2] Nomenclatura em inglês para *Stalker Digital*

[3] *Periculum in mora* é uma expressão latina utilizada no Direito Processual que significa “perigo na demora”. Refere-se ao risco de que a espera pela decisão final do processo cause dano irreparável ou de difícil reparação à parte, justificando a concessão de medidas urgentes, como tutelas provisórias ou medidas protetivas, a fim de evitar o agravamento da situação enquanto o mérito não é definitivamente julgado.

[4] A Convenção de Budapeste, formalmente denominada Convenção sobre o Crime Cibernético (2001), é um tratado internacional elaborado no âmbito do Conselho da Europa que estabelece diretrizes para a prevenção, investigação e repressão de crimes praticados no ambiente digital. Seu objetivo é harmonizar legislações nacionais, facilitar a cooperação jurídica entre países e aprimorar mecanismos de coleta e compartilhamento de provas eletrônicas, sendo considerada o principal instrumento internacional no combate à criminalidade cibernética.

cooperação, mas ainda encontram desafios devido à velocidade com que novas formas de crimes digitais emergem.

Outro aspecto essencial é a falta de especialização. Muitos sistemas judiciários não contam com profissionais treinados em perícia digital. “A ausência de documentação adequada fragiliza o enfrentamento jurídico, e a vítima muitas vezes demora a consideração que está sendo vigiada, permitindo que o perseguidor amplie sua atuação” (Barbosa, 2025).

Além disso, a falta de formação adequada pode resultar em interpretações errôneas das leis, comprometendo a aplicação correta das normas. Sem essa preparação, o sistema jurídico está suscetível a se tornar ultrapassado em relação aos métodos criminosos atuais, permitindo que hackers, fraudadores e perseguidores digitais aproveitem as lacunas legais e técnicas.

Portanto, é vital investir em formação contínua, estabelecer núcleos especializados e promover a colaboração entre profissionais do direito e especialistas em tecnologia. Segundo Oliveira Filho (2024), uma carência de formação especializada sobre questões de gênero dentro das instituições de justiça brasileira contribui para a revitimização das mulheres, uma vez que o despreparo dos agentes públicos impede uma resposta judicial adequada e sensível à realidade da violência doméstica.

O futuro do direito digital depende de legislações mais flexíveis e adaptáveis, maior cooperação internacional e educação contínua para os profissionais. Somente assim poderemos enfrentar os desafios de um mundo em que a tecnologia avança de maneira acelerada, enquanto o direito precisa não apenas acompanhar, mas também antecipar os riscos associados a essa evolução.

2.1 OS DESAFIOS PROBATÓRIOS E A INVISIBILIDADE DO AGRESSOR NO ESPAÇO VIRTUAL

A efetividade da resposta judicial em casos de *stalking* digital enfrenta um obstáculo significativo na fase de coleta de provas. Ao contrário dos delitos ocorridos em ambientes físicos, onde há maior facilidade para adquirir vestígios e depoimentos de testemunhas, a perseguição online é caracterizada pela instabilidade dos dados e pelo uso de métodos de anonimização.

A simples criação e destruição de perfis falsos, juntamente com o uso de Redes Privadas Virtuais (VPNs), cria desafios consideráveis para a identificação do autor, um elemento essencial para o início do processo penal.

Além da identificação do perpetrador, garantir a preservação das provas digitais é um desafio tanto para a vítima quanto para os profissionais do direito. Segundo Souza (2024), a eficácia da proteção ao crime de perseguição digital enfrenta obstáculos severos devido à natureza efêmera das provas online e à facilidade com que o agressor oculta a sua identidade real, gerando um estado de "invisibilidade" que desafia a atuação do sistema de justiça brasileiro.

A captura de tela, embora comum, tem um valor probatório reduzido em tribunais superiores devido à facilidade de sua manipulação, exigindo abordagens mais rigorosas como a Ata Notarial ou a utilização de plataformas de *blockchain*[5] para assegurar a manutenção da integridade da cadeia de custódia. Essa complexidade técnica cria um cenário que requalifica a vítima. Frequentemente, quando a vítima de *stalking* digital busca ajuda do Estado, ela se depara com:

A) Demora nas plataformas: A lentidão dos provedores de serviços em disponibilizar dados de conexão (IPs) e registros de acesso, que frequentemente requerem ordens judiciais específicas.

B) Desaparecimento da prova: A natureza passageira das interações digitais (como mensagens que se apagam ou perfis deletados) pode resultar na perda de evidências antes que a autoridade policial tenha a chance de preservá-las.

C) Ceticismo institucional: Uma tendência a desvalorizar o impacto psicológico da perseguição online na ausência de um contato físico iminente, desconsiderando que o espaço virtual é uma extensão da realidade cotidiana.

