

A INTELIGÊNCIA ARTIFICIAL COMO FERRAMENTA PARA PROPAGAÇÃO DA VIOLÊNCIA DE GÊNERO - UMA ANÁLISE JURÍDICA ACERCA DAS *DEEP FAKES* A LUZ DO CÓDIGO PENAL BRASILEIRO

LA INTELIGENCIA ARTIFICIAL COMO HERRAMIENTA PARA LA PROPAGACIÓN DE LA VIOLENCIA DE GÉNERO: UN ANÁLISIS JURÍDICO DE LOS *DEEPFAKES* A LA LUZ DEL CÓDIGO PENAL BRASILEÑO

ARTIFICIAL INTELLIGENCE AS A TOOL FOR THE PROPAGATION OF GENDER-BASED VIOLENCE: A LEGAL ANALYSIS OF *DEEPFAKES* IN LIGHT OF THE BRAZILIAN PENAL CODE

Ana Dallara Freitas Calheiros¹
Ariane Loudemila Silva de Albuquerque²

RESUMO: A inteligência artificial tem promovido transformações significativas no ambiente digital, ao mesmo tempo em que passou a ser instrumentalizada para a prática de condutas ilícitas, notadamente por meio da utilização das *deepfakes*. Essa tecnologia, capaz de gerar conteúdos audiovisuais falsificados com elevado grau de realismo, tem sido amplamente empregada na reprodução e disseminação de violência de gênero, atingindo de forma desproporcional mulheres, sobretudo por meio da criação e circulação de imagens e vídeos íntimos fraudulentos. A relevância da temática decorre do crescimento exponencial dessas práticas, bem como da dificuldade enfrentada pelo ordenamento jurídico em acompanhar, de maneira eficaz, a rapidez e a complexidade do avanço tecnológico. Objetivou-se analisar a adequação do ordenamento penal brasileiro frente às novas formas de violência de gênero mediadas por tecnologias de inteligência artificial. Quanto à metodologia, realizou-se pesquisa qualitativa, de caráter exploratório e descritivo, desenvolvida por meio de revisão bibliográfica narrativa e pesquisa documental, com análise de artigos científicos, obras doutrinárias, trabalhos acadêmicos, legislação e documentos oficiais relacionados à inteligência artificial, às *deepfakes*, à violência de gênero e ao Direito Penal brasileiro. A análise dos resultados demonstra que, embora existam avanços legislativos voltados à repressão da pornografia não consentida, ainda persistem lacunas normativas que comprometem a efetiva responsabilização penal dos agentes e a proteção integral das vítimas. Conclui-se que o enfrentamento da violência de gênero potencializada pela inteligência artificial demanda não apenas a atualização do sistema penal, mas também a implementação de políticas públicas integradas, voltadas à prevenção, à educação digital e à tutela efetiva dos direitos da personalidade das mulheres.

Palavras-chave: Violência contra a mulher. Proteção da imagem. Manipulação digital.

¹Discente. Universidade Estadual de Alagoas.

²Orientadora. docente, pesquisadora Universidade Estadual de Alagoas.

RESUMEN: La inteligencia artificial ha promovido transformaciones significativas en el entorno digital, al mismo tiempo que ha pasado a ser utilizada como instrumento para la comisión de conductas ilícitas, especialmente mediante el uso de *deepfakes*. Esta tecnología, capaz de generar contenidos audiovisuales falsificados con un elevado grado de realismo, ha sido ampliamente empleada en la reproducción y difusión de la violencia de género, afectando de manera desproporcionada a las mujeres, sobre todo mediante la creación y circulación de imágenes y videos íntimos fraudulentos. La relevancia del tema se debe al crecimiento exponencial de estas prácticas, así como a la dificultad que enfrenta el ordenamiento jurídico para acompañar, de manera eficaz, la rapidez y la complejidad de los avances tecnológicos. El objetivo de este estudio fue analizar la adecuación del ordenamiento penal brasileño frente a las nuevas formas de violencia de género mediadas por tecnologías de inteligencia artificial. En cuanto a la metodología, se realizó una investigación cualitativa, de carácter exploratorio y descriptivo, desarrollada mediante una revisión bibliográfica narrativa y una investigación documental, con el análisis de artículos científicos, obras doctrinales, trabajos académicos, legislación y documentos oficiales relacionados con la inteligencia artificial, los *deepfakes*, la violencia de género y el Derecho Penal brasileño. El análisis de los resultados demuestra que, aunque existen avances legislativos orientados a la represión de la pornografía no consentida, todavía persisten lagunas normativas que dificultan la efectiva responsabilización penal de los autores y la protección integral de las víctimas. Se concluye que el enfrentamiento de la violencia de género potenciada por la inteligencia artificial exige no solo la actualización del sistema penal, sino también la implementación de políticas públicas integradas destinadas a la prevención, la educación digital y la protección efectiva de los derechos de la personalidad de las mujeres.

Palabras clave: Violencia contra la mujer. Protección de la imagen. Manipulación digital.

ABSTRACT: Artificial intelligence has brought about significant transformations in the digital environment, while also being used as a tool for the commission of unlawful conduct, particularly through the use of *deepfakes*. This technology, which is capable of generating falsified audiovisual content with a high degree of realism, has been widely employed in the reproduction and dissemination of gender-based violence, disproportionately affecting women, especially through the creation and circulation of fraudulent intimate images and videos. The relevance of this topic stems from the exponential growth of these practices, as well as from the difficulties faced by the legal system in effectively keeping pace with the speed and complexity of technological advancements. This study aimed to analyze the adequacy of the Brazilian criminal law framework in addressing new forms of gender-based violence mediated by artificial intelligence technologies. Regarding the methodology, a qualitative, exploratory, and descriptive study was conducted through a narrative literature review and documentary research, including the analysis of scientific articles, legal scholarship, academic papers, legislation, and official documents concerning artificial intelligence, deepfakes, gender-based violence, and Brazilian criminal law. The analysis of the results demonstrates that, although legislative progress has been made toward combating non-consensual pornography, regulatory gaps still remain, hindering the effective criminal accountability of offenders and the comprehensive protection of victims. It is concluded that addressing gender-based violence intensified by artificial intelligence requires not only the modernization of the criminal justice system, but also the implementation of integrated public policies aimed at prevention, digital education, and the effective protection of women's personality rights.

Keywords: Violence against women. Image protection. Digital manipulation.

