ANA VICTÓRIA BATISTA DE SOUSA

O DECRETO Nº 12.976/2026 E O ENFRENTAMENTO DA VIOLÊNCIA CIBERNÉTICA CONTRA A MULHER: AVANÇOS NORMATIVOS E LIMITAÇÕES ESTRUTURAIS

Salvador/BA
2026

ANA VICTÓRIA BATISTA DE SOUSA

O DECRETO Nº 12.976/2026 E O ENFRENTAMENTO DA VIOLÊNCIA CIBERNÉTICA CONTRA A MULHER: AVANÇOS NORMATIVOS E LIMITAÇÕES ESTRUTURAIS

Trabalho de Conclusão de Curso apresentado ao Programa de Pós-graduação em Ciências Criminais, da Universidade Católica do Salvador, como requisito parcial para obtenção do grau de Especialista em Ciências Criminais.

Orientadora: Profª. Mestra Alcilene Coutinho.

Salvador/BA
2026

RESUMO:

O presente trabalho teve como objetivo analisar o Decreto nº 12.976, de 20 de maio de 2026, como marco normativo contemporâneo no enfrentamento da violência cibernética contra a mulher no Brasil, identificando suas principais inovações e as limitações jurídicas e institucionais que podem comprometer sua efetividade. Quanto à metodologia, adotou-se uma abordagem qualitativa, de natureza exploratória e descritiva, baseada em pesquisa bibliográfica e documental. Foram analisados diplomas normativos (Decreto nº 12.976/2026, Lei nº 11.340/2006 e Lei nº 12.965/2014), decisões judiciais do Supremo Tribunal Federal (Temas 533 e 987) e documentos oficiais (dados do Ligue 180, DataSenado e ONU Mulheres), além da doutrina especializada publicada entre 2016 e 2026, consultada nas bases SciELO, Capes Periódicos e Google Acadêmico. Os resultados evidenciaram avanços significativos do Decreto, como a consagração da centralidade da vítima, a vedação à revitimização, a ampliação do conceito de conteúdo íntimo para abranger manipulações por inteligência artificial (*deepfakes*), a responsabilização dos provedores por falha sistêmica, a imposição de prazo de até duas horas para remoção de conteúdo íntimo não autorizado com marcação digital para bloqueio de reenvios, o dever de mitigação proativa do alcance de ataques coordenados independentemente de notificação e a vedação expressa à geração de *deepfakes* de natureza íntima. Paralelamente, identificaram-se limitações estruturais persistentes: dificuldades na produção e validação da prova digital e na observância da cadeia de custódia, anonimato dos agressores, transnacionalidade dos delitos, insuficiência de recursos tecnológicos e de capacitação especializada nas instituições de segurança pública, bem como a dependência da colaboração voluntária das plataformas digitais. Nas considerações finais, conclui-se que, embora o Decreto represente um avanço normativo significativo, sua plena efetividade depende da superação das barreiras institucionais identificadas, o que exige investimentos massivos em perícia digital, capacitação multidisciplinar de agentes públicos, cooperação internacional eficiente e a implementação de políticas públicas integradas, a fim de que o ciberespaço deixe de ser um território de impunidade para a violência de gênero.

Palavras-chave: Decreto nº 12.976/2026; Violência Cibernética; Violência Contra a Mulher; Prova Digital; Limitações Estruturais.

ABSTRACT:

This study aimed to analyze Decree No. 12,976, of May 20, 2026, as a contemporary normative framework in addressing cyber violence against women in Brazil, identifying its main innovations and the legal and institutional limitations that may compromise its effectiveness. Regarding methodology, a qualitative, exploratory, and descriptive approach was adopted, based on bibliographic and documentary research. Normative instruments (Decree No. 12,976/2026, Law No. 11,340/2006, and Law No. 12,965/2014), judicial decisions of the Supreme Federal Court (Themes 533 and 987), and official documents (data from the 180 Helpline, DataSenado, and UN Women) were analyzed, in addition to specialized doctrine published between 2016 and 2026, consulted in the SciELO, Capes Periodicals, and Google Scholar databases. The results highlighted significant advancements in the Decree, such as the establishment of victim-centeredness, the prohibition of revictimization, the expansion of the concept of intimate content to encompass manipulations by artificial intelligence (deepfakes), the accountability of providers for systemic failures, the imposition of a deadline of up to two hours for the removal of unauthorized intimate content with digital tagging to block resending, the duty of proactive mitigation of the reach of coordinated attacks regardless of notification, and the express prohibition of the generation of deepfakes of an intimate nature. In parallel, persistent structural limitations were identified: difficulties in the production and validation of digital evidence and in observing the chain of custody, anonymity of perpetrators, transnationality of the crimes, insufficient technological resources and specialized training in public security institutions, as well as dependence on the voluntary collaboration of digital platforms. In conclusion, although the Decree represents a significant normative advance, its full effectiveness depends on overcoming the identified institutional barriers, which requires massive investments in digital forensics, multidisciplinary training of public agents, efficient international cooperation, and the implementation of integrated public policies, so that cyberspace ceases to be a territory of impunity for gender-based violence.

Keywords: Decree No. 12.976/2026; Cyber Violence; Violence Against Women; Digital Evidence; Structural Limitations.

SUMÁRIO

INTRODUÇÃO

1.1. Contextualização da Violência de Gênero no Ambiente Digital e Delimitação do Problema de Pesquisa

A ampliação do acesso à internet, impulsionada pela popularização de dispositivos eletrônicos cada vez mais acessíveis e pela expansão das redes digitais, contribuiu para a formação de uma sociedade hiperconectada, na qual interações sociais, relações de trabalho, manifestações culturais e práticas cotidianas passaram a ocorrer de forma significativa no ambiente virtual. Nesse cenário, o Direito é constantemente desafiado a se adaptar a novas realidades, buscando acompanhar a velocidade das inovações tecnológicas e garantir a proteção de direitos fundamentais em um espaço marcado pela fluidez, descentralização e complexidade.

Todavia, paralelamente às inegáveis vantagens proporcionadas pela era digital, observa-se a emergência de novas formas de violação de direitos, que se aproveitam das especificidades do ambiente virtual para potencializar práticas ilícitas. A internet, ao mesmo tempo em que amplia possibilidades de comunicação e acesso à informação, também se configura como um espaço propício à prática de crimes, especialmente em razão de fatores como o anonimato, a facilidade de disseminação de conteúdos, a rapidez na propagação de informações e a ausência de fronteiras territoriais (SILVA, 2022). Tais características impõem desafios significativos ao sistema jurídico, que frequentemente se mostra incapaz de responder com a mesma celeridade e eficácia às transformações sociais impulsionadas pela tecnologia (OLIVEIRA; SCHLEMPER, 2025).

A desterritorialização das condutas ilícitas, possibilitada pela conectividade global, representa um dos principais entraves à atuação estatal, uma vez que dificulta a identificação dos autores, a produção de provas e a aplicação de sanções (OLIVEIRA; SCHLEMPER, 2025). A possibilidade de que um agente pratique um delito em um país, utilize servidores localizados em outro e cause danos em múltiplas jurisdições evidencia a complexidade da repressão aos crimes cibernéticos, exigindo mecanismos de cooperação internacional que, muitas vezes, são marcados por entraves burocráticos e morosidade procedimental (OLIVEIRA; SCHLEMPER, 2025). Esse contexto contribui para a ampliação de um cenário de impunidade, no qual a responsabilização dos infratores se torna incerta e, por vezes, inviável (OLIVEIRA; SCHLEMPER, 2025).

No âmbito da violência de gênero, tais desafios assumem contornos ainda mais graves, uma vez que o ambiente digital tem sido amplamente utilizado como instrumento de perpetuação de práticas misóginas e de controle sobre os corpos e a autonomia das mulheres. A violência cibernética contra a mulher manifesta-se por meio de diversas condutas, como a divulgação não consentida de conteúdo íntimo (*revenge porn*), a sextorsão, o estupro virtual e o cyberstalking, configurando formas contemporâneas de agressão que produzem impactos profundos na dignidade, na privacidade e na integridade psicológica das vítimas (SILVA, 2022; OLIVEIRA; SCHLEMPER, 2025). Essas práticas evidenciam a transposição da violência de gênero para o ambiente virtual, demonstrando que o avanço tecnológico não elimina desigualdades estruturais, mas, ao contrário, pode amplificá-las (PNUD, 2023).

Diante desse cenário, a construção de respostas normativas adequadas torna-se imperativa. No contexto brasileiro, o Decreto nº 12.976, de 20 de maio de 2026 (BRASIL, 2026), emerge como um relevante instrumento na tentativa de sistematizar diretrizes voltadas ao enfrentamento da violência cibernética contra a mulher, incorporando princípios como a centralidade da vítima, a vedação à revitimização e o reconhecimento de novas modalidades de agressão mediadas por tecnologias emergentes, como a inteligência artificial e os deepfakes. Trata-se de uma iniciativa que busca alinhar o ordenamento jurídico às novas demandas sociais, promovendo uma abordagem mais estruturada e sensível às especificidades da violência digital de gênero.