Assim, a falha jurídica vai além do texto legal, residindo na incapacidade do sistema estatal de analisar evidências tecnológicas com a mesma agilidade que a criminalidade se manifesta. Essa deficiência revela não apenas um atraso estrutural, mas também uma lacuna metodológica, pois o aparato jurídico ainda não dispõe de protocolos sólidos para garantir a autenticidade e a integridade de provas digitais. Sousa atesta que:

> A volatilidade dos dados em rede exige que a vítima e as autoridades atuem com celeridade extrema, sob o risco de que as provas da perseguição desapareçam antes mesmo de serem formalizadas no inquérito policial, favorecendo a impunidade do agressor virtual (Sousa, 2024).

A falta de diretrizes para investigações digitais e de cooperação com empresas de tecnologia fomenta a impunidade no ciberespaço. Sem protocolos claros e instrumentos técnicos adequados, a proteção das provas é comprometida, fragilizando a perseguição penal. Essa lacuna institucional ameaça a efetividade da justiça, que se mostra incapaz de acompanhar o ritmo da criminalidade contemporânea.

[5] *Blockchain* é uma tecnologia de registro distribuído que armazena informações em blocos interligados e protegidos por criptografia, formando uma cadeia cronológica imutável. Cada bloco contém dados validados e, uma vez registrado, não pode ser alterado sem comprometer toda a estrutura da rede. Por sua característica de descentralização, transparência e segurança, o *blockchain* tem sido utilizado para garantir a integridade e a autenticidade de informações digitais, inclusive como mecanismo auxiliar na preservação de provas no contexto jurídico.

2.2 A TRANSNACIONALIDADE DO DELITO E A INSUFICIÊNCIA DA ESPECIALIZAÇÃO INSTITUCIONAL

A estrutura da internet, definida pela ausência de limites físicos, apresenta ao Judiciário um dos desafios mais difíceis da atualidade: a deslocalização do crime. No caso do *stalking* digital, é frequente que o agressor recorra a servidores localizados em países estrangeiros ou atue a partir de outras nações para atacar vítimas localizadas no Brasil.

Essa característica transnacional provoca um choque de responsabilidades e uma lentidão burocrática que, na prática, impede a proteção rápida. Rivelli (2025) argumenta que a rapidez das inovações tecnológicas impõe ao Estado o desafio de modernizar as suas estruturas de resposta. Segundo o autor, para que o combate à violência digital seja eficaz, é necessário que os agentes públicos recebam formação especializada para a gestão de evidências eletrônicas, adaptando o sistema de justiça às constantes mudanças desta realidade.

Embora questões internacionais, como a Convenção de Budapeste, tentem uniformizar a colaboração jurídica, a agilidade das respostas governamentais ainda não se iguala à velocidade das trocas de dados digitais, permitindo que o agressor utilize lacunas de soberania para prolongar a violência sem punições.

A maioria das estruturas policiais e judiciárias brasileiras ainda opera de maneira analógica, sem grupos de inteligência que consigam realizar investigações digitais complexas em tempo real. Para investigar um caso de perseguição online, é necessário ter conhecimentos que vão além do campo do Direito, incluindo a análise de metadados, o mapeamento de IPs ocultos e a supervisão de ataques em camadas escondidas da rede.

Quando os sistemas carecem de profissionais capacitados nessas áreas, ocorre uma condução processual inadequada, frequentemente levando ao arquivamento de inquéritos por suposta "falta de autoria", quando, na verdade, a questão é a incapacidade técnica de identificação.

Essa limitação institucional cria um ciclo de vulnerabilidade e reavivamento. De acordo com Rivelli (2025), a violência praticada no meio digital diferencia-se da física pela sua capacidade de ser onipresente e contínua, uma vez que as ferramentas tecnológicas permitem o controle remoto da vítima. Esta nova dimensão do abuso exige que o Direito e as instituições adotem uma perspectiva multidimensional, reconhecendo que a dignidade humana deve ser protegida com o mesmo rigor tanto no espaço físico quanto no digital.

O possível déficit de conhecimento técnico entre juízes e delegados pode resultar em interpretações equivocadas sobre a seriedade das ações, fazendo com que a perseguição online seja vista como meros "incômodos do dia a dia", ignorando o profundo impacto psicológico e a limitação da liberdade da vítima. Sem investimentos em capacitação contínua e no estabelecimento de varas especializadas que entendam a dinâmica do ciberespaço, o sistema jurídico permanece vulnerável ao

desatualismo. Assim, a falha na proteção legal não provém apenas do texto legislativo, mas da carência de uma estrutura estatal que consiga transformar rastros digitais em uma resposta punitiva concreta, assegurando a preservação da dignidade humana tanto no ambiente físico quanto no virtual.