INTRODUÇÃO

A inteligência artificial (IA) tem assumido papel central nas transformações sociais, econômicas e comunicacionais da contemporaneidade, influenciando de modo significativo a

forma como as relações humanas se estabelecem no ambiente digital. Tecnologias baseadas em algoritmos de aprendizado de máquina e *deep learning* passaram a integrar o cotidiano, ampliando possibilidades de criação, automação e disseminação de informações. Contudo, paralelamente aos benefícios proporcionados por esses avanços, emergem riscos expressivos associados ao uso indevido da IA, sobretudo quando empregada como instrumento de violação de direitos fundamentais. Nesse contexto, destacam-se as *deepfakes*, tecnologia capaz de produzir imagens, vídeos e áudios falsificados com elevado grau de realismo, que vêm sendo amplamente utilizadas para fins ilícitos, especialmente na propagação da violência de gênero.

As *deepfakes* configuram uma das manifestações mais complexas da violência digital contemporânea, uma vez que permitem a criação de conteúdos falsos de caráter sexual, difamatório ou vexatório, direcionados majoritariamente às mulheres. Trata-se de um fenômeno que extrapola o campo tecnológico e alcança dimensões jurídicas, sociais, éticas e psicológicas, atingindo diretamente a dignidade da pessoa humana, a honra, a privacidade e o direito à imagem das vítimas. Ao possibilitar a fabricação de cenas íntimas inexistentes, essa tecnologia potencializa práticas como a pornografia não consentida, o *revenge porn* e o *image-based sexual abuse*, reforçando o potencial de revitimização e perpetuando desigualdades estruturais de gênero. (Santos, Cardin, Tena, 2025).

3

A relevância do tema justifica-se pela crescente incidência de casos envolvendo *deepfakes* e pela evidente dificuldade do ordenamento jurídico em acompanhar, com a mesma velocidade, os avanços tecnológicos. Embora o Código Penal brasileiro tenha passado por atualizações recentes voltadas à proteção da dignidade sexual e à repressão da pornografia de vingança, ainda se observa a ausência de dispositivos específicos capazes de abarcar, de forma plena, as particularidades das condutas praticadas por meio da inteligência artificial. Tal lacuna normativa impõe desafios à responsabilização penal dos agentes e à efetiva tutela das vítimas, tornando imprescindível a análise crítica da adequação do sistema penal vigente frente a essas novas formas de violência. (Medon, 2021).

Diante desse cenário, o problema de pesquisa consiste em compreender em que medida o Código Penal brasileiro se mostra suficiente para enfrentar o uso das *deepfakes* como ferramenta de propagação da violência de gênero, especialmente no que tange à proteção dos direitos fundamentais das mulheres no ambiente digital. A partir dessa problematização, o objetivo geral do estudo é analisar a eficácia do ordenamento jurídico penal brasileiro diante das condutas envolvendo *deepfakes*, à luz da dignidade da pessoa humana e da tutela dos direitos da

personalidade. Como objetivos específicos, busca-se examinar o funcionamento das tecnologias de inteligência artificial associadas às *deepfakes*, identificar os dispositivos penais atualmente aplicáveis a essas práticas e refletir sobre a necessidade de aprimoramento legislativo e de políticas jurídicas específicas para o enfrentamento da violência de gênero mediada por tecnologia.

Quanto aos procedimentos metodológicos, o estudo adota abordagem qualitativa, exploratória e descritiva, desenvolvida por meio de revisão bibliográfica narrativa e pesquisa documental, conforme detalhado na seção seguinte. Ao discutir os impactos sociais e jurídicos das *deepfakes*, busca-se contribuir para o debate acadêmico acerca dos desafios impostos pela inteligência artificial ao Direito Penal, evidenciando a necessidade de respostas jurídicas compatíveis com a proteção da dignidade, da privacidade e dos direitos das mulheres no ambiente digital.

METODOLOGIA

Foi realizada uma abordagem qualitativa, com objetivos exploratórios e descritivos, uma vez que busca compreender as repercussões jurídicas e sociais da utilização das *deepfakes* como instrumento de violência de gênero, bem como examinar a adequação da legislação penal brasileira diante dessas novas formas de violência praticadas no ambiente digital.

4

Quanto aos procedimentos técnicos, o estudo foi desenvolvido por meio de revisão bibliográfica e pesquisa documental. A revisão bibliográfica abrangeu artigos científicos, obras doutrinárias, capítulos de livros, trabalhos de conclusão de curso e outras produções acadêmicas relacionadas à inteligência artificial, às *deepfakes*, à violência de gênero, aos direitos da personalidade e ao Direito Penal. A pesquisa documental, por sua vez, compreendeu o exame da Constituição Federal, do Código Penal, de leis especiais, decretos, projetos legislativos e demais documentos oficiais pertinentes ao objeto da investigação.

A busca bibliográfica foi realizada nas bases Google Acadêmico, Portal de Periódicos da Capes e SciELO. Foram empregados, isoladamente e de forma combinada, os seguintes descritores: “inteligência artificial”, “*deepfake*”, “*deepfakes*”, “violência de gênero”, “violência digital contra a mulher”, “pornografia não consentida”, “pornografia de vingança”, “direito à imagem”, “direitos da personalidade” e “Direito Penal brasileiro”. Foram utilizados os correspondentes em língua inglesa, especialmente “*artificial intelligence*”, “*deepfake pornography*”, “*gender-based violence*”, “*image-based sexual abuse*” e “*non-consensual intimate images*”.

Como critérios de inclusão, foram selecionados materiais publicados entre 2016 e 2026, disponíveis integralmente, em língua portuguesa, inglesa ou espanhola, e que apresentassem relação direta com a utilização de inteligência artificial na produção de conteúdos falsificados, com a violência de gênero no ambiente digital ou com o enquadramento jurídico dessas condutas. Também foram incluídas normas jurídicas anteriores ao recorte temporal quando indispensáveis à compreensão do sistema normativo vigente, a exemplo da Constituição Federal e do Código Penal.

Foram excluídos os materiais duplicados, as publicações sem identificação de autoria, os textos de natureza exclusivamente jornalística, os trabalhos sem relação direta com o problema de pesquisa e as produções que mencionavam a inteligência artificial ou as *deepfakes* apenas de forma incidental, sem desenvolvimento jurídico, social ou tecnológico relevante.

A análise do material ocorreu de forma descritiva, interpretativa e crítica. Inicialmente, as fontes foram organizadas em eixos temáticos: inteligência artificial e transformações tecnológicas; origem e funcionamento das *deepfakes*; violência de gênero no ambiente digital; direitos da personalidade; enquadramento penal; lacunas normativas; e perspectivas de prevenção e responsabilização. Posteriormente, os conteúdos bibliográficos foram confrontados com a legislação brasileira, com o objetivo de identificar os tipos penais aplicáveis, seus limites interpretativos e a necessidade de aperfeiçoamento normativo.