Entretanto, a existência de avanços no plano normativo não implica, necessariamente, sua efetividade prática. A complexidade inerente aos crimes cibernéticos revela a persistência de limitações estruturais que desafiam a implementação das medidas previstas, especialmente no que se refere à produção e à validação da prova digital, ao rigor técnico exigido pela cadeia de custódia, à identificação dos agressores e à atuação coordenada entre diferentes instituições. Ademais, a dependência da colaboração de plataformas digitais, aliada à insuficiência de recursos tecnológicos e à carência de capacitação especializada, evidencia a existência de um descompasso entre a sofisticação das práticas ilícitas e a capacidade institucional de enfrentamento (OLIVEIRA; SCHLEMPER, 2025).

Nesse contexto, propõe-se analisar o Decreto nº 12.976/2026 como instrumento normativo de enfrentamento da violência cibernética contra a mulher, identificando suas principais inovações e as limitações jurídicas e institucionais que podem comprometer sua efetividade no contexto brasileiro.

Diante desse cenário, a presente pesquisa parte da seguinte questão central: em que medida o Decreto nº 12.976/2026, responde aos desafios contemporâneos da violência cibernética contra a mulher e quais limitações jurídicas e institucionais podem restringir sua efetividade?

1.2. Justificativa

A escolha do tema justifica-se pela crescente relevância da violência cibernética contra a mulher no contexto da sociedade digital contemporânea, marcada pela intensificação do uso das tecnologias da informação e comunicação. A ampliação do acesso à internet e a popularização das redes sociais, embora tenham proporcionado avanços significativos na democratização da informação, também contribuíram para a expansão de novas formas de violência, que atingem de maneira desproporcional as mulheres, reproduzindo e intensificando desigualdades estruturais de gênero no ambiente virtual.

Nesse cenário, a violência cibernética configura-se como um fenômeno complexo e multifacetado, que desafia os modelos tradicionais de compreensão e enfrentamento da criminalidade. Práticas como a divulgação não consentida de conteúdo íntimo, a sextorsão, o *cyberstalking* e outras formas de agressão digital evidenciam a necessidade de uma abordagem jurídica mais específica e eficaz, capaz de responder às particularidades dessas condutas e aos impactos profundos que produzem na vida das vítimas.

A relevância acadêmica do estudo reside na necessidade de aprofundar a análise sobre a efetividade dos instrumentos normativos recentemente instituídos no ordenamento jurídico brasileiro, em especial o Decreto nº 12.976/2026, que se apresenta como um marco na tentativa de sistematizar diretrizes voltadas ao enfrentamento da violência cibernética contra a mulher. A investigação crítica desse diploma normativo permite identificar não apenas seus avanços, mas também suas limitações estruturais, contribuindo para o aprimoramento do debate jurídico e para o desenvolvimento de soluções mais eficazes.

Sob o ponto de vista social, a pesquisa mostra-se pertinente diante da persistência de elevados índices de violência de gênero, agora potencializados pelo ambiente digital, onde a rapidez na disseminação de conteúdos e a dificuldade de controle ampliam os danos causados às vítimas. A sensação de anonimato e a complexidade técnica envolvida na identificação dos agressores

favorecem a impunidade, reforçando a necessidade de mecanismos mais eficientes de prevenção, investigação e responsabilização.

A gravidade do fenômeno é corroborada por dados oficiais recentes. Em âmbito global, estima-se que 38% das mulheres já sofreram violência online, e menos de 40% dos países dispõem de leis que as protejam contra assédio ou perseguição digital, deixando cerca de 1,8 bilhão de mulheres e meninas sem qualquer proteção legal (ONU MULHERES, 2025). No Brasil, a Central de Atendimento à Mulher – Ligue 180 registrou, em 2025, 155.111 denúncias de violência contra mulheres, um aumento de 17,4% em relação ao ano anterior, sendo que 2,96% dessas violações ocorreram especificamente em ambiente virtual (internet) (BRASIL, 2026). Além disso, a 11ª edição da Pesquisa Nacional de Violência contra a Mulher, realizada pelo DataSenado em 2025, revelou que aproximadamente 8,8 milhões de brasileiras (10% da população feminina com 16 anos ou mais) sofreram algum tipo de violência digital nos últimos 12 meses, com destaque para o envio recorrente de mensagens ofensivas ou ameaçadoras (BRASIL, 2025). Esses números evidenciam a urgência de medidas eficazes de enfrentamento, tornando ainda mais premente a análise crítica do Decreto nº 12.976/2026 e de sua efetividade prática.

Por fim, a presente pesquisa contribui para o fortalecimento das políticas públicas voltadas à proteção das mulheres, ao evidenciar a necessidade de integração entre diferentes atores institucionais, investimento em tecnologia e capacitação especializada dos profissionais envolvidos na persecução penal. Assim, o estudo busca não apenas compreender a dinâmica da violência cibernética de gênero, mas também fomentar reflexões que subsidiem a construção de um ambiente digital mais seguro, justo e igualitário.

1.3. Objetivos

1.3.1. Objetivo geral

O presente trabalho tem como objetivo geral analisar o Decreto nº 12.976/2026 como instrumento normativo de enfrentamento da violência cibernética contra a mulher, identificando suas principais inovações e as limitações jurídicas e institucionais que podem comprometer sua efetividade no contexto brasileiro.

1.3.2. Objetivos específicos

Como objetivos específicos, o presente estudo busca: caracterizar a violência cibernética contra a mulher e suas principais manifestações no contexto da sociedade digital; examinar as inovações introduzidas pelo Decreto nº 12.976/2026 para o enfrentamento da violência cibernética contra a mulher; analisar os desafios relacionados à produção da prova digital, à identificação dos agressores e à responsabilização das plataformas digitais; e, por fim, identificar as limitações jurídicas e institucionais que podem restringir a efetividade do Decreto nº 12.976/2026.

1.4. METODOLOGIA

O presente estudo adota uma abordagem metodológica de natureza qualitativa, pautada pelos objetivos exploratório e descritivo, visando analisar o impacto normativo e as limitações práticas do Decreto nº 12.976/2026. A escolha por este método justifica-se pela necessidade de compreender um fenômeno social e jurídico complexo, que exige uma análise interpretativa das normas e da realidade social em que estão inseridas.

A pesquisa é exploratória por buscar ampliar a compreensão acerca de um fenômeno contemporâneo ainda em processo de consolidação no campo jurídico e nas políticas públicas – a violência de gênero mediada por tecnologias digitais – e descritiva por examinar as características do Decreto, suas diretrizes, mecanismos de proteção e os desafios relacionados à sua implementação.

Quanto aos procedimentos, a pesquisa classifica-se como bibliográfica e documental. A vertente bibliográfica foi realizada a partir do levantamento de marcos teóricos publicados prioritariamente nos últimos dez anos (2016-2026), com consulta às bases SciELO, Capes Periódicos e Google Acadêmico, utilizando os descritores "violência cibernética", "violência de gênero digital", "prova digital" e "cadeia de custódia". Foram selecionados livros, artigos científicos e periódicos especializados sobre violência de gênero e Direito Digital, assegurando a sustentação doutrinária necessária à compreensão dos conceitos fundamentais.

A pesquisa documental concentrou-se na análise de diplomas normativos, atos administrativos e documentos institucionais relacionados ao objeto de estudo, com destaque para o Decreto nº 12.976/2026, a Lei nº 11.340/2006 (Lei Maria da Penha), a Lei nº 12.965/2014 (Marco Civil da Internet) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), além de relatórios e dados produzidos por órgãos públicos e organismos nacionais e internacionais,

tais como Ministério das Mulheres, Senado Federal, Conselho Nacional de Justiça, Fórum Brasileiro de Segurança Pública e ONU Mulheres.

O método de análise adotado foi o dedutivo, partindo da análise geral das evoluções tecnológicas e dos crimes cibernéticos para a análise específica das diretrizes do Decreto. A técnica de interpretação empregada foi a hermenêutica jurídica, orientada pela interpretação sistemática e crítica das normas, buscando compreender sua articulação com os princípios constitucionais, com a legislação infraconstitucional e com os desafios contemporâneos da proteção dos direitos das mulheres no ambiente digital.

Registra-se, por fim, que a recente publicação do Decreto (maio/2026) inviabilizou a análise jurisprudencial, razão pela qual o estudo concentrou-se na interpretação sistemática e nos desafios estruturais apontados pela doutrina. Por se tratar de pesquisa bibliográfica e documental, sem envolvimento direto de seres humanos, não houve necessidade de submissão ao Comitê de Ética em Pesquisa.