3 A LEI MARIA DA PENHA FRENTE AO *STALKING*

Embora a Lei nº 11.340/2006, que é popularmente chamada de Lei Maria da Penha, represente um grande progresso na legislação brasileira, sua aplicação no ambiente digital atual mostra preocupações sérias que afetam a segurança das mulheres. Criada em uma época em que a violência doméstica era principalmente vinculada a espaços físicos e interações presenciais. Rivelli declara:

> A teoria do Ser Humano Digital propõe uma nova abordagem para entender as complexidades do indivíduo na era digital. Nela, o ser humano é visto como uma entidade multidimensional, composta pelas esferas física, biológica, social e digital, que coexistem simultaneamente e se entrelaçam de forma contínua.Essa teoria inovadora ao reconhecer que a experiência do ser humano moderno não pode ser fragmentada em partes isoladas, mas deve ser compreendida em sua totalidade [...] (Rivelli, 2025, p. 72).

Essa lei enfrenta obstáculos sérios ao lidar com o *stalking* digital, uma forma de perseguição que ignora limites geográficos e se introduz na intimidação da pessoa alvo através de algoritmos e telas. As principais falhas residem na natureza das Medidas Protetivas de Urgência (MPUs), que, em sua concepção, priorizam o afastamento do agressor do lar ou a definição de distâncias a serem mantidas.

No contexto do cibercrime, essas medidas se tornam ineficazes, pois o perseguidor pode realizar vigilância contínua e controle psicológico mesmo a grandes distâncias, utilizando perfis falsos, aplicativos de monitoramento conhecidos como *stalkerwares*[6], ou ações coordenadas em redes sociais que destroem a tranquilidade da vítima sem que o agressor se aproxime fisicamente.

Além do mais, a Lei Maria da Penha requer que exista um relacionamento íntimo, uma situação de coabitação ou um laço familiar para que sua aplicação seja pertinente. Entretanto, o *stalking* digital muitas vezes transcende esses critérios, ocorrendo com pessoas com quem a vítima teve apenas contatos superficiais ou virtuais, o que torna difícil encaixar o caso na legislação específica e pode forçá-lo a seguir o processo comum, frequentemente mais lento e menos protetivo.

Há, ainda, um desafio significativo em termos de provas e fiscalização: enquanto a violação de uma medida de distanciamento físico é facilmente identificável pela ação policial, o descumprimento

[6] O termo ***Stalkerware*** refere-se a softwares de monitoramento ou espionagem utilizados para vigiar a vida privada de uma pessoa através de seus dispositivos (celulares ou computadores) sem o seu consentimento. Diferente de malwares comuns, ele é projetado para operar de forma invisível, permitindo que um terceiro acesse mensagens, fotos, localização em tempo real e até ative a câmera ou o microfone remotamente. É frequentemente associado a contextos de controle e violência doméstica.

digital requer uma perícia técnica avançada e uma agilidade das plataformas tecnológicas em disponibilizar dados de acesso que o sistema judiciário ainda não consegue assegurar.

Essa lentidão nas respostas do Estado e na tecnologia cria uma barreira à proteção, onde uma vítima, mesmo com a proteção de uma decisão judicial, permanece vulnerável a uma violência invisível, mas extremamente prejudicial. Conforme ressaltado por Leila Barros, a Lei Maria da Penha necessita de atualizações que contemplam as novas formas de violência surgidas no ambiente virtual e nos dispositivos tecnológicos (Barros, 2025).

A criminalização da perseguição pela Lei nº 14.132/2021, quando integrada aos mecanismos da Lei Maria da Penha, exige que o Judiciário reconheça o ambiente virtual como uma extensão do espaço privado da vítima. De acordo com a teoria do Ser Humano Digital, as agressões virtuais são onipresentes e atemporais, permitindo que o agressor atualize um controle remoto e constante que ignora fronteiras físicas.

Portanto, a proteção jurídica deve ser multidimensional, garantindo que a dignidade da pessoa humana seja preservada tanto no campo analógico quanto nas interações digitais. Para que o enfrentamento ao *cyberstalking* seja eficaz, as medidas protetivas de urgência precisam evoluir para incluir bloqueios de estruturas de rede e a interrupção de interferências digitais.

A aplicação conjunta da legislação penal com o Marco Civil da Internet é fundamental para neutralizar ferramentas de vigilância, como o uso de *spywares*[7] para monitoramento ilícito. Essa reinterpretação dos mecanismos de proteção busca garantir que o afastamento do agressor seja real, impedindo que a tecnologia seja utilizada como um instrumento de perpetuação do abuso doméstico

3.1 DA INSTRUÇÃO PROBATÓRIA E A CADEIA DE CUSTÓDIA DIGITAL

A mudança da busca no espaço físico para o digital apresenta ao Direito Processual Penal o desafio de lidar com provas que são imateriais, instáveis e facilmente modificáveis. A preservação da prova digital é o maior desafio processual no *stalking*.