Inteligência Artificial e Transformações Tecnológicas no Ambiente Digital

A adoção crescente de técnicas de inteligência artificial (IA) tem impulsionado profundas transformações no ambiente digital contemporâneo. Atualmente, algoritmos inteligentes encontram-se integrados às mais diversas esferas da vida social, abrangendo desde atividades empresariais, educacionais e profissionais até as relações interpessoais estabelecidas por meio de plataformas digitais. A utilização dessas tecnologias apresenta múltiplas possibilidades de aplicação, como a automatização de tarefas, a análise de grandes volumes de dados, o reconhecimento de imagens e padrões, a personalização de serviços e a criação de conteúdos digitais.

A presença da inteligência artificial também se estende aos campos político, econômico, jurídico e da segurança pública, com aplicações que incluem o processamento de informações, a identificação de riscos, a proteção de dados, o desenvolvimento de sistemas automatizados e a criação de programas voltados ao bem-estar coletivo. Nesse sentido, as tecnologias de IA

redefiniram a forma como as pessoas produzem, acessam e compartilham informações, proporcionando maior rapidez, eficiência e alcance aos processos comunicacionais.

Entretanto, os mesmos avanços tecnológicos que promovem benefícios econômicos e sociais também criam novos desafios. O desenvolvimento de técnicas modernas de aprendizado de máquina e aprendizado profundo tornou possível a geração de conteúdos sintéticos cada vez mais sofisticados e realistas. Esses recursos permitem a criação ou alteração de textos, imagens, áudios e vídeos de maneira artificial, dificultando, em determinadas situações, a distinção entre conteúdos verdadeiros e falsificados.

Castella e Karvat (2025), afirmam que o desenvolvimento das tecnologias de inteligência artificial, especialmente das *deepfakes*, introduziu novas formas de violência digital, capazes de produzir impactos profundos sobre os direitos fundamentais dos indivíduos no ambiente virtual. A manipulação de imagens, vozes e vídeos pode ser utilizada para atribuir falsamente a uma pessoa comportamentos, declarações ou situações que jamais ocorreram, afetando sua honra, sua imagem, sua privacidade e sua dignidade.

Embora essas tecnologias possuam aplicações legítimas em áreas como entretenimento, cinema, publicidade, educação, pesquisa científica e acessibilidade, também passaram a ser instrumentalizadas para a prática de condutas ilícitas. Entre os possíveis usos indevidos estão a disseminação de desinformação, a realização de fraudes, a falsificação de identidades, a manipulação política, a extorsão, a difamação e a criação de conteúdos íntimos falsos. Nesse cenário, destaca-se o fenômeno das *deepfakes*, cuja capacidade de reproduzir artificialmente a aparência e a voz de pessoas reais ampliam os riscos de violação de direitos no ambiente digital.

A facilidade de acesso a ferramentas de edição e geração de conteúdos por inteligência artificial também contribui para o agravamento do problema. Recursos anteriormente restritos a profissionais especializados e a equipamentos de alto desempenho tornaram-se acessíveis a usuários comuns por meio de programas e aplicativos de fácil utilização. Consequentemente, a produção de conteúdos manipulados deixou de exigir conhecimentos técnicos avançados, aumentando tanto as possibilidades legítimas de criação quanto o potencial de utilização abusiva dessas tecnologias.

Além disso, a velocidade de circulação das informações nas redes sociais amplia os efeitos das falsificações digitais. Uma imagem ou um vídeo manipulado pode alcançar milhares de usuários em poucos minutos, sendo reproduzido em diferentes plataformas antes mesmo que a vítima tenha conhecimento de sua existência. Ainda que posteriormente seja comprovada a

falsidade do conteúdo, sua completa remoção do ambiente virtual mostra-se difícil, uma vez que arquivos podem ser copiados, armazenados e novamente compartilhados por inúmeros usuários.

Essa dinâmica evidencia que os danos produzidos pela inteligência artificial não decorrem apenas da criação do conteúdo falso, mas também de sua capacidade de disseminação rápida, permanente e praticamente ilimitada. A aparência de autenticidade das *deepfakes* pode induzir terceiros ao erro, comprometer a reputação das vítimas e produzir consequências psicológicas, profissionais, familiares e sociais duradouras.

A ambivalência inerente ao progresso tecnológico, marcado por potenciais simultaneamente construtivos e destrutivos, constitui uma das principais características das transformações do ambiente digital contemporâneo. A inteligência artificial não possui, por si mesma, natureza ilícita ou prejudicial; os riscos surgem da forma como ela é desenvolvida, disponibilizada e utilizada. Por esse motivo, a análise de seus impactos não pode ficar restrita aos aspectos técnicos, devendo considerar também suas implicações éticas, sociais e jurídicas.

Portanto, embora a inteligência artificial represente um importante instrumento de inovação e desenvolvimento, seu uso indevido exige atenção redobrada do Estado, das instituições, das empresas de tecnologia e da sociedade. O Direito deve acompanhar essas transformações, estabelecendo mecanismos capazes de prevenir abusos, responsabilizar os agentes e proteger os direitos das pessoas atingidas. Essa necessidade torna-se ainda mais evidente diante da utilização das *deepfakes* para reproduzir e intensificar formas de violência de gênero, especialmente contra mulheres, tema que será aprofundado nos tópicos seguintes.

Deep Fakes: Origem, Funcionamento e Usos Ilícitos

O termo *deepfake* deriva da fusão de *deep learning* (aprendizado profundo) e *fake* (falsificação), aludindo à técnica de inteligência artificial utilizada em sua criação. Em essência, trata-se de um algoritmo de aprendizado autônomo capaz de criar vídeos falsos a partir de imagens e cliques pré-existentes, normalmente mediante a sobreposição digital do rosto de uma pessoa ao corpo de outra em um vídeo. Essa tecnologia emergiu no final de 2017, quando um usuário anônimo da plataforma *Reddit*, sob o pseudônimo “*deepfakes*”, divulgou os primeiros vídeos falsos de conteúdo pornográfico envolvendo atrizes famosas.

Exemplos iniciais incluíam supostas cenas íntimas de celebridades como Daisy Ridley e Gal Gadot, que circulavam como se fossem reais. Posteriormente, após a investigação de outros

usuários é que se confirmou tratar-se de montagens digitais, dado que o autor original não rotulou os vídeos explicitamente como falsos. Em resposta, no início de 2018 o *Reddit* banuiu o fórum dedicado a *deepfakes* e sites pornográficos adotaram políticas para remover esse tipo de conteúdo, embora a disseminação já tivesse ganho impulso próprio em outras plataformas.