2. EVOLUÇÕES DIGITAIS

Para compreender o fenômeno da violência cibernética contra a mulher e os desafios impostos ao Direito no ambiente virtual, faz-se necessário, primeiramente, recuperar a trajetória histórica e tecnológica da internet, bem como a evolução das práticas criminosas que emergiram desse espaço. A compreensão dessas transformações permite situar a violência digital de gênero como um desdobramento contemporâneo de um processo mais amplo de digitalização das relações sociais, que não apenas reproduz, mas também amplifica desigualdades estruturais preexistentes. Assim, este capítulo aborda o surgimento da internet, a evolução dos crimes cibernéticos e, finalmente, as manifestações específicas da violência contra a mulher no ciberespaço, estabelecendo as bases conceituais para a análise do Decreto nº 12.976/2026.

2.1. O surgimento da Internet

A origem da internet remonta ao período da Guerra Fria, quando foi desenvolvida com o objetivo de garantir a comunicação entre bases militares, mesmo diante de eventuais falhas nos sistemas tradicionais. Inicialmente concebida como um projeto estratégico, sua evolução ao longo das décadas possibilitou a ampliação de seu uso para fins acadêmicos, científicos e,

posteriormente, sociais, tornando-se um dos principais instrumentos de comunicação da contemporaneidade (ALMEIDA, 2015).

Com o avanço tecnológico, especialmente a partir da segunda metade do século XX, a internet passou a integrar o cotidiano da sociedade, acompanhando o desenvolvimento de computadores cada vez mais acessíveis e eficientes. No Brasil, sua implementação teve início no final da década de 1980, sendo consolidada nos anos 1990 com a criação da Rede Nacional de Pesquisa (RNP), responsável por estruturar a infraestrutura necessária para a expansão do acesso em âmbito nacional (VIEIRA, 2003).

A partir desse processo de expansão, a internet deixou de ser um recurso restrito a instituições e passou a configurar-se como um espaço global de interação, promovendo transformações significativas nas formas de comunicação, trabalho e sociabilidade. Contudo, esse mesmo ambiente, marcado pela rapidez na circulação de informações e pela facilidade de acesso, também passou a apresentar vulnerabilidades que possibilitaram o surgimento de novas práticas ilícitas, exigindo do Direito constante adaptação para enfrentar os desafios decorrentes da sociedade digital.

2.2. Evolução dos Crimes Cibernéticos

A evolução dos crimes cibernéticos acompanha diretamente o desenvolvimento das tecnologias da informação e a expansão do uso da internet. Os primeiros registros desse tipo de prática remontam às décadas de 1970 e 1980, período em que sistemas informatizados passaram a ser adotados de forma mais ampla por instituições públicas e privadas. Nesse contexto inicial, as condutas ilícitas estavam, em grande parte, associadas a acessos não autorizados realizados por indivíduos motivados pela curiosidade ou pelo desafio técnico, sem, necessariamente, objetivos econômicos ou de causar danos significativos (CAZAROTI; PINHEIRO, 2021).

Com o avanço tecnológico e a crescente interconexão entre sistemas, especialmente a partir da popularização da internet nos anos 1990, os crimes cibernéticos passaram por um processo de transformação, tanto em suas motivações quanto em suas formas de execução. As ações antes pontuais e exploratórias deram lugar a práticas estruturadas, frequentemente voltadas ao lucro, à obtenção indevida de dados e à realização de fraudes. Episódios como a disseminação do *worm Morris* evidenciaram o potencial destrutivo dessas condutas e contribuíram para o reconhecimento da necessidade de mecanismos jurídicos

específicos para seu enfrentamento (CRUZ; RODRIGUES, 2018).

A partir dos anos 2000, com a consolidação da internet como ferramenta essencial para atividades econômicas e sociais, verificou-se um aumento significativo na complexidade dos crimes cibernéticos. A expansão das redes sociais, do comércio eletrônico e dos serviços digitais ampliou o número de potenciais vítimas, ao mesmo tempo em que proporcionou novas oportunidades para a atuação criminosa. Nesse cenário, os delitos passaram a abranger não apenas interesses patrimoniais, mas também violações à honra, à privacidade e à dignidade dos indivíduos (SOUZA; CERVINSKI, 2021).

Paralelamente, o ambiente digital favoreceu o surgimento de condutas ilícitas de natureza interpessoal, como o *cyberbullying*, a difamação e a exposição indevida de informações pessoais, refletindo transformações nas formas de interação social. Essas práticas evidenciam que os crimes cibernéticos não se limitam a danos materiais, mas podem gerar consequências profundas na esfera psicológica e social das vítimas (HERNANDEZ; DE TOLEDO, 2021).

Além disso, a globalização da internet introduziu desafios adicionais à repressão dessas condutas, especialmente no que se refere à jurisdição e à cooperação internacional. A possibilidade de que crimes sejam praticados em múltiplos territórios, com utilização de servidores distribuídos globalmente, dificulta a identificação dos autores e a efetiva aplicação da lei penal, contribuindo para a sensação de impunidade (LIMA et al., 2022).

Nesse contexto evolutivo, observa-se que os crimes cibernéticos passaram a incorporar, de forma cada vez mais evidente, práticas de violência de gênero, especialmente direcionadas às mulheres. O ambiente digital, marcado pelo anonimato e pela rápida disseminação de conteúdos, tornou-se um espaço propício para a reprodução e amplificação de condutas misóginas, evidenciando a necessidade de respostas jurídicas mais específicas e eficazes, como aquelas propostas pelo Decreto nº 12.976, de 20 de maio de 2026.

2.3. Violência cibernética contra a mulher

A violência contra as mulheres revela-se como um fenômeno estrutural e multifacetado, que ultrapassa as barreiras do espaço físico e se projeta, com intensidade crescente, no ambiente virtual. Nesse contexto, observa-se que, além de historicamente serem vítimas de diversas formas de violência no mundo concreto, as mulheres passaram a ocupar posição de destaque também como principais alvos de ataques no ciberespaço. Dados apresentados por

MONTEIRO (2019, p. 8) evidenciam essa realidade ao demonstrar que, no Estado do Espírito Santo, Brasil, entre os anos de 2016 e 2018, aproximadamente 86% dos crimes cibernéticos tiveram o gênero feminino como vítima, o que reforça o caráter seletivo e estrutural dessas práticas.

No ambiente digital, a violência assume contornos ainda mais severos, sobretudo em razão da velocidade de propagação das informações e da amplitude do alcance dos conteúdos. Em questão de minutos, uma vítima pode ser exposta a situações de humilhação perante familiares, amigos e um número indeterminado de indivíduos, ampliando significativamente os danos à sua honra, imagem e integridade psicológica. Tal cenário evidencia que o ciberespaço não apenas reproduz as desigualdades de gênero existentes na sociedade, mas também potencializa suas consequências.

As transformações decorrentes do avanço das tecnologias da informação têm provocado profundas mudanças na organização social contemporânea, gerando um descompasso entre os institutos tradicionais do Direito e as novas demandas emergentes da era digital. Conforme destaca PINHEIRO (2012), a evolução tecnológica criou um verdadeiro hiato entre a dinâmica social e a capacidade de resposta do ordenamento jurídico. Assim, a mesma tecnologia que se apresenta como ferramenta essencial para o desenvolvimento humano também se converte em instrumento de perpetuação da violência de gênero, sem que, até o momento, tenham sido plenamente implementados mecanismos eficazes para seu enfrentamento.

Com a popularização da internet, das redes sociais e dos dispositivos móveis, a violência contra a mulher passou a contar com novos meios de execução, tornando-se mais sofisticada, silenciosa e de difícil repressão. Diariamente, inúmeras mulheres são vítimas de práticas criminosas no ambiente digital, frequentemente motivadas por sentimentos de ódio, vingança ou interesses econômicos (SANTOS et al., 2024). Nesse cenário, destacam-se condutas como a pornografia de vingança (*revenge porn*), caracterizada pela divulgação não autorizada de conteúdos íntimos com o intuito de expor e constranger a vítima; a sextorsão, que consiste na obtenção e utilização de material íntimo mediante ameaça de divulgação para fins de coação (SANTOS et al., 2024); e o chamado estupro virtual, entendido como a imposição de atos de natureza sexual por meio de coerção no ambiente digital, ainda que sem contato físico direto (GONÇALVES, 2024). Tais práticas evidenciam a necessidade de constante atualização do Direito Penal frente às novas formas de violação de direitos fundamentais.

Nesse sentido, Fiorillo e Conte (2016, p. 17) ressaltam que o Direito deve acompanhar as transformações sociais, sob pena de perder sua função primordial de regular as relações humanas e assegurar a convivência social. Para os autores, a relação entre Direito e Internet não se trata de fenômeno transitório, mas de uma realidade consolidada que exige análise aprofundada e atuação efetiva por parte das ciências jurídicas, especialmente no que diz respeito à proteção e à efetivação de direitos fundamentais.

Entretanto, observa-se que ainda há significativa dificuldade no reconhecimento dessas práticas como formas legítimas de violência contra a mulher. Muitas condutas são naturalizadas ou minimizadas, variando desde comportamentos aparentemente simples, como o controle de senhas e acessos pessoais, até práticas mais graves, como a exigência de envio de conteúdos íntimos ou a imposição de atos de natureza sexual por meio de plataformas digitais. Tal invisibilização contribui para a perpetuação dessas violências e para a manutenção de um cenário de impunidade (VERAS, 2020).