Conforme leciona Penteado (2025), a cadeia de custódia da prova digital deve seguir etapas rigorosas de isolamento e fixação para que o vestígio eletrônico não perca sua validade jurídica diante de sua volatilidade intrínseca, no caso do *stalking*, as evidências digitais frequentemente representam o único vestígio do crime.

Contudo, o emprego de capturas de tela como forma exclusiva de prova tem sido alvo de múltiplas críticas e reavaliações pelo Superior Tribunal de Justiça. A Corte observa que a impressão não assegura a integridade, pois não retém metadados nem confirma que uma conversa não foi alterada

[7] ***Spyware***: Um tipo de software malicioso (malware) concebido para se infiltrar num dispositivo, recolher dados confidenciais e monitorizar as atividades do utilizador sem o seu consentimento. As informações recolhidas, como palavras-passe, dados bancários ou hábitos de navegação, são posteriormente transmitidas a entidades externas para fins ilícitos ou publicitários.

ou que partes do contexto não foram eliminadas. Portanto, a insuficiência de proteção jurídica no ambiente digital se reflete na falta de métodos viáveis para manter a cadeia de custódia.

A título de ilustração prática da fragilidade probatória discutida, destaca-se o entendimento firmado pelo Superior Tribunal de Justiça no Recurso em Habeas Corpus nº 133.430/PE. No referido julgamento, a Sexta Turma decidiu, por unanimidade, pela invalidade de capturas de tela (prints) obtidas através do WhatsApp Web como prova exclusiva da materialidade delitiva.

O fundamento central da Corte referia-se à impossibilidade de garantir a integridade da cadeia de custódia, uma vez que a ferramenta permite a exclusão seletiva de mensagens sem que se deixem vestígios da alteração no fluxo comunicativo original. Essa vulnerabilidade técnica compromete o acervo do probatório, inviabilizando a verificação da cronologia dos fatos e violando o contraditório e a ampla defesa no processo penal.

Este precedente jurisprudencial ratifica a tese de que a mera reprodução visual de diálogos digitais, desprovida de metadados ou de espelhamento técnico via perícia oficial, é insuficiente para romper a presunção de inocência, especialmente em crimes de perseguição obsessiva onde o contexto das interações é determinante para a configuração do tipo penal.

Para que uma evidência digital seja considerada confiável, é necessário que siga os passos de isolamento, fixação, coleta, transporte, processamento, armazenamento e descarte, conforme estipulado no Pacote Anticrime[8]. Contudo, a realidade enfrentada por vítimas de *stalking* é marcada pela falta de conhecimento técnico. Muitas vezes, ao excluir mensagens por medo ou exaustão emocional, a vítima acaba comprometendo a prova do crime. Segundo aduz Sousa:

> A instrução probatória no crime de fiscalização digital exige um rigoroso respeito à cadeia de custódia, uma vez que a prova eletrônica é marcada por uma fragilidade intrínseca. Sem o devido espelhamento e a preservação de metadados, as impressões de tela isoladas tornam-se insuficientes no processo penal, pois não garantem a inalterabilidade do conteúdo, dificultando a demonstração da autoria e da materialidade delitiva perante o juízo (Sousa, 2024).

Além disso, a obtenção de provas técnicas indiscutíveis, como a salvaguarda de dados através de *blockchain* ou a formalização de atos por notários, implica gastos elevados, limitando o acesso à justiça e aumentando a vulnerabilidade de mulheres que não possuem recursos financeiros. Outro desafio é a identificação do autor.

O emprego de redes de anonimato e a lentidão dos provedores em cumprir com ordens judiciais que solicitam a quebra de sigilo de dados frequentemente levam à prescrição da ação penal ou à perda

[8] O chamado *Pacote Anticrime* refere-se ao conjunto de alterações legislativas introduzidas pela Lei nº 13.964/2019 no ordenamento jurídico brasileiro, com o objetivo de aprimorar o combate à criminalidade e tornar mais eficiente o sistema de justiça penal. A norma promoveu mudanças no Código Penal, no Código de Processo Penal e em legislações especiais, destacando-se a inclusão de regras sobre a cadeia de custódia da prova, mecanismos de acordo de não persecução penal e medidas voltadas ao enfrentamento da criminalidade organizada.

do foco da investigação. A instabilidade dos dados requer uma intervenção imediata que o sistema judiciário, com sua atual burocracia, não consegue oferecer.