Do ponto de vista técnico, a criação de *deepfakes* tornou-se altamente acessível ao público comum. O software original foi disponibilizado em código aberto, permitindo que usuários em geral o utilizassem e aperfeiçoassem. Atualmente, qualquer pessoa com um computador doméstico mediano e uma placa gráfica razoável pode, sem conhecimento avançado de programação, produzir vídeos falsos com grau de realismo preocupante. Existem aplicativos móveis com funcionalidades similares (por exemplo, o *FakeApp*), capazes de realizar filtros faciais e montagens ainda que com menor fidelidade democratizando ainda mais o acesso a essa tecnologia. Com isto, a evolução dos *deepfakes* eliminou barreiras técnicas que antes limitavam a manipulação audiovisual sofisticada a agentes especializados, o que agrava seu potencial de uso indevido.

Embora existam usos recreativos ou artísticos para *deepfakes* como vídeos humorísticos trocando rostos de atores famosos, foi nos usos ilícitos que essa tecnologia se popularizou e causou maior alarme. O caso paradigmático de 2017 evidenciou a vocação inicial dos *deepfakes* para a chamada “pornografia não consensual”, ao inserir celebridades em cenas de sexo fictícias.

8

Observa-se que pesquisas posteriores confirmaram que essa tendência permanece: em 2019, estimava-se que 96% de todos os vídeos *deepfakes* na internet tinham conteúdo pornográfico, sendo as vítimas mulheres em 100% dos casos nesses vídeos. Tais montagens de cunho sexual são frequentemente utilizadas para coagir, humilhar e atacar moralmente as mulheres retratadas.

As *deepfakes* são rotineiramente empregados para produzir conteúdo sexual falso que expõe mulheres a “situações de chantagem, humilhação pública e sofrimento psicológico”, caracterizando nitidamente um uso ilícito da tecnologia. Importa frisar que o potencial lesivo dos *deepfakes* vai muito além da esfera sexual.

De acordo com Oliveira (2019), afirma que apesar de seu primeiro emprego ter sido na pornografia falsa de celebridades, essa ferramenta pode ser utilizada para diversos delitos, “em especial contra a dignidade sexual e contra a honra”, dada sua facilidade operacional e amplo acesso público. Em outras palavras, qualquer pessoa pode vir a ser vítima de crimes viabilizados pelos *deepfakes*, seja por meio de vídeos difamatórios (atingindo a honra e reputação), falsos

flagrantes em situações vexatórias, ou mesmo extorsões mediante ameaça de divulgação de conteúdo fabricado.

Portanto, a única limitação prática parece ser a imaginação de quem emprega a ferramenta ilicitamente. Assim, os *deepfakes* configuram hoje uma tecnologia ambivalente: ao mesmo tempo em que demonstram o avanço impressionante da IA em gerar imagens realistas, servem de instrumento para novas modalidades de fraude, abuso e violência no meio digital.

Violência de Gênero no Ambiente Digital

A violência de gênero no ambiente digital consiste em atos de agressão, coerção ou humilhação dirigidos contra indivíduos majoritariamente mulheres mediante o uso de ferramentas tecnológicas e plataformas online, em razão de seu gênero. Tais condutas manifestam-se de variadas formas, incluindo assédio moral ou sexual em redes sociais, divulgação não autorizada de conteúdos íntimos (*revenge porn*), ameaças virtuais, exposição da vida privada e, mais recentemente, a produção e disseminação de mídias sintéticas degradantes (caso dos *deepfakes* pornográficos).

Em essência, a tecnologia tem sido utilizada para replicar e ampliar dinâmicas misóginas já existentes *offline*, agora com o poder de alcance global e anonimato proporcionado pela internet. Um exemplo ilustrativo é a prática da pornografia de vingança, definida como a divulgação, sem consentimento, de fotos ou vídeos íntimos originalmente registrados em contexto de confiança (geralmente por ex-parceiros).

O intuito do ofensor, na maioria dos casos, é retaliar o término de um relacionamento ou ferir a mulher emocionalmente, colocando a vítima quase sempre do sexo feminino em situação constrangedora diante de familiares, amigos ou colegas. A literatura aponta que a vítima, nessas situações, sofre clara violação de seus direitos de personalidade, “*principalmente à sua privacidade, imagem e honra*”, dada a exposição não autorizada de sua intimidade. Esse tipo de violência digital reflete padrões culturais de *slut-shaming* e objetificação, nos quais a sexualidade da mulher é explorada para fins de controle e punição social.

Os *deepfakes* agravam e diversificam esse quadro de violência de gênero online. Se no *revenge porn* clássico o agressor difundia material íntimo real obtido sem permissão, agora ele pode fabricar artificialmente imagens ou vídeos falsos, tornando possível vitimar mulheres que jamais tenham se exposto.

Trata-se, como já se apontou, de uma “evolução perversa da pornografia de vingança”, pois amplia exponencialmente o alcance do dano: inocentes podem ter suas faces colocadas em cenas sexuais inventadas ou situações degradantes, enfrentando o mesmo estigma e trauma que decorreriam de um vazamento real. Nesse contexto, as *deepfakes* vêm sendo empregados deliberadamente para atacar mulheres, seja para retaliação pessoal, difamação pública ou simples abuso motivado por misoginia.

Estudos recentes confirmam esse viés de gênero: vídeos falsos de teor sexual vitimizam exclusivamente mulheres, servindo muitas vezes a objetivos de chantagem e humilhação pública. As consequências para as vítimas são severas ansiedade, depressão, danos à reputação e à vida profissional, isolamento social e outros tipos de sofrimento psicológico.

Portanto, observa-se que a violência de gênero mediada por tecnologias digitais se configura hoje como um fenômeno tangível e alarmante, no qual as *deepfakes* despontam como uma das ferramentas mais insidiosas de violação, exigindo respostas efetivas do ordenamento jurídico e da sociedade.

Direitos da Personalidade e a Proteção da Mulher no Ambiente Digital

No ordenamento jurídico brasileiro, os direitos da personalidade tais como a honra, a imagem, a vida privada e a intimidade gozam de tutela especial, sendo reconhecidos como direitos fundamentais pela Constituição Federal (art. 5º, X) e pela legislação infraconstitucional. Esses direitos asseguram a cada indivíduo um âmbito mínimo de dignidade e respeito à sua identidade pessoal, moral e social. No caso das mulheres, a proteção dos direitos da personalidade no ambiente digital mostra-se crucial, pois é exatamente nessa esfera que ocorrem muitas das violações contemporâneas ligadas à violência de gênero.

Verifica-se que os ataques virtuais que visam denegrir a imagem, maculam a honra ou expõe indevidamente a vida íntima de mulheres representam afrontas diretas a esses direitos e, por conseguinte, à própria dignidade da pessoa humana. A tutela jurídica da imagem, privacidade e honra das mulheres tem evoluído para acompanhar os desafios tecnológicos. Situações de abuso como o *revenge porn* ou as *deepfakes* pornográficas constituem, sem dúvida, lesões graves a esses atributos personalíssimos.