Ademais, essas práticas frequentemente se inserem em uma lógica de dominação marcada por desigualdades de gênero, na qual o agressor se aproveita, muitas vezes, de maior conhecimento tecnológico para exercer controle, coerção e violência psicológica sobre a vítima (GONÇALVES, 2024). Essa assimetria de poder reforça a vulnerabilidade feminina no ambiente digital e evidencia a necessidade de medidas específicas de proteção e repressão.

Diante desse panorama, torna-se imprescindível a análise crítica das novas formas de violência contra a mulher no ciberespaço, bem como a investigação das lacunas existentes no ordenamento jurídico. A complexidade dessas condutas, aliada à rapidez com que se transformam, exige respostas jurídicas igualmente dinâmicas e eficazes, capazes de garantir não apenas a punição dos agressores, mas também a proteção integral das vítimas.

3. O DECRETO Nº 12.976/2026 E O ENFRENTAMENTO DA VIOLÊNCIA CIBERNÉTICA CONTRA A MULHER

O Decreto nº 12.976, de 20 de maio de 2026, representa a mais recente e abrangente iniciativa normativa do Estado brasileiro voltada ao enfrentamento da violência cibernética contra a mulher. Editado no âmbito das ações do Pacto Nacional Brasil Contra o Feminicídio, o diploma reconhece a urgência de se adaptar o ordenamento jurídico às novas formas de agressão mediadas pelas tecnologias digitais, que reproduzem e amplificam as desigualdades de gênero no ambiente virtual. Este capítulo dedica-se à análise sistemática do Decreto,

dividindo-se em quatro eixos principais: (i) o diálogo normativo com a Lei Maria da Penha e o Marco Civil da Internet; (ii) os princípios orientadores e as definições trazidas pela norma; (iii) a responsabilização dos provedores de aplicações de internet, incluindo os procedimentos de notificação, remoção de conteúdo e mitigação de alcance; (iv) a vedação à geração e modificação de conteúdo íntimo por inteligência artificial. Ao final, apresenta-se uma síntese dos avanços normativos identificados, que servirá de base para a discussão, no capítulo seguinte, das limitações estruturais que desafiam a efetividade prática do Decreto.

3.1. Diálogo normativo com a Lei Maria da Penha e o Marco Civil da Internet

O Decreto nº 12.976/2026 não surge em um vácuo legislativo, mas dialoga diretamente com dois marcos normativos fundamentais do ordenamento jurídico brasileiro: a Lei nº 11.340/2006 (Lei Maria da Penha) (BRASIL, 2006) e a Lei nº 12.965/2014 (Marco Civil da Internet) (BRASIL, 2014). Essa integração normativa é essencial para a compreensão sistemática do enfrentamento à violência cibernética contra a mulher, uma vez que o novo decreto complementa, sem revogar ou substituir, os diplomas anteriores.

A Lei Maria da Penha, reconhecida internacionalmente como um dos mais avançados instrumentos de proteção à mulher **(**INSTITUTO MARIA DA PENHA, s.d.), prevê cinco formas de violência: física, psicológica, sexual, patrimonial e moral (Art. 7º , Lei nº 11.340/2006). Embora elaborada em um contexto anterior à ampla disseminação das tecnologias digitais, suas disposições são plenamente aplicáveis às condutas perpetradas no ambiente virtual. O cyberstalking, por exemplo, configura-se como violência psicológica, ao passo que a sextorsão e a divulgação não consentida de conteúdo íntimo podem ser enquadradas como violência sexual e moral, respectivamente (PADILHA; GOULART, 2025). Nesse sentido, o Decreto nº 12.976/2026 atua como norma complementar, explicitando procedimentos e diretrizes específicos para a aplicação da Lei Maria da Penha no ciberespaço, sem com ela concorrer ou estabelecer antinomias.

Por sua vez, o Marco Civil da Internet estabelece os princípios, garantias e deveres para o uso da internet no Brasil, incluindo a disciplina da responsabilidade dos provedores por conteúdo gerado por terceiros. Em sua redação original, o Art. 19 do Marco Civil condiciona a responsabilização dos provedores ao descumprimento de ordem judicial específica (BRASIL, 2014), o

que, na prática, gerava lentidão na remoção de conteúdos ilícitos e dificultava a proteção urgente das vítimas. O Decreto nº 12.976/2026 inova ao introduzir o conceito de "falha sistêmica" (Art. 4º), que permite a responsabilização extrajudicial dos provedores quando não comprovarem a adoção de medidas adequadas de prevenção ou remoção de conteúdos criminosos. Essa alteração representa um significativo avanço em relação ao regime anterior, ao mesmo tempo em que respeita os princípios constitucionais da liberdade de expressão e da vedação à censura prévia.

Dessa forma, o Decreto nº 12.976/2026 não substitui a Lei Maria da Penha nem o Marco Civil da Internet, mas com eles estabelece um diálogo normativo de complementaridade, preenchendo lacunas procedimentais e adaptando o ordenamento jurídico às especificidades da violência digital de gênero. A aplicação conjunta desses diplomas exige do operador do direito uma interpretação sistemática e integrada, que considere a proteção integral da mulher como vetor axiológico fundamental.

3.2. Princípios orientadores e definições

A gênese do Decreto nº 12.976/2026 está intrinsecamente ligada às ações do Pacto Nacional Brasil Contra o Feminicídio (BRASIL, 2024), representando o compromisso estatal em expandir a rede de proteção às mulheres para o espaço virtual. A norma reconhece que as agressões digitais são, muitas vezes, o prelúdio ou o agravamento da violência física (PADILHA; GOULART, 2025), o que justifica a necessidade de uma intervenção jurídica específica e célere.

Nesse cenário, o Decreto estrutura-se sobre um conjunto de princípios orientadores que visam a uma abordagem mais humanizada e eficaz. Conforme o Art. 2º do diploma normativo (BRASIL, 2026), destacam-se a não discriminação em razão da condição do sexo feminino, a centralidade da vítima, a proteção de dados e da privacidade, a não revitimização e o reconhecimento da discriminação por múltiplos critérios como fator de agravamento da violência. Esses princípios são cruciais para garantir que as ações de prevenção e sanção sejam pautadas pelo respeito à dignidade da mulher (DIAS, 2024).

É importante ressaltar que, embora a norma utilize a terminologia técnica de "divulgação não consentida de conteúdo íntimo", tal fenômeno é amplamente reconhecido na doutrina e no debate público como pornografia de vingança (revenge porn) (PADILHA; GOULART, 2025). O uso desse termo no ambiente acadêmico serve para evidenciar a carga de controle e humilhação social que acompanha essas condutas, embora o Decreto adote uma nomenclatura mais

ampla para abranger casos que vão além do sentimento de vingança, como o lucro ou a simples misoginia.

Adicionalmente, o Art. 3º do Decreto (BRASIL, 2026) apresenta definições importantes para a aplicação de suas disposições. O conceito de conteúdo íntimo é ampliado para incluir não apenas imagens e vídeos reais, mas também qualquer conteúdo que exponha nudez ou de natureza sexual produzido ou manipulado por inteligência artificial (deepfakes) (SILVA, 2025; PADILHA; GOULART, 2025). A definição de violência cibernética é igualmente abrangente, englobando danos físicos, sexuais, psicológicos, políticos ou econômicos facilitados pelo uso de tecnologias (BRASIL, 2026; DIAS, 2024), o que demonstra o esforço em cobrir todas as manifestações contemporâneas da violência de gênero no ciberespaço (BRASIL, 2026; BRASIL, 2025).

3.3. Responsabilidade dos Provedores de Aplicações de Internet

Um dos avanços mais significativos do Decreto reside na responsabilização dos provedores de aplicações de internet. O Art. 4º estabelece que esses provedores, que realizam intermediação de conteúdo gerado por terceiro, serão responsabilizados em caso de falha sistêmica na indisponibilização imediata de conteúdos que configurem crimes ou atos ilícitos praticados contra mulheres (BRASIL, 2026). A falha sistêmica é caracterizada pela não comprovação da adoção de medidas adequadas de prevenção ou remoção de conteúdos criminosos ou ilícitos, que forneçam os mais elevados níveis de segurança e inibam a circulação massiva desses conteúdos (RIBEIRO; AZEVEDO, 2024).

Esta disposição representa um avanço em relação ao Marco Civil da Internet (Lei nº 12.965/2014), que, em regra, exime os provedores de responsabilidade por conteúdo gerado por terceiros, salvo em caso de descumprimento de ordem judicial (BRASIL, 2014). O Supremo Tribunal Federal, ao julgar os Temas 533 e 987, reconheceu que o regime do Art. 19 do Marco Civil não conferia proteção suficiente a bens jurídicos constitucionais, como a proteção das mulheres contra a violência digital (STF, 2025). O Decreto nº 12.976/2026, ao introduzir o conceito de falha sistêmica, impõe aos provedores um dever de cuidado mais proativo (DONEDA, 2023; SOUZA, 2022), exigindo a implementação de mecanismos robustos de moderação e prevenção, especialmente em casos de violência de gênero (PADILHA; GOULART, 2025). Isso busca coibir a disseminação de conteúdos lesivos e incentivar as plataformas a atuarem de forma mais diligente na proteção das mulheres

(BRASIL, 2026).