Assim, a proteção legal se torna ineficaz, não por falta de tipificação, mas pela incapacidade do Estado de converter o vestígio digital em prova válida em juízo, perpetuando uma situação de impunidade onde o infrator se oculta na imaterialidade dos dados.

4 PERSPECTIVAS PARA A MODERNIZAÇÃO DO ORDENAMENTO JURÍDICO

A aceleração do progresso tecnológico e a transformação das interações sociais para o ambiente digital apresentam ao sistema jurídico brasileiro um desafio sem precedentes: a substituição de um modelo baseado em analogia por uma estrutura legal que seja dinâmica e resistente. A atualização do sistema jurídico não pode ser vista apenas como uma revisão de normas, mas sim como uma mudança estrutural que assegure a eficácia das leis em um panorama de incerteza tecnológica.

Nesse cenário, quatro abordagens principais se destacam como fundamentais para essa mudança: a adoção da neutralidade em tecnologia, a capacitação dos servidores públicos, o fortalecimento da colaboração internacional e a implementação do letramento digital como uma diretriz do Estado. Em primeiro lugar, é relevante que a formulação de leis passe a considerar o princípio da neutralidade em tecnologia.

Normas que se relacionam a ferramentas, programas ou plataformas específicas rapidamente se tornam obsoletas; o enfoque do legislador deve estar na conduta e na proteção do bem jurídico, possibilitando uma norma que seja suficientemente versátil para incluir tecnologias ainda não inventadas. Em segundo lugar, a modernização exige a especialização técnica do governo.

A criação de varas e áreas dedicadas a crimes digitais, com peritos capacitados para analisar cadeias de custódia em *blockchain* e monitorar ativos digitais, é o que distingue a intenção legislativa da real eficácia processual. Sem uma estrutura de perícia sólida, o sistema judicial continuará a enfrentar problemas de impunidade devido à fragilidade das evidências digitais.

A terceira abordagem é a necessidade de uma colaboração internacional simplificada. Dado que crimes digitais, como *stalking* e fraudes complexas, ocorrem de maneira transnacional, o Brasil deve implementar acordos, como a Convenção de Budapeste, com maior rapidez, facilitando a troca de informações entre diferentes jurisdições. Por fim, a modernização da legislação também envolve um aspecto educacional. Conforme assevera Rivelli:

> A modernização do ordenamento jurídico não deve se restringir à criação de novos tipos penais, mas sim à construção de uma hermenêutica que compreenda a ubiquidade do ambiente digital. É imperativo que o Direito evolua para reconhecer a dignidade do 'ser humano digital', garantindo que as proteções fundamentais [...] sejam eficazes contra formas contemporâneas de invisibilidade e controle tecnológico (Rivelli, 2025).

Para equilibrar privacidade e punição eficaz, é necessário compreender bem os mecanismos de controle e supervisão. Dessa forma, o Direito deixa de ser passivo diante das inovações tecnológicas e passa a atuar ativamente na promoção da segurança jurídica, protegendo a dignidade humana tanto no mundo físico quanto no digital.

4.1 DA REATIVIDADE À RESILIÊNCIA: ESTRATÉGIAS PARA A EFETIVIDADE DO ORDENAMENTO NO CIBERESPAÇO

A passagem da sociedade para uma conectividade intensa e contínua exige que o Direito brasileiro deixe de lado sua abordagem tradicionalmente reativa. Tradicionalmente, o sistema jurídico atua com uma lógica de "pós-fato", onde a norma é criada apenas como reação a conflitos que já foram estabelecidos. Conforme esclarece Fachin e Rocha:

> Para que o alcance jurídico efetividade no ciberespaço, a regulação não pode se limitar ao modelo tradicional de normas impositivas. É necessária uma estratégia de regulação multinível, que combine a legislação estatal (o Direito), as normas sociais, as forças de mercado e, fundamentalmente, a arquitetura do sistema (o código). Como assevera *Lawrence Lessig,* 'o código é a lei', o que implica que a proteção dos direitos no ambiente virtual depende de como as plataformas e os protocolos são para impedir abusos ou garantir a privacidade (Fachin; Rocha, 2021).

Contudo, a rapidez das mudanças digitais torna esse modelo ineficaz, pois no tempo necessário para a criação de uma nova lei, uma tecnologia que essa norma buscava regular já pode ter se tornado ultrapassada. Para lidar com perseguições digitais e outras formas de crimes cibernéticos, é fundamental que o sistema se desenvolva para um estado que mantenha sua resiliência, assegurando autoridade e eficácia, independentemente das ferramentas que o agressor possa usar.