De acordo com Teffé (2025), na divulgação não autorizada de cenas íntimas a vítima em geral mulher é colocada em embaraço público e “a lesão à personalidade da vítima é evidente, principalmente à sua privacidade, imagem e honra”. Em outras palavras, a violação tecnológica

de cunho sexual ou moral implica simultaneamente violação à esfera da intimidade (vida privada), à imagem (representação perante terceiros) e à honra (reputação e autoestima) da mulher atingida. Tais valores são resguardados tanto no âmbito civil, que admite reparação por danos morais e materiais, quanto na esfera penal, que prevê a punição de condutas específicas que os ataquem.

Nos últimos anos, o legislador brasileiro adotou medidas importantes visando reforçar a proteção da mulher contra abusos digitais, precisamente salvaguardando seus direitos de personalidade. Destaca-se, por exemplo, a Lei nº 13.772/2018, que alterou o Código Penal para explicitar como crime a produção ou registro não autorizado de conteúdo íntimo de caráter sexual.

Com essa alteração, o artigo 216-B do CP passou a criminalizar “produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual de caráter íntimo e privado sem autorização dos participantes”, incluindo expressamente quem “realiza montagem em fotografia, vídeo ou outro registro” para inserir alguém em conteúdo sexual sem consentimento. Tal dispositivo claramente motivado pelo aumento de casos de pornografia de vingança e situações análogas veio colmatar uma lacuna, protegendo o direito à imagem e à intimidade sexual das mulheres contra incursões tecnológicas abusivas.

11

Observa-se que outra iniciativa legislativa digna de nota é a Lei nº 14.192/2021, que trata da violência política de gênero. Essa norma, embora voltada ao contexto eleitoral e político, pode ser invocada em casos em que *deepfakes* sejam utilizados para desacreditar ou constranger mulheres no espaço público-político, configurando assédio ou discriminação de gênero na política. Trata-se de reconhecer que ataques virtuais misóginos inclusive via falsificações digitais ferem não apenas a vítima individual, mas também a representação feminina nas instituições.

Porém, apesar desses avanços, persiste um consenso de que a tutela dos direitos da personalidade das mulheres no meio digital ainda não é plenamente eficaz diante das novas ameaças tecnológicas. As *deepfakes*, em particular, desafiam os mecanismos tradicionais de proteção, pois permitem forjar violações sem precedentes (como atribuir falsamente à vítima comportamentos ou falas ultrajantes).

Com isto, proteger a mulher no ambiente digital implica não só aplicar rigorosamente as leis existentes que asseguram honra, imagem e privacidade, mas também interpretá-las e, quando necessário, aprimorá-las para abarcar as situações inéditas geradas pela inteligência

artificial. Portanto, o ordenamento jurídico deve continuar evoluindo para garantir que os direitos da personalidade das mulheres permaneçam invioláveis mesmo frente às transformações tecnológicas, assegurando-lhes um ambiente online mais seguro e respeitoso.

O Enquadramento Jurídico das *Deep Fakes* no Ordenamento Brasileiro

A problemática das *deepfakes* coloca sérios desafios de tipificação no direito penal brasileiro. Atualmente, não existe no Código Penal um tipo penal específico que abarque a produção e a disseminação de conteúdo audiovisual falsificado por inteligência artificial. Diante dessa ausência, juristas e aplicadores da lei têm buscado enquadrar as condutas envolvendo *deepfakes* em tipos penais já existentes, ainda que de forma aproximativa.

Em casos de *deepfakes* de caráter pornográfico, a conduta tende a ser enquadrada nas disposições recentemente introduzidas para coibir a pornografia não consensual (pornografia de vingança). Conforme mencionado, o artigo 216-B do CP (incluído em 2018) penaliza a criação de conteúdo sexual íntimo não autorizado, o que abrange a fabricação de vídeos falsos de sexo envolvendo vítimas reais, graças à referência expressa a montagens audiovisuais.

Além disso, a divulgação desse material pode ser punida pelo artigo 218-C do CP (igualmente criado em 2018 pela Lei 13.718/18), que criminaliza ofertar, trocar ou divulgar cenas de nudez ou sexo sem consentimento, tipificando assim o *revenge porn*. Desse modo, no âmbito da dignidade sexual, pode-se dizer que o ordenamento passou a dispor de mecanismos penais para responsabilizar quem produz ou dissemina *deepfakes* pornográficos não consentidos. De fato, a legislação pátria mostrou-se relativamente ágil nesse ponto, estando “atualizada e pronta para lidar com crimes desta natureza, ao menos no âmbito sexual”.

A dificuldade maior reside nos usos de *deepfakes* fora da seara sexual, os quais não encontram previsão específica na lei penal vigente. As tentativas de enquadramento têm recorrido, nesses casos, aos crimes contra a honra (calúnia, difamação, injúria, previstos nos arts. 138 a 140 do CP). Por exemplo, se um vídeo falso imputa a alguém uma conduta criminoso ou moralmente reprovável, poderia configurar calúnia ou difamação.

Contudo, esses enquadramentos estão longe de ser perfeitos ou suficientes. Uma montagem ultrarrealista mostrando uma pessoa em situação vexatória que não envolva nudez ou crime por exemplo, um profissional público embriagado em local impróprio causa evidente dano reputacional, mas pode escapar das definições estritas dos delitos contra a honra.

Mais recentemente, o tratamento jurídico da matéria foi complementado pelo Decreto nº 12.976, de 20 de maio de 2026, que estabeleceu diretrizes para a proteção das mulheres na internet e para o enfrentamento da violência contra mulheres no ambiente digital. Para fins de aplicação de suas disposições, o Decreto passou a considerar como conteúdo íntimo aquele que exponha nudez, seminudez, ato sexual ou contexto sexualizante, ainda que seja “produzido e manipulado, no todo ou em parte, por sistema de inteligência artificial” ou recurso tecnológico equivalente (BRASIL, 2026, art. 3º, I).

O Decreto também reconhece expressamente como formas de violência contra a mulher em ambiente digital a violência psicológica praticada mediante inteligência artificial ou recurso que altere a imagem ou o som da vítima; a divulgação não consentida de cena de sexo, nudez ou ato libidinoso, relacionada ao art. 218-C do Código Penal; e o registro não autorizado de cena íntima previsto no art. 216-B, “inclusive mediante montagem ou uso de inteligência artificial” (BRASIL, 2026, art. 3º, II, alíneas “e”, “f” e “g”).