3.3.1. Notificação e Remoção de Conteúdo

O Decreto também detalha os procedimentos para a notificação e remoção de conteúdos. O Art. 5º determina que os provedores deverão indisponibilizar, em resposta às notificações, os conteúdos que configurem crimes ou atos ilícitos contra as mulheres em ambiente digital (BRASIL, 2026). É importante ressaltar que a notificação deve ser apresentada por meio de canal oficial e dedicado, disponibilizado pelo provedor, e deve conter elementos que permitam a identificação da ilegalidade, informações específicas do conteúdo a ser indisponibilizado e a identificação do notificante (BRASIL, 2026).

Um ponto de destaque é o Art. 7º, que trata da remoção de conteúdo íntimo gerado por terceiros. Nesses casos, a indisponibilização deve ocorrer no prazo de até duas horas, contado da notificação (BRASIL, 2026). A notificação pode ser feita pela vítima, seu representante legal, advogados, autoridades policiais, Ministério Público e Defensorias Públicas (BRASIL, 2026). Além disso, o conteúdo íntimo deverá ser indisponibilizado de toda a aplicação e marcado digitalmente para que o seu reenvio seja automaticamente bloqueado (BRASIL, 2026). Essa medida é fundamental para combater a persistência e a reincidência da divulgação de revenge porn e outros conteúdos íntimos não consentidos (PADILHA; GOULART, 2025).

3.3.2. Mitigação de Alcance e Visibilidade em Casos de Assédio Digital

Outra inovação relevante é o dever de mitigação de alcance e visibilidade em casos de assédio digital, previsto no Art. 8º (BRASIL, 2026). Os provedores de aplicações de internet deverão adotar medidas técnicas e proporcionais para reduzir tempestivamente o alcance e a visibilidade de ataques coordenados contra mulheres que configurem violência contra a mulher (BRASIL, 2026). O mais importante é que essa medida se aplica independentemente de notificação ou denúncia prévia pela vítima, exigindo que o provedor aja de ofício ao identificar indicadores de ocorrência (BRASIL, 2026).

Essa disposição é particularmente importante para combater campanhas de ódio e assédio orquestradas, que visam silenciar e intimidar mulheres (PADILHA; GOULART, 2025), especialmente aquelas com exposição pública, como profissionais da imprensa ou políticas (INSTITUTO MARIA DA PENHA, s.d.; BIROLI; MIGUEL, 2023). Ao impor um dever de ação proativa aos provedores (SOUZA, 2022; DONEDA, 2023), o Decreto busca proteger a

participação feminina no espaço público digital e garantir um ambiente mais seguro para a expressão e atuação das mulheres (BRASIL, 2026).

3.4. Vedação à Geração e Modificação de Conteúdo Íntimo por Inteligência Artificial

O Capítulo III do Decreto aborda a questão da geração e modificação de conteúdo íntimo por inteligência artificial ou qualquer outro recurso tecnológico (BRASIL, 2026). O Art. 9º veda aos provedores de aplicações de internet a geração e a modificação de conteúdo íntimo de terceiro mediante uso de inteligência artificial ou de qualquer outro recurso tecnológico que altere imagem ou som da vítima (BRASIL, 2026). Complementarmente, o Art. 10º exige que os provedores baseados em funcionalidades de inteligência artificial implementem salvaguardas técnicas e procedimentais para identificar e bloquear solicitações de geração de conteúdo íntimo (BRASIL, 2026).

Essa vedação expressa e a exigência de salvaguardas são cruciais para enfrentar o desafio dos deepfakes e outras manipulações digitais (SILVA, 2025), que podem ser utilizadas para criar e disseminar conteúdo íntimo falso, causando danos irreparáveis às vítimas (PADILHA; GOULART, 2025; LEMOS, 2023). A legislação reconhece a gravidade dessas tecnologias e busca prevenir seu uso abusivo para fins de violência de gênero (DIAS, 2024), embora ainda se identifique a necessidade de tipificações penais específicas no ordenamento brasileiro (PADILHA; GOULART, 2025).

3.5. Síntese dos Avanços Normativos do Decreto nº 12.976/2026

Em síntese, o Decreto nº 12.976/2026 representa um avanço significativo na proteção das mulheres no ambiente digital (BRASIL, 2026; PADILHA; GOULART, 2025). Entre suas principais contribuições, destacam-se a consagração de princípios orientadores como a centralidade da vítima e a não revitimização (BRASIL, 2026; DIAS, 2024), a ampliação conceitual de conteúdo íntimo para abranger manipulações por inteligência artificial (BRASIL, 2026; SILVA, 2025), a responsabilização dos provedores por falha sistêmica na remoção de conteúdos ilícitos (BRASIL, 2026; RIBEIRO; AZEVEDO, 2024), a imposição de prazo de até duas horas para remoção de conteúdo íntimo não autorizado com marcação digital para bloqueio de reenvios (BRASIL, 2026), o dever de mitigação proativa do alcance de ataques coordenados independentemente de notificação (BRASIL, 2026; DONEDA, 2023) e a vedação

expressa à geração de deepfakes de natureza íntima (BRASIL, 2026; PADILHA; GOULART, 2025). Trata-se, portanto, de um marco normativo que articula princípios, definições, responsabilidades e procedimentos de forma sistemática. Contudo, a efetividade dessas medidas depende da superação de limitações estruturais (CHAGAS JUNIOR, 2025), que serão abordadas na próxima seção.

4. LIMITAÇÕES ESTRUTURAIS E DESAFIOS NA APLICAÇÃO DO DECRETO Nº 12.976/2026

Embora o Decreto nº 12.976/2026 represente um avanço significativo no plano normativo para o enfrentamento da violência cibernética contra a mulher, sua efetividade prática é desafiada por uma série de limitações estruturais e obstáculos inerentes à natureza do ambiente digital e à capacidade institucional de resposta. A transposição da violência de gênero para o ciberespaço não apenas amplifica os danos, mas também impõe complexidades adicionais à sua prevenção, investigação e responsabilização.

4.1. Dificuldades na Produção e Validação da Prova Digital

Um dos principais entraves à aplicação efetiva do Decreto reside na produção e validação da prova digital. A natureza volátil e efêmera dos dados no ambiente virtual, aliada à facilidade de manipulação e exclusão de informações, torna a coleta e preservação de evidências um desafio constante (SILVA; ROCHA, 2025; BELLÉ; SOUZA, 2025). Conforme destaca Badaró (2024), a validade epistêmica da prova digital depende da observância rigorosa dos standards metodológicos próprios da computação forense. A cadeia de custódia digital, que garante a integridade e autenticidade da prova desde sua origem até a apresentação em juízo (BADUR, 2025), exige rigor técnico e conhecimento especializado que nem sempre estão disponíveis nas instituições responsáveis pela persecução penal.

A desterritorialização das condutas ilícitas, mencionada na seção introdutória desta pesquisa, agrava essa dificuldade. Servidores localizados em diferentes países, a utilização de redes privadas virtuais (VPNs) e a criptografia dificultam a rastreabilidade dos agressores e a obtenção de dados que possam subsidiar a investigação (NEVES; ROSA, 2025). A dependência de cooperação internacional, muitas vezes morosa e burocrática, compromete a celeridade necessária para a coleta de provas antes que sejam perdidas ou alteradas.

4.2. Anonimato e Identificação dos Agressores

O anonimato no ambiente digital é outro fator que impõe severas limitações à responsabilização dos agressores. Embora o Marco Civil da Internet estabeleça a necessidade de identificação dos usuários, a prática demonstra que a ocultação da identidade é relativamente fácil para indivíduos com conhecimento técnico. Conforme destaca o Cyberbullying Research Center, a perseguição online pode ser realizada de localizações geograficamente distantes, tornando exponencialmente mais difícil identificar, localizar e processar os agressores (CYBERBULLYING RESEARCH CENTER, s.d.). Perfis falsos, uso de proxies e a proliferação de plataformas que permitem a postagem de conteúdo sem a necessidade de identificação robusta dificultam sobremaneira a localização dos perpetradores da violência cibernética.

Essa dificuldade na identificação não apenas frustra a busca por justiça das vítimas, mas também contribui para a sensação de impunidade, encorajando a reincidência e a prática de novas condutas ilícitas. A ausência de uma identidade clara do agressor impede a aplicação de medidas protetivas e a efetivação das sanções previstas no ordenamento jurídico. Como observam Santana, Oliveira e Oliveira (2024), as medidas protetivas convencionais, concebidas para o âmbito físico, têm eficácia limitada no ciberespaço, onde o agressor consegue exercer contato e controle à distância sem ser prontamente identificado.