Fachin e Rocha (2021) defendem que a regulação do ciberespaço exige uma superação da soberania estatal territorial. Para os autores, a proteção dos direitos e a segurança digital depende de uma gestão multissetorial que integra o Direito aos códigos tecnológicos e às forças de mercado.

O legislador deve evitar a tentação de descrever técnicas específicas, concentrando-se na essência da conduta e na proteção do bem jurídico, como a liberdade e a privacidade das mulheres. Uma legislação resiliente é aquela que não se torna ineficaz com a troca de uma rede social por outra ou com o aparecimento de novas formas de comunicação criptografada.

Ao focar em comportamentos obsessivos e nos danos provocados, a norma continua a ser relevante e válida ao longo do tempo, garantindo que o Direito não se torne um observador tardio das inovações. Essa neutralidade tecnológica permite que o arcabouço jurídico mantenha sua força impositiva e eficácia social, independentemente do surgimento de novas plataformas digitais ou métodos de ocultação.

Além de uma adaptação nas normas, a efetividade no ciberespaço requer a atualização do aparato estatal. A resiliência do sistema jurídico é avaliada durante a fase de coleta de provas: sem peritos qualificados em análise de metadados, rastreamento de ativos em *blockchain* e conservação de provas digitais efêmeras, a lei se transforma em uma "folha de papel" sem aplicação prática.

A especialização dos tribunais e do Ministério Público não é apenas um aspecto técnico, mas a base que garante segurança jurídica na era digital. Sem esse suporte, a impunidade nos ambientes digitais continuará a minar a confiança nas instituições. Além disso, essa especialização fortalece a capacidade do Estado de responder de forma ágil e eficaz às novas formas de criminalidade digital. Conforme afirmam Fachin e Rocha:

> O ciberespaço, por sua natureza desterritorializada, desafia a noção clássica de soberania, pois as infraestruturas, os dados e os agentes de um mesmo evento jurídico podem estar dispersos em múltiplas jurisdições simultaneamente. Essa característica impõe a necessidade de mecanismos de cooperação internacional que superem a lentidão dos métodos rogatórios tradicionais, sob pena de tornar inócua a pretensão punitiva estatal diante da violência das evidências digitais (Fachin; Rocha, 2021).

A resiliência jurídica deve ser internacional e educativa, contra crimes digitais exige colaboração internacional ágil, superando burocracias para igualar a velocidade dos agressores. Para garantir a proteção da dignidade humana no ambiente virtual, é essencial unir legislações flexíveis, perícia especializada e a alfabetização digital dos profissionais do Direito.

5 A INSTITUIÇÃO DAS MEDIDAS PROTETIVAS DIGITAIS NA LEI MARIA DA PENHA

A atualização da Lei Maria da Penha é essencial diante da Antinomia Jurídica Digital. O descompasso ocorre porque a Lei nº 11.340/2006 foi criada antes da era das redes sociais, em um contexto em que a violência dependia da presença física do agressor. Como destaca a Comissão de Constituição e Justiça do Senado, a inclusão da violência digital na Lei Maria da Penha busca justamente corrigir essa lacuna, reconhecendo práticas como perseguição online e exposição da intimidade como formas de agressão que necessitam de tutela jurídica específica (TV Senado, 2025).

No cenário atual, as medidas protetivas que incluem "proibição de contato por qualquer meio" se mostram amplas e inadequadas, permitindo que o agressor explore lacunas tecnológicas, como o uso de mensagens via transações "PIX", notificações de aplicativos de entrega ou comentários em jogos, a fim de continuar o abuso psicológico da vítima.

Assim, a formulação precisa das ações digitais proibidas é essencial para assegurar a eficácia da proteção judicial, evitando que a tecnologia sirva como um meio de impunidade. Nesse contexto, a articulação entre a defesa dos direitos das mulheres e o Marco Civil da Internet (Lei nº 12.965/14) se torna um elemento fundamental. A sugestão de adiar a remoção de conteúdos não pretende alterar a

responsabilidade civil das plataformas, mas sim considerar que, em situações de violência doméstica, o risco associado ao tempo é essencial para a saúde mental e emocional da vítima.

Agir rapidamente na exclusão de informações expostas ou ofensivas é uma ação essencial para minimizar danos antes de uma discussão mais profunda sobre o tema, assegurando que o ambiente online não continue sendo um local de revitimização constante. Para garantir que essa proteção seja eficaz, é necessário que a decisão judicial inclua a exigência de manter os registros de acesso e conexão.

A proteção da cadeia de custódia é vital para evitar que o agressor, ao ser informado da medida protetiva, destrua as provas digitais que demonstram a autoria e a gravidade do *stalking*. Dessa forma, a evidência digital é resguardada para processos futuros, enfrentando a instabilidade natural dos dados eletrônicos. Por fim, a proposta de reforma legislativa visa estabelecer o conceito de "Distância Digital".