Embora o Decreto não crie, por si só, novos tipos penais, sua edição representa importante avanço no reconhecimento jurídico das *deepfakes* como possíveis instrumentos de violência de gênero. A norma aproxima as formas de manipulação audiovisual por inteligência artificial dos tipos penais já existentes e estabelece parâmetros regulatórios destinados à prevenção dos danos, à proteção das vítimas e à responsabilização dos provedores de aplicações de internet.

13

Nesses casos, não há acusação falsa de crime (requisito da calúnia) nem necessariamente “atribuição de fato ofensivo” nos termos tradicionais da difamação é a própria encenação visual que gera o prejuízo moral. Trata-se de uma zona cinzenta, na qual o conteúdo *deepfake* tem aparência lícita (não mostra um ilícito nem nudez) mas produz grave constrangimento ilegal ou violência simbólica contra a vítima. A doutrina aponta que a legislação penal não alcança adequadamente tal situação, “carecendo de previsão legal específica” para coibi-la eficazmente.

Outra possibilidade criminosa habilitada pelos *deepfakes* é a extorsão mediante conteúdo falso. Um agente pode criar um vídeo sexualmente explícito falso de determinada mulher e, em seguida, chantageá-la exigindo dinheiro ou favores sob a ameaça de divulgar o vídeo na internet. Essa conduta configura, em tese, o crime de extorsão (art. 158 CP), independentemente da veracidade do material.

Contudo, a prática evidencia a conveniência de disposições legais mais precisas: por exemplo, tipificar de modo expreso a ameaça de divulgação de *deepfake* difamatório como

forma de extorsão. Autores sugerem que uma reforma legislativa deveria prever que a divulgação ou mesmo a promessa de divulgação de vídeo falso com conteúdo difamatório ou calunioso seja enquadrada explicitamente nos delitos pertinentes (calúnia, difamação, extorsão), para evitar dúvidas interpretativas.

Em síntese, o enquadramento jurídico das *deepfakes* no Brasil ainda é incipiente e fragmentado. Lida-se com um mosaico de normas existentes: crimes contra a honra, dispositivos de pornografia não consensual, extorsão, falsidade ideológica em alguns casos etc., numa aplicação analógica e caso a caso. Essa abordagem remediativa enfrenta limites constitucionais notadamente o princípio da legalidade estrita, que desautoriza interpretações extensivas em matéria penal.

Por isso, há um entendimento crescente de que a via penal necessita atualização específica para acompanhar a sofisticação e o alcance lesivo das *deepfakes*. Enquanto não sobrevier legislação ad hoc, a repressão penal dessas condutas tende a operar de forma limitada, deixando brechas de impunidade ou tratamento insuficiente.

Portanto, observa-se que outros países já se movimentam nesse sentido. Nos Estados Unidos, por exemplo, mais de uma dúzia de entes federativos criminalizaram expressamente o uso de *deepfakes* em pornografia de vingança, e discute-se até mesmo a proibição de certas *deepfakes* em períodos eleitorais, visando proteger a lisura do debate político. Esses precedentes estrangeiros evidenciam caminhos possíveis para o legislador brasileiro enfrentar o problema de forma mais abrangente.

Desafios Jurídicos e Perspectivas de Enfrentamento da Violência de Gênero Mediada por Inteligência Artificial

A ascensão das *deepfakes* como ferramenta de violência de gênero expõe desafios multidimensionais ao direito. Em primeiro lugar, há um desafio jurídico-normativo: o ordenamento precisa adaptar-se rapidamente para acompanhar o ritmo das inovações tecnológicas, algo que tradicionalmente ocorre de forma mais lenta.

Como visto, a falta de tipos penais específicos para condutas possibilitadas pela inteligência artificial gera insegurança jurídica e dificuldades na responsabilização de agressores. Enquanto a lei permanece desatualizada, infratores se valem dessa “zona cinzenta” para perpetrar abusos, muitas vezes transnacionais e anônimos, o que dificulta a identificação e punição efetiva.

Além disso, a natureza viral da internet implica que o dano causado às vítimas é de difícil reparação, pois conteúdos íntimos ou difamatórios, uma vez vazados, espalham-se rapidamente e não há mecanismo eficaz para removê-los completamente da rede. Esse cenário de impunidade relativa e irreversibilidade do dano aprofunda a vulnerabilidade das mulheres online.

Outro desafio relevante reside na capacitação técnica e institucional dos órgãos estatais responsáveis pela persecução penal. As autoridades investigativas e o Poder Judiciário necessitam desenvolver competências especializadas para a identificação, análise e valoração de provas produzidas ou manipuladas em ambientes digitais.

Nesse contexto, a perícia forense computacional assume papel central, ao possibilitar a distinção entre conteúdos autênticos e falsificações tecnicamente sofisticadas, contribuindo para a adequada formação da convicção judicial e para a efetividade da tutela penal.

Em relação ao campo probatório, surge a questão de saber até que ponto um vídeo pode ser tido como prova fidedigna ou contestado sob alegação de possível *deepfake* fenômeno chamado de “efeito *liar’s dividend*”, em que qualquer flagrante em vídeo é desacreditado sob a desculpa de adulteração digital.

Nesse contexto, o Poder Judiciário depara-se com um duplo desafio: por um lado, evitar ser induzido a erro por *deepfakes* produzidas com finalidade maliciosa; por outro, não desconsiderar provas digitais autênticas com base unicamente na alegação abstrata da possibilidade tecnológica de falsificação.

Trata-se de um equilíbrio particularmente sensível, que exige constante atualização técnica dos operadores do Direito, investimentos em tecnologias de detecção automatizada de conteúdos sintéticos e o estabelecimento de protocolos claros e padronizados para a coleta, preservação, análise e valoração de mídias digitais no âmbito processual.

No campo das políticas públicas e da conscientização social, as perspectivas de enfrentamento envolvem ações amplas. Estudos recentes recomendam fortemente a revisão das leis nacionais e a implementação de políticas públicas voltadas à educação digital, proteção de dados e combate à violência online. Isso significa não apenas criar novas normas penais, mas também promover programas educativos que alertem sobre os riscos das *deepfakes* e orientem potenciais vítimas sobre como reagir.

A integração de esforços entre o Poder Legislativo, Judiciário e setores tecnológicos será crucial para uma resposta efetiva. Por exemplo, é urgente envolver as grandes plataformas digitais (redes sociais, sites de vídeo, provedores de conteúdo) no desenvolvimento de

mecanismos de detecção e remoção ágil de *deepfakes* nocivos, bem como na facilitação da identificação dos responsáveis por sua criação e disseminação.