A questão da impunidade é agravada pela própria natureza transnacional do ambiente digital. O UNODC (s.d.) alerta que a evolução das tecnologias facilita a automação e propagação dos ataques, intensificando a impunidade em todas as plataformas e fronteiras, o que inclui a usurpação de identidade e o assédio direcionado em escala nunca antes vista.

4.3. Insuficiência de Recursos Tecnológicos e Capacitação Especializada

A capacidade institucional de enfrentamento da violência cibernética contra a mulher é frequentemente comprometida pela insuficiência de recursos tecnológicos e pela carência de capacitação especializada. As polícias, o Ministério Público e o Poder Judiciário, muitas vezes, não dispõem dos equipamentos, softwares e da expertise técnica necessários para lidar com a complexidade dos crimes digitais. Conforme demonstrado por Silva (2025), as unidades periciais dos estados brasileiros enfrentam desafios como limitações tecnológicas, falta de padronização e necessidade premente de capacitação profissional. A velocidade das inovações tecnológicas exige uma atualização

constante que nem sempre é acompanhada pelos investimentos públicos.

A falta de peritos digitais em número suficiente e a ausência de treinamento adequado para agentes de segurança e operadores do direito em áreas como forense digital, análise de dados e investigação de crimes cibernéticos são gargalos que impedem a efetiva aplicação das normas. Chagas Junior (2025) observa que, embora a perícia forense digital seja essencial para a efetividade da persecução penal, há necessidade de maior capacitação técnica dos profissionais envolvidos e de atualização normativa para acompanhar os avanços tecnológicos. A sofisticação das práticas ilícitas, que utilizam tecnologias emergentes como a inteligência artificial para criar deepfakes ou para coordenar ataques, exige uma resposta igualmente sofisticada por parte do Estado, o que pressupõe a integração entre Direito e tecnologia, apontada pela doutrina como indispensável (CHAGAS JUNIOR, 2025).

4.4. Dependência da Colaboração de Plataformas Digitais

A efetividade do Decreto também depende, em grande medida, da colaboração das plataformas digitais. Embora o diploma normativo imponha um dever de cuidado e responsabilize os provedores por falha sistêmica na indisponibilização de conteúdos, a cooperação proativa e transparente dessas empresas é fundamental. A velocidade na remoção de conteúdo, a preservação de dados de acesso e a disponibilização de informações para as autoridades são cruciais para o sucesso das investigações.

No entanto, a atuação das plataformas é frequentemente pautada por interesses comerciais e por diferentes legislações em nível global, o que pode gerar conflitos e entraves à cooperação. Como observa a doutrina, *big techs* sediadas nos Estados Unidos frequentemente recusam-se a cumprir ordens judiciais brasileiras com base no *CLOUD Act*, aplicando a jurisdição americana em detrimento da brasileira (LEGALE, 2025). O Supremo Tribunal Federal, em julgamento histórico de junho de 2025, declarou parcialmente inconstitucional o artigo 19 do Marco Civil da Internet, estabelecendo que provedores serão responsabilizados por falha sistêmica na indisponibilização de conteúdos que configurem crimes contra a mulher, independentemente de ordem judicial prévia (STF, Temas 533 e 987).

A pressão por celeridade na remoção de conteúdo deve ser equilibrada com a garantia da liberdade de expressão, e a definição de critérios claros para a moderação de conteúdo ainda é um desafio. Conforme apontam Oliveira e

Schlemper (2025), os principais desafios regulatórios no enfrentamento da violência digital de gênero incluem justamente a necessidade de equilibrar a remoção de conteúdo com a garantia da liberdade de expressão. A ausência de um consenso global sobre o que constitui conteúdo ilegal ou prejudicial online dificulta a harmonização das políticas das plataformas e a efetivação das medidas de proteção. Nesse sentido, Brasil e União Europeia têm buscado aprimorar a cooperação em governança digital, reconhecendo os desafios regulatórios e as preocupações éticas associadas às plataformas digitais (BRASIL, 2025).

4.5. Desafios na Atuação Coordenada e Políticas Públicas Integradas

A complexidade da violência cibernética contra a mulher exige uma atuação coordenada entre diferentes instituições e a implementação de políticas públicas integradas. Como destacam Simões e Amaral (2024), uma abordagem multifacetada envolvendo educação, regulamentação e inovação tecnológica é essencial para enfrentar a violência online contra as mulheres. O enfrentamento desse fenômeno não se restringe à esfera jurídica, demandando a participação de órgãos de segurança pública, Ministério Público, Poder Judiciário, instituições de ensino, organizações da sociedade civil e, crucialmente, das próprias plataformas digitais. A fragmentação das ações e a falta de comunicação entre esses atores podem comprometer a eficácia das medidas de prevenção e repressão, razão pela qual a Política Judiciária Nacional de Enfrentamento à Violência contra as Mulheres (Resolução CNJ n. 254/2018) enfatiza a necessidade de articulação entre o Poder Judiciário e outros órgãos governamentais e não governamentais (BRASIL, 2018). Ademais, a necessidade de fortalecimento de políticas públicas integradas é evidente. Isso inclui campanhas de conscientização e educação digital, programas de apoio psicossocial às vítimas, investimentos em pesquisa e desenvolvimento de tecnologias de segurança, e a promoção da igualdade de gênero no ambiente digital. Sem uma abordagem multifacetada que contemple as dimensões social, educacional, tecnológica e jurídica – tal como proposto por Simões e Amaral (2024) – o Decreto, por si só, terá sua efetividade limitada.

Em conclusão, enquanto o Decreto nº 12.976/2026 representa um passo importante na proteção das mulheres contra a violência cibernética, sua aplicação prática enfrenta desafios consideráveis. A superação das limitações relacionadas à prova digital, ao anonimato, à capacitação institucional, à colaboração das plataformas e à coordenação de políticas públicas é

fundamental para que os avanços normativos se traduzam em uma proteção efetiva e integral para as mulheres no ambiente digital.

CONSIDERAÇÕES FINAIS

O presente trabalho teve como objetivo geral analisar a efetividade do Decreto nº 12.976, de 20 de maio de 2026, no enfrentamento da violência cibernética contra a mulher no Brasil, identificando seus avanços normativos e os principais obstáculos à sua aplicação prática. Para tanto, buscou-se conceituar a violência cibernética, examinar o Decreto em seus fundamentos e inovações, e discutir as limitações estruturais que desafiam sua plena efetivação.

Constatou-se que o ambiente digital, embora promotor de inúmeras oportunidades, tornou-se também um palco para a perpetuação e amplificação de formas de violência de gênero, com as mulheres sendo desproporcionalmente afetadas por condutas como a divulgação não consentida de conteúdo íntimo (popularmente conhecida como pornografia de vingança), a sextorsão e o *cyberstalking*. Nesse contexto, o Decreto nº 12.976/2026 emerge como uma resposta normativa crucial, refletindo a crescente preocupação estatal em adaptar o ordenamento jurídico aos desafios da era digital.

Entre os avanços normativos mais significativos trazidos pelo Decreto, destacam-se a clara definição de princípios orientadores, como a centralidade da vítima e a não revitimização, e a ampliação do conceito de conteúdo íntimo para incluir manipulações por inteligência artificial. A norma impõe um dever de cuidado mais proativo aos provedores de aplicações de internet, responsabilizando-os por falha sistêmica na indisponibilização de conteúdos ilícitos e estabelecendo prazos céleres para a remoção de conteúdo íntimo não autorizado, com a inovadora previsão de marcação digital para bloquear reenvios. Adicionalmente, o Decreto aborda a mitigação de alcance e visibilidade em casos de assédio digital coordenado e veda expressamente a geração e modificação de conteúdo íntimo por inteligência artificial, demonstrando um esforço em cobrir as novas fronteiras da violência digital.

Não obstante os inegáveis avanços, a análise revelou que a efetividade prática do Decreto nº 12.976/2026 é confrontada por limitações estruturais persistentes. As dificuldades na produção e validação da prova digital, a complexidade da cadeia de custódia e a desterritorialização das condutas ilícitas representam obstáculos significativos. O anonimato no ambiente digital continua a ser um desafio para a identificação e responsabilização dos agressores, contribuindo para a sensação de impunidade. A insuficiência de recursos

tecnológicos e a carência de capacitação especializada nas instituições de persecução penal, somadas à dependência da colaboração das plataformas digitais – que muitas vezes operam sob lógicas comerciais e regulatórias distintas –, fragilizam a aplicação das medidas previstas. Por fim, a necessidade de uma atuação coordenada entre diferentes instituições e a implementação de políticas públicas integradas são cruciais para superar a fragmentação das ações e garantir uma resposta estatal eficaz.

Diante desse panorama, conclui-se que o Decreto nº 12.976/2026 representa um passo fundamental na construção de um arcabouço jurídico mais robusto para o enfrentamento da violência cibernética contra a mulher no Brasil. Contudo, sua plena efetividade dependerá da superação das limitações estruturais identificadas, o que exige investimentos contínuos em tecnologia, capacitação profissional, cooperação interinstitucional e internacional, e o fortalecimento de políticas públicas que contemplem a educação digital e o apoio psicossocial às vítimas. A norma, por si só, não é suficiente; ela deve ser acompanhada de uma transformação cultural e de um compromisso coletivo para garantir um ambiente digital seguro, respeitoso e igualitário para todas as mulheres.