Assim como a lei define uma distância física de afastamento (como 300 metros de uma residência), deve-se introduzir a necessidade de um limite virtual. A literatura contemporânea chama essa forma de proteção de Inviolabilidade do Domicílio Virtual. Conforme destaca a Constituição Federal de 1988, “a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador” (art. 5º, XI), princípio que pode ser reinterpretado para abranger também os espaços digitais, garantindo a proteção da esfera íntima no ambiente virtual. Fachin e Rocha asseveram que:

> A proteção dos direitos da personalidade no ciberespaço exige o reconhecimento de que a vida privada e a intimidade não se limitem ao espaço físico, mas se estende às questões digitais do indivíduo. Assim, a garantia constitucional da inviolabilidade do domicílio deve ser interpretada de forma extensiva para abranger o 'domicílio digital', assegurando que a esfera íntima do sujeito seja preservada contra invasões, monitoramentos e perseguições indesejadas que ocorrem por meio de dispositivos tecnológicos (Fachin; Rocha, 2021).

Nesse sentido, o agressor deve ser impedido de estar "digitalmente presente" na vida da mulher, garantindo a autodeterminação informativa e a privacidade da vítima. Apenas através dessa atualização legal será possível adaptar a eficácia da Lei Maria da Penha ao século XXI, fechando a lacuna entre a norma rígida e a rápida evolução dos crimes virtuais.

6 CONCLUSÃO

O estudo realizou mostra que a Lei Maria da Penha, apesar de constituir um marco na proteção das mulheres contra a violência doméstica e familiar, revela-se insuficiente frente às novas modalidades de agressão que surgem no universo digital. O stalking virtual, definido pela perseguição obsessiva, pela invasão de privacidade e pelo controle psicológico mediante o uso de tecnologias,

evidencia falhas no ordenamento jurídico que enfraquecem a proteção das vítimas e alimentam a sensação de impunidade.

Nesse cenário, a Lei nº 14.132/2021 representa um progresso significativo ao tipificar o crime de perseguição (stalking) no Código Penal, ampliando a tutela penal e reconhecendo a gravidade de condutas reiteradas, inclusive no meio digital. A investigação indicou que as medidas protetivas originalmente previstas na Lei nº 11.340/2006 foram pensadas para situações físicas e presenciais, mostrando-se ineficazes quando aplicadas ao ciberespaço.

A exigência de relacionamentos próximos ou familiares para a aplicação da lei, combinada com os desafios de provar os casos e a falta de especialização técnica nas instituições, restringe a eficácia da reação estatal. Ademais, as decisões judiciais recentes evidenciam a fragilidade da cadeia de custódia digital, o que destaca a necessidade de instrumentos mais sólidos para garantir a autenticidade das provas, mesmo com a tipificação apresentada pela Lei nº 14.132/2021.

A implementação de medidas protetivas digitais específicas constitui um passo necessário para alinhar a legislação às novas dinâmicas da era digital, em harmonia com os progressos já realizados pela Lei nº 14.132/2021. Igualmente, é essencial investir na formação contínua dos profissionais do direito, na colaboração internacional para enfrentar crimes transnacionais e na promoção da educação digital como uma política pública.

Portanto, a proteção das mulheres contra o assédio digital demanda uma abordagem holística: atualização das leis, fortalecimento das instituições e aumento da conscientização social, com a implementação de políticas públicas eficazes voltadas à prevenção e ao enfrentamento dessa forma de violência.

Por meio de um sistema jurídico resiliente, que consiga integrar normas como a Lei Maria da Penha e a Lei nº 14.132/2021, antecipar riscos e reagir rapidamente às novas formas de violência, será possível assegurar a dignidade humana e garantir que o ambiente digital não se torne um local de vulnerabilidade, mas sim de liberdade e segurança.

REFERÊNCIAS

AZEREDO, C. M. de O.; CARLOS, P. P. de; WENDT, E. A internet e a violência contra a mulher: uma análise sobe a aplicação da Lei Maria da Penha aos casos de violência psicológica no contexto virtual. Revista Brasileira de Ciências Criminais, São Paulo, v. 24, n. 119, p. 305-326, mar./abr. 2016.

DIAS, M. B. Lei Maria da Penha: a efetividade da Lei 11.340/2006 de combate à violência doméstica e familiar contra a mulher. 4. ed. São Paulo: Revista dos Tribunais, 2015.

FIORILLO, C. P.; CONTE, C. P. Crimes no meio ambiente digital. 2. ed. São Paulo: Saraiva, 2016.