No âmbito das políticas de enfrentamento da violência digital, merece destaque a edição do Decreto nº 12.976, de 20 de maio de 2026, que estabeleceu diretrizes específicas para a proteção das mulheres na internet. A norma adota como princípios a não discriminação, a centralidade da vítima, a proteção da intimidade, da honra e da imagem, a não revitimização e o reconhecimento das múltiplas formas de discriminação capazes de agravar a violência contra a mulher (BRASIL, 2026, art. 2º).

O referido Decreto apresenta uma definição abrangente de violência contra mulheres em ambiente digital, compreendendo os crimes e atos ilícitos que causem danos ou sofrimentos físicos, sexuais, psicológicos, políticos, econômicos ou patrimoniais e que sejam cometidos, facilitados ou agravados, total ou parcialmente, pelo emprego de tecnologias digitais. Entre as modalidades expressamente reconhecidas encontram-se a violência doméstica e familiar praticada por meios digitais, a violência política contra a mulher, a ameaça, a perseguição digital, a violência psicológica cometida por meio de inteligência artificial, a divulgação não consentida de cenas íntimas e a realização de montagens ou manipulações de caráter sexual (BRASIL, 2026, art. 3º, II).

16

No que se refere especificamente às *deepfakes*, o Decreto reconhece como conteúdo íntimo a imagem, o vídeo, o áudio, a mensagem escrita ou a combinação desses elementos que exponha nudez, seminudez, ato sexual ou contexto sexualizante, mesmo quando o conteúdo tenha sido produzido ou manipulado, total ou parcialmente, por sistema de inteligência artificial ou tecnologia equivalente (BRASIL, 2026, art. 3º, I). Essa definição é relevante porque afasta a ideia de que somente conteúdos íntimos originalmente verdadeiros mereceriam proteção jurídica, abrangendo também os materiais sintéticos que falsamente atribuam à vítima comportamentos ou exposições de natureza sexual.

A norma também atribui deveres específicos aos provedores de aplicações de internet. O art. 4º prevê sua responsabilização em caso de falha sistêmica na indisponibilização imediata de conteúdos que configurem crimes ou atos ilícitos praticados contra mulheres, exigindo a adoção de medidas adequadas de prevenção e remoção e de mecanismos destinados a impedir a circulação massiva desses materiais (BRASIL, 2026, art. 4º). O art. 5º, por sua vez, determina a indisponibilização de conteúdos ilícitos em resposta às notificações regularmente apresentadas,

assegurando procedimentos de comunicação, avaliação e contestação das decisões adotadas pelas plataformas (BRASIL, 2026, arts. 5º e 6º).

Em relação aos conteúdos íntimos gerados por terceiros, o Decreto determina que os provedores promovam sua indisponibilização no prazo de até duas horas após a notificação da vítima ou de seu representante. Além da remoção de toda a aplicação, o material deverá ser digitalmente marcado para que eventuais tentativas de reenvio sejam bloqueadas automaticamente, conforme futura regulamentação da autoridade competente (BRASIL, 2026, art. 7º, §§ 1º e 4º).

Também foram estabelecidas medidas específicas para os ataques coordenados contra mulheres. O art. 8º determina que as plataformas adotem providências técnicas e proporcionais para reduzir o alcance e a visibilidade dessas ações, independentemente de notificação prévia, sempre que identificarem indicadores de sua ocorrência. A atuação deverá ser prioritária nos casos de violência política contra a mulher e quando a vítima possuir exposição pública em razão de suas atividades profissionais, especialmente quando os ataques tiverem a finalidade de constrangê-la, silenciá-la ou restringir sua participação pública (BRASIL, 2026, art. 8º).

No campo da prevenção, os arts. 9º e 10 do Decreto proíbem que os provedores de aplicações de internet promovam a geração ou a modificação de conteúdo íntimo de terceiros mediante inteligência artificial ou recurso que altere a imagem ou o som da vítima. As aplicações baseadas em inteligência artificial também deverão implementar salvaguardas técnicas e procedimentais capazes de identificar e bloquear solicitações destinadas à produção desses conteúdos (BRASIL, 2026, arts. 9º e 10).

Apesar de sua relevância, o Decreto nº 12.976/2026 não institui novo tipo penal para a produção e a divulgação de *deepfakes*. Sua função consiste principalmente em definir diretrizes, reconhecer modalidades de violência digital e disciplinar deveres preventivos e reativos dos provedores de aplicações de internet. A criação de crimes e penas permanece submetida ao princípio da reserva legal, exigindo a aprovação de lei em sentido formal.

Nesse contexto, encontra-se em tramitação o Projeto de Lei nº 3.821/2024, destinado a inserir o art. 216-C no Código Penal. A proposta pretende tipificar as condutas de manipular, produzir ou divulgar, por qualquer meio, conteúdo falso de nudez ou ato sexual gerado por inteligência artificial ou por outros meios tecnológicos, estabelecendo pena de reclusão de dois a seis anos e multa, quando o fato não constituir crime mais grave. O projeto também prevê causas de aumento quando a vítima for mulher, criança, adolescente, pessoa idosa ou pessoa

com deficiência, bem como quando houver disseminação em massa por redes sociais ou plataformas digitais.

O Projeto de Lei nº 3.821/2024 também propõe acrescentar o art. 326-C ao Código Eleitoral, criminalizando a criação, divulgação ou compartilhamento de imagens sexualmente explícitas ou simuladas, manipuladas por inteligência artificial, envolvendo candidatos ou candidatas. Para essa modalidade, o texto prevê pena de reclusão de dois a oito anos, além de causas de aumento e possíveis consequências eleitorais quando a conduta for praticada por candidato.

Em 19 de julho de 2026, a página oficial do Senado Federal indicava que o Projeto de Lei nº 3.821/2024 permanecia em tramitação, com situação de “aguardando despacho”. Consequentemente, as disposições propostas, incluindo a criação do art. 216-C do Código Penal, ainda não constituem legislação vigente.

A tramitação dessa proposta demonstra o reconhecimento legislativo de que os dispositivos atualmente existentes, embora permitam a responsabilização penal em determinadas situações, não abrangem de maneira suficientemente clara e uniforme todas as condutas relacionadas à produção e à disseminação de *deepfakes* de conteúdo sexual. A eventual criação de um tipo penal específico poderá reduzir as controvérsias interpretativas, reforçar a observância do princípio da legalidade penal e conferir maior proteção às vítimas.

18

No âmbito legislativo, discute-se a elaboração de uma lei específica sobre *deepfakes*, que contemple os aspectos técnicos e jurídicos da sua produção e disseminação, preenchendo lacunas hoje existentes. Tal lei poderia tipificar condutas, agravar penas quando o crime envolver motivação de gênero, e prever medidas de apoio às vítimas (como *takedown* rápido de conteúdo).