Diante do diagnóstico apresentado, impõe-se a formulação de sugestões concretas para cada uma das limitações estruturais identificadas ao longo desta pesquisa.

Quanto à produção e validação da prova digital, recomenda-se a padronização nacional dos procedimentos de cadeia de custódia digital, nos moldes do que propõem Neves e Rosa (2025), com a criação de um protocolo único a ser adotado por todas as unidades periciais do país, incluindo o uso obrigatório de hash para verificação de integridade e a implementação de sistemas baseados em blockchain para rastreabilidade das evidências. Exemplos internacionais exitosos incluem o National Institute of Standards and Technology (NIST) dos Estados Unidos, que mantém guias detalhados para a coleta e preservação de provas digitais, e o European Cybercrime Centre (EC3) da Europol, que oferece treinamento especializado e suporte técnico aos Estados-membros da União Europeia.

Quanto ao anonimato e à identificação dos agressores, sugere-se o fortalecimento de mecanismos de identificação civil no ambiente digital, aliado à criação de um cadastro nacional de usuários para plataformas de alto risco, inspirado no modelo português do "Cartão de Cidadão" associado à chave móvel digital (CMD), que permite a identificação segura em transações e interações

online. Além disso, a experiência alemã com a Network Enforcement Act (NetzDG), que exige das plataformas a manutenção de canais eficientes para denúncias e a identificação de usuários reincidentes em práticas de discurso de ódio, oferece parâmetros valiosos para o aperfeiçoamento da legislação brasileira.

Quanto à insuficiência de recursos tecnológicos e capacitação especializada, a proposta central reside na criação de núcleos especializados em crimes cibernéticos de gênero no âmbito das polícias civis e federal, com investimento público em softwares de forense digital, como as soluções utilizadas pelo FBI (Case Management System) e pela Policía Nacional da Espanha (Sistema de Análisis de Huellas Digitales). A capacitação continuada de magistrados, promotores e delegados – nos moldes do que já ocorre no Conselho Nacional de Justiça com o "Programa de Capacitação em Inteligência Artificial e Prova Digital" – deve ser ampliada e tornada obrigatória. Ademais, a experiência britânica com o National Cyber Security Centre (NCSC), que oferece treinamento gratuito para pequenas empresas e órgãos públicos, demonstra a viabilidade de políticas de capacitação em larga escala.

Quanto à dependência da colaboração das plataformas digitais, defende-se a aprovação de um marco regulatório nacional que harmonize as diretrizes do Decreto nº 12.976/2026 com a decisão do STF nos Temas 533 e 987, estabelecendo deveres claros para os provedores, como a obrigatoriedade de transparência algorítmica, a manutenção de canais de notificação em português e a nomeação de representantes legais no território brasileiro. Inspirado no Digital Services Act (DSA) da União Europeia – que classifica as plataformas por porte e risco, impondo obrigações proporcionais para remoção de conteúdos ilegais, auditoria externa e acesso a dados para pesquisadores –, o Brasil pode avançar na construção de um ambiente regulatório que equilibre a proteção das vítimas com a garantia da liberdade de expressão, vedada qualquer forma de censura prévia.

Quanto à necessidade de atuação coordenada e políticas públicas integradas, sugere-se a criação de um comitê gestor interinstitucional permanente, composto por representantes do Ministério da Justiça e Segurança Pública, Ministério das Mulheres, Conselho Nacional de Justiça, Conselho Nacional do Ministério Público, além de entidades da sociedade civil e das plataformas digitais. Esse comitê seria responsável pela implementação do Plano Nacional de Enfrentamento à Violência Cibernética contra a Mulher, com metas bienais, indicadores de desempenho e relatórios públicos de progresso.

A experiência canadense com o "*CyberScan*" – uma plataforma colaborativa que reúne forças policiais, organizações não governamentais e universidades para monitorar e responder a incidentes de violência digital – oferece um modelo promissor a ser adaptado à realidade brasileira.

Por fim, reforça-se que a efetividade do Decreto nº 12.976/2026 não decorrerá apenas de sua existência normativa, mas sim da implementação coordenada de políticas públicas que superem as limitações estruturais identificadas. O diálogo com experiências internacionais exitosas – como o Digital Services Act europeu, a Network Enforcement Act alemã, o sistema português de identificação digital e os programas de capacitação britânico e canadense – oferece caminhos concretos para o aperfeiçoamento contínuo das políticas públicas brasileiras, em um esforço que deve envolver não apenas o Poder Executivo e o Legislativo, mas toda a sociedade.

REFERÊNCIAS

ALMEIDA, Maria Paula Castro de. A evolução no combate aos crimes virtuais. 2015. Trabalho apresentado (Curso de Formação de Magistrados) – Escola de Magistratura do Estado do Rio de Janeiro, Rio de Janeiro, 2015.

BADARÓ, Gustavo Henrique Righi Ivahy. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. Boletim IBCCRIM, São Paulo, v. 29, n. 343, p. 7-9, 2024.

BADUR, Nelson Antonio Satto. A importância da cadeia de custódia digital na preservação da prova eletrônica. Brazilian Journal of Development, Curitiba, v. 11, n. 5, e79668, 2025. DOI: 10.34117/bjdv11n5-037.

BELLÉ, Adriano Vottri; SOUZA, Ayleen Dywaine. Provas digitais no processo penal: autenticidade, manipulação por inteligência artificial e desafios ao devido processo. Gralha Azul: Revista do Tribunal de Justiça do Paraná, Curitiba, v. 1, n. 1, 2025. DOI: 10.62248/cbjxxr83.

BIROLI, Flávia; MIGUEL, Luis Felipe. Gênero, violência e política. São Paulo: Boitempo, 2023.

BRASIL. Decreto nº 12.976, de 20 de maio de 2026.

BRASIL. Lei nº 11.340, de 7 de agosto de 2006. Cria mecanismos para coibir a violência doméstica e familiar contra a mulher. Diário Oficial da União: Brasília, DF, 8 ago. 2006. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11340.htm. Acesso em: 06 junho 2026.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 06 junho 2026.

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: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

Acesso em: 06 junho 2026.

BRASIL. Conselho Nacional de Justiça. Resolução CNJ n. 254, de 4 de setembro de 2018. Política Judiciária Nacional de Enfrentamento à Violência contra as Mulheres. Brasília: CNJ, 2018. Disponível em: https://www.cnj.jus.br/programas-e-acoes/violencia-contra-a-mulher/. Acesso em: 06 junho 2026.

BRASIL. Ministério das Mulheres. Pacto Nacional Brasil Contra o Feminicídio. Brasília: Ministério das Mulheres, 2024. Disponível em: https://www.gov.br/mulheres/pt-br. Acesso em: 06 junho 2026.

BRASIL. Senado Federal. DataSenado. 11ª Pesquisa Nacional de Violência contra a Mulher: relatório geral. Brasília: Senado Federal, 2025. Disponível em: https://www.senado.leg.br/institucional/datasenado/relatorio_online/pesquisa_violencia_domestica/2025/interativo.html. Acesso em: 06 junho 2026.

BRASIL. Ministério das Mulheres. Canal Ligue 180 registra crescimento de 45% nos atendimentos e 17% nas denúncias de violência em 2025. Brasília: Ministério das Mulheres, 2026. Disponível em: https://www.gov.br/mulheres/pt-br/central-de-conteudos/noticias/2026/abril/canal-ligue-180-registra-crescimento-de-27-nas-denuncias-e-10-nos-atendimentos-no-primeiro-trimestre-de-2026. Acesso em: 06 junho 2026.

BRASIL. Secretaria de Comunicação Social da Presidência da República. Brasil e União Europeia reforçam cooperação em governança digital e reafirmam seus marcos de legislação na área digital. Gov.br, 12 fev. 2025. Disponível em: https://www.gov.br/secom/pt-br/acompanhe-a-secom/noticias/2025/02/brasil-e-uniao-europeia-reforcam-cooperacao-em-governanca-digital-e-reafirmam-seus-marcos-de-legislacao-na-area-digital. Acesso em: 06 junho 2026.

CAZAROTI, Bruno; PINHEIRO, Rodrigo. Crimes cibernéticos: evolução, tipificação e desafios. São Paulo: Atlas, 2021.

CHAGAS JUNIOR, Rodrigo Aloizio. Desafios e implicações da perícia forense digital no direito penal brasileiro. Contribuciones a Las Ciencias Sociales, v. 18, n. 9, 2025. DOI: 10.55905/revconv.18n.9-011. Disponível em: https://ojs.revistacontribuciones.com/ojs/index.php/clcs/article/view/20488.

Acesso em: 06 junho 2026.

CRUZ, Rafael; RODRIGUES, Fernanda. A evolução dos crimes cibernéticos e a resposta do direito penal brasileiro. Revista de Direito Penal Contemporâneo, São Paulo, v. 12, n. 45, p. 87-104, 2018.