FREITAS, V. P. de. A tecnologia vai impactar o Direito e seus profissionais. Conjur, ago. 2017. Disponível em: <http://www.conjur.com.br/2017-ago-06/segunda-leitura tecnologiaimpactar-direito-profissionais>. Acesso em: 06 abril 2025.

BARROS, Francisco Dirceu. Estudo doutrinário do stalking (crime de perseguição persistente, novo art. 147 – A do Código Penal). GenJurídico, São Paulo, 2021. Atualidades, Penal. Disponível em: <http://genjuridico.com.br/2021/04/05/estudo-doutrinario-dostalking/>Acesso em: 16 fev. 2025.

BRASIL. Superior Tribunal de Justiça. Recurso em Habeas Corpus nº 133.430/PE. Relator: Ministro Nefi Cordeiro, Sexta Turma, em julgado 02/09/2021. Brasília, DF: STJ, 2021.

CASSANTI, Moacir. Crimes cibernéticos: o crime de computador e a prova pericial. 2. ed. Curitiba: Juruá, 2024.

CRESPO, Marcelo Xavier de Freitas. Crimes digitais: uma análise jurídica. São Paulo: Saraiva, 2023.

LIMA, Renato Brasileiro de. Manual de processo penal: volume único. 13. ed. Salvador: JusPodivm, 2025.

PENTEADO, Walter Barbosa. Cadeia de custódia da prova digital. 2. ed. São Paulo: Thomson Reuters Brasil, 2025.

SANTOS, Ivana David. Stalking e o Direito Penal brasileiro. 2. ed. Rio de Janeiro: Lumen Juris, 2024.

BRASIL. Senado Federal. Comissão de Constituição e Justiça. CCJ aprova inclusão de violência digital na Lei Maria da Penha. Brasília: TV Senado, 01 out. 2025. Disponível em:https://www12.senado.leg.br/noticias/materias/2025/10/01/ccj-projeto-inclui-violencia-digital-contra-mulher-nos-crimes-previstos-na-lei-maria-da-penhaAcesso em: 15 de março de 2026.

BARROS, Esther Brisa da Silva; OLIVEIRA, Lucas Lucena. Políticas públicas de proteção às mulheres vítimas de violência doméstica: uma análise vitimológica e criminal sob a realidade brasileira. Lumen et Virtus, São José dos Pinhais, v. 47, pág. 4369-4383, abr.2025.

BARBOSA, Yêda Maria Ferreira. Stalking digital e tutela jurídica na violência contemporânea. Migalhas, 17 dez. 2025. Disponível em:https://www.migalhas.com.br/depeso/446011/stalking-digital-e-tutela-juridica-na-violencia-contemporanea. Acesso em: 20 de março de 2026.

SENADO FEDERAL. CCJ: projeto inclui violência digital nos crimes previstos na Lei Maria da Penha. Senado Notícias, Brasília, 1 out. 2025. Disponível em: https://www12.senado.leg.br/noticias/materias/2025/10/01/ccj-projeto-inclui-violencia-digital-contra-mulher-nos-crimes-previstos-na-lei-maria-da-penha Acesso em: 21 de março de 2026.

OLIVEIRA FILHO, Mário de. O impacto da falta de especialização em gênero no sistema de justiça brasileiro. LinkedIn, 2024. Disponível em:https://pt.linkedin.com/pulse/o-impacto-da-falta-de-especializa%C3%A7%C3%A3o-em-brasil-m-sc-3qexf. Acesso em: 21 de março de 2026.

SOUZA, Sandyluana Nascimento. A eficácia da proteção jurídica contra o crime de perseguição no Brasil: desafios na aplicação da lei 14.132/2021 no meio digital. Revista FT, v. 132, 2024. Disponível em:https://revistaft.com.br/a-eficacia-da-protecao-juridica-contra-o-crime-de-perseguicao-no-brasil-desafios-na-aplicacao-da-lei-14-132-2021-no-meio-digital/. Acesso em: 22 de março de 2026.

RIVELLI, Fabio. A violência digital e seus efeitos nas vítimas: desafios contemporâneos e perspectiva do ser humano digital. Revista de Vitimologia e Justiça Restaurativa, São Paulo, v. 3, pág. 56-71, fev.2025.

FACHIN, Zulmar; ROCHA, Leonardo. Desafios da regulação do ciberespaço e da proteção dos direitos da personalidade. Revista Jurídica (FURB), v. 56, pág. 1-18, jan./abr. 2021.

CASTRO, Ana Lara Camargo De; SYDOW, Spencer Toth. STALKING E CYBERSTALKING: OBSESSÃO, INTERNET, AMEDRONTAMENTO. Belo Horizonte-MG: D'Plácido, 2017. 175 p. v. 2.