CYBERBULLYING RESEARCH CENTER. Cyberstalking. In: Cyberbullying Research Center, [s.d.]. Disponível em: https://cyberbullying.org/cyberstalking. Acesso em: 06 junho 2026.

DIAS, Maria Berenice. Manual de Direito das Mulheres. 5. ed. Salvador: JusPodivm, 2024.

DONEDA, Danilo. A proteção de dados pessoais como direito fundamental. São Paulo: Revista dos Tribunais, 2023.

FIORILLO, Celso Antônio Pacheco; CONTE, Emanuela. Direito e internet: aspectos jurídicos relevantes. São Paulo: Saraiva, 2016.

GONÇALVES, Thamires Meireles. O reconhecimento do estupro virtual: discussões sobre a (não) violação ao princípio da legalidade. Trabalho de Conclusão de Curso (Graduação em Direito) – Pontifícia Universidade Católica de Goiás, Goiânia, 2024. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/7969. Acesso em: 06 junho 2026.

HERNANDEZ, Erika Fernanda Tangerino; DE TOLEDO, Nathália Karina Abucci. Crimes cibernéticos: seus efeitos revolucionários diante de uma legislação em constante evolução. Revista Jurídica da UniFil, Londrina, v. 17, n. 17, p. 72-84, 2021.

INSTITUTO MARIA DA PENHA. Tipos de violência. In: Lei Maria da Penha comentada. Disponível em: https://www.institutomariadapenha.org.br/lei-11340/tipos-de-violencia.html. Acesso em: 06 junho 2026.

LEGALE. Advocacia Digital: Cibercrime, Prova e Cooperação Global. Legale, 2025. Disponível em: https://legale.com.br/blog/advocacia-digital-cibercrime-

prova-e-cooperacao-global/. Acesso em: 06 junho 2026.

LEMOS, Ronaldo. Deepfakes e a proteção da imagem e privacidade. Rio de Janeiro: Editora FGV, 2023.

LIMA, Yasmin Victoria et al. Direito digital: aplicação nos crimes cibernéticos. In: ANAIS da Semana de Pesquisa Jurídica, 1., 2022. Anais... [s.l.]: [s.n.], 2022. v. 1, p. 42.

MONTEIRO, Carlos Augusto. Violência cibernética no Espírito Santo: análise estatística dos crimes contra a mulher. Revista Capixaba de Segurança Pública, Vitória, v. 8, n. 1, p. 5-18, 2019.

NEVES, Luiz Gabriel Batista; ROSA, Hiuston César dos Santos. Technology and digital evidence: challenges and proposals for the chain of custody in the Judiciary. Boletim IBCCRIM, São Paulo, v. 34, n. 398, p. 29-31, 2025. DOI: 10.5281/zenodo.17914684.

OLIVEIRA, Dessano Plum de; MACIAL FERREIRA, Fernanda Souza Mendes. Resolução CNJ n. 591/2024: julgamentos eletrônicos, devido processo legal e prerrogativas da advocacia. Revista CNJ, v. 9, n. 2, 2025. DOI: 10.54829/revistacnj.v9i2.792.

OLIVEIRA, Shirley Ayres; SCHLEMPER, Maricélia. A violência de gênero na era digital: análise de novas formas de agressão, desafios regulatórios e perspectivas éticas. SIERT, 2025. Disponível em: https://periodicos.univel.br/ojs/index.php/siert/article/view/592. Acesso em: 06 junho 2026.

ONU MULHERES. Quase metade das mulheres e meninas do mundo não conta com proteção legal contra violência digital. Nova York: ONU Mulheres, 18 nov. 2025. Disponível em: https://www.onumulheres.org.br/noticias/quase-metade-das-mulheres-e-meninas-mundo-nao-conta-com-protecao-legal-contra-violencia-online/. Acesso em: 06 junho 2026.

PADILHA, Bruno Barcelos Franco; GOULART, Líbia Kicela. Violência digital de gênero: a ascensão dos crimes cibernéticos contra as mulheres. RCMOS -

Revista Científica Multidisciplinar O Saber, v. 1, n. 1, 2025. DOI: 10.51473/rcmos.v1i1.2025.1075. Disponível em: https://submissoesrevistarcmos.com.br/rcmos/article/view/1075. Acesso em: 06 junho 2026.

PINHEIRO, Patrícia Peck. Direito Digital. 4. ed. São Paulo: Saraiva, 2012.

PNUD. Uso apropriado de tecnologias digitais impulsiona igualdade de gênero. PNUD Brasil, 10 abr. 2023. Disponível em: https://www.undp.org/pt/brazil/news/uso-apropriado-de-tecnologias-digitais-impulsiona-igualdade-de-genero. Acesso em: 06 junho 2026.

RIBEIRO, Mariana; AZEVEDO, Isabela. Falha sistêmica: o impacto da ausência de moderação nas plataformas digitais. Revista de Direito, Inovação e Tecnologia, v. 8, n. 2, p. 45-62, 2024.

SANTANA, Rackel Cunha de; OLIVEIRA, Lucas Lucena; OLIVEIRA, Luziane Lucena Souza. Stalking digital: uma análise da Lei Maria da Penha à luz da Lei 14.132/2021. Revista GeoTemas, v. 17, n. 4, 2024. DOI: 10.56238/revgeov17n4-115.

SANTOS, Daniel Alves dos; COSTA, Larissa de Paula; MARROQUE, Nathalya Reis dos Santos; GAMA, Percy Lucas dos Santos; PAULA, Wanderson Machado de. Crimes sexuais e a era digital: estupro virtual. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Rede Doctum de Ensino, Serra/ES, 2024. Disponível em: https://dspace.doctum.edu.br/handle/123456789/4990. Acesso em: 06 junho 2026.

SILVA, Alexsandro Yuri Felizardo. Perícia Forense em Sistemas Eletrônicos Digitais: uma pesquisa quanto à atuação das unidades periciais dos estados brasileiros. Trabalho de Conclusão de Curso (Engenharia Eletrônica) – Universidade Federal de Pernambuco, Recife, 2025. Disponível em: https://repositorio.ufpe.br/jspui/bitstream/123456789/64918/3/Pericia_Forense_em_Sistemas_Eletronicos_Digitais_TCC_REVISAO_V4_assinado.pdf. Acesso em: 06 junho 2026.

SILVA, Frank Mendes da. Crimes cibernéticos: deepfake, direito digital e a

LGPD. 2025. Disponível em: https://frankmendesilva.com.br/crimes-ciberneticos. Acesso em: 06 junho 2026.

SILVA, Mariana Almeida da. A internet como ambiente facilitador à violência de gênero: cyberstalking, sextorsão e revenge porn. Revista do Ministério Público do Estado do Rio de Janeiro, Rio de Janeiro, n. 86, p. 195-212, out./dez. 2022. Disponível em: https://www.mprj.mp.br/documents/20184/3600511/Mariana+Almeida+da+Silva_RMP-86.pdf. Acesso em: 06 junho 2026.

SILVA, Paulo Daniel Bonfim da; ROCHA, Siomara Dias da. Estado da Arte sobre a perícia digital forense. Cuadernos de Educación y Desarrollo, v. 17, n. 6, e8601, 2025. DOI: 10.55905/cuadv17n6-046.

SIMÕES, Rita Basílio de; AMARAL, Inês. Educação, regulamentação e inovação tecnológica: perceções de stakeholders da violência online contra as mulheres. In: Género, violência e ódio online: conceitos e representações. Coimbra: Imprensa da Universidade de Coimbra, 2024. Disponível em: https://estudogeral.sib.uc.pt/handle/10316/118605. Acesso em: 06 junho 2026.

SOUZA, Carlos Affonso Pereira de. Marco Civil da Internet: desafios e perspectivas. Belo Horizonte: Fórum, 2022.

SOUZA, Rodrigo; CERVINSKI, Letícia. A proteção da honra e privacidade na era digital: novos desafios ao direito penal. Revista de Direito Penal e Criminologia, Rio de Janeiro, v. 22, n. 3, p. 201-225, 2021.

SUPREMO TRIBUNAL FEDERAL. Tema 533 e Tema 987 da Repercussão Geral. Julgamento conjunto sobre a constitucionalidade do artigo 19 do Marco Civil da Internet. STF, Plenário, julgado em 26 de junho de 2025.

UNODC. Violência digital. In: UNODC Moçambique, [s.d.]. Disponível em: https://www.unodc.org/rosaf/mozambique/violencia-digital.html. Acesso em: 06 junho 2026

VERAS, Natália Lopes. Estupro virtual: análise, viabilidade prática e necessidade de nova tipificação. Trabalho de Conclusão de Curso (Graduação em Direito) –

Universidade Presbiteriana Mackenzie, São Paulo, 2020. Disponível em: https://dspace.mackenzie.br/handle/10899/30044. Acesso em: 06 junho 2026

VIEIRA, José Carlos. A história da internet no Brasil: da RNP à banda larga. Rio de Janeiro: Editora UFRJ, 2003.