Porém, no plano preventivo, é indispensável fomentar a conscientização social. Afinal, como destacam Castella e Karvat (2025), compreender os riscos e usos potencialmente abusivos das *deepfakes* é essencial para construir “um ambiente virtual mais seguro e acolhedor para as mulheres”.

Portanto, o enfrentamento da violência de gênero mediada por inteligência artificial exige uma resposta multifacetada, com isso, os desafios jurídicos do aprimoramento legislativo à capacitação técnica do sistema de justiça devem ser tratados com prioridade e urgência, sob pena de a sociedade permanecer vulnerável a práticas lesivas que corroem a privacidade, a honra e a integridade das pessoas.

Paralelamente, mostra-se imprescindível a promoção de uma mudança cultural de modo a fomentar a intolerância a práticas de violência digital contra as mulheres e a estimular respostas sociais e institucionais céleres e eficazes diante dessas ocorrências. Somente a partir da articulação entre um arcabouço normativo atualizado instituições devidamente capacitadas e sociedade civil consciente será possível mitigar os riscos trazidos pelas *deepfakes* e pela IA maliciosa, garantindo que o avanço tecnológico esteja a serviço do bem-estar, da igualdade e da dignidade humana e não da perpetuação de violência e da discriminação de gênero.

CONSIDERAÇÕES FINAIS

Evidenciou-se com a presente pesquisa, que a inteligência artificial, embora represente um marco de progresso tecnológico, tem sido instrumentalizada de forma nociva para a propagação da violência de gênero, especialmente por meio das *deepfakes*, que se consolidam como uma das manifestações mais graves da violência digital contemporânea. A utilização dessas tecnologias para criar conteúdo falsificados de caráter sexual ou difamatório direcionados majoritariamente às mulheres demonstra que o ambiente digital reproduz e, por vezes, intensifica desigualdades históricas de gênero, convertendo-se em espaço de violação sistemática de direitos fundamentais, como a dignidade da pessoa humana, a honra, a privacidade e o direito à imagem.

19

No plano jurídico, a análise revelou que o ordenamento penal brasileiro, embora tenha avançado com a tipificação de condutas relacionadas à pornografia não consentida, ainda apresenta limitações importantes frente às especificidades das *deepfakes*. A aplicação de tipos penais genéricos, como os crimes contra a honra ou dispositivos voltados à dignidade sexual, mostra-se insuficiente para abarcar todas as nuances dessas novas formas de violência, sobretudo quando os conteúdos falsificados não envolvem nudez explícita, mas produzem elevado dano moral e social à vítima.

Verificou-se, ainda, que o enfrentamento desse fenômeno exige uma atuação que ultrapasse a esfera penal, envolvendo o aprimoramento legislativo, a capacitação dos operadores do Direito, a atuação das plataformas digitais e o fortalecimento de políticas públicas voltadas à prevenção e à proteção das vítimas.

Por fim, conclui-se que o enfrentamento da violência de gênero propagada por meio da inteligência artificial exige respostas urgentes, articuladas e multidisciplinares. A consolidação de um ambiente digital mais seguro e igualitário passa pelo reconhecimento das *deepfakes* como

instrumento de violência, pela atualização legislativa e pela promoção de uma cultura jurídica e social comprometida com a proteção da dignidade feminina. Assim, o estudo reafirma a centralidade do Direito na mediação dos impactos tecnológicos, destacando seu papel essencial na defesa dos direitos fundamentais diante dos desafios impostos pela era digital.

REFERÊNCIAS

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Rio de Janeiro, RJ: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 19 jul. 2026.

BRASIL. **Lei nº 13.718, de 24 de setembro de 2018.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13718.htm. Acesso em: 19 jul. 2026.

BRASIL. **Lei nº 13.772, de 19 de dezembro de 2018.** Altera a Lei nº 11.340, de 7 de agosto de 2006, e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar e para criminalizar o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13772.htm. Acesso em: 19 jul. 2026.

BRASIL. **Lei nº 15.123, de 24 de abril de 2025.** Altera o art. 147-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para estabelecer causa de aumento de pena no crime de violência psicológica contra a mulher quando praticado com o uso de inteligência artificial ou de qualquer outro recurso tecnológico que altere imagem ou som da vítima. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15123.htm. Acesso em: 19 jul. 2026.

BRASIL. **Decreto nº 12.976, de 20 de maio de 2026.** Estabelece diretrizes para a proteção de mulheres na internet e para o enfrentamento da violência contra mulheres em ambiente digital. *Diário Oficial da União*: Brasília, DF, 21 maio 2026.

BRASIL. Senado Federal. **Projeto de Lei nº 3.821, de 2024.** Altera o Código Penal para tipificar o crime de conteúdo sexual manipulado por inteligência artificial e o Código Eleitoral para tipificar a manipulação de imagens de conteúdo sexual envolvendo candidatos ou candidatas. Brasília, DF: Senado Federal, 2024. Em tramitação.

CASTELLA, Thaila Camila; KARVAT, Jacieli Santos. *O impacto dos deep fakes na violência digital: uma análise do uso de IA e a violação da privacidade e dignidade feminina no Brasil*. Joinville: Faculdade Unisociosc de Santa Catarina, 2025. Trabalho de Conclusão de Curso (Bacharelado em Direito).

DINIZ, Pedro David Barreto. Os desafios regulatórios e a necessidade de tutela jurídica frente à proliferação de deepfakes. **Revista Tópicos**, v. 1, n. 1, p. 1–25, 2025. DOI: 10.5281/zenodo.15750005. Disponível em: <https://doi.org/10.5281/zenodo.15750005>. Acesso em: 28 jan. 2026.

MANUEL, Garcia Isaías; SÁ, Vítor J.; GOMES, Paulo Veloso; MARQUES, António; PEREIRA, Javier. *Estudo da utilização de deepfakes no ciberespaço, impacto e suas consequências no ambiente social*. In: **CAPSI 2022 – 22ª Conferência da Associação Portuguesa de Sistemas de Informação**, Braga, 2022. p. 221–233. DOI: 10.18803/capsi.v22.221-233.

MEDON, Filipe. O direito à imagem na era das deepfakes. *Revista Brasileira de Direito Civil – RBDCivil*, Belo Horizonte, v. 27, p. 251–277, jan./mar. 2021. DOI: 10.33242/rbdc.2021.01.011. MOMBACH, Vanessa Vieira; BRACHTVOGEL, Caterine de Moura; ARNHOLD, Ana Laura; SCHWENGBER, Maria Simone Vione. *Mulheres, tecnologias e violências de gênero: uma revisão bibliográfica narrativa*. In: **Debates sobre Inteligência Artificial (D.I.A.)**, 2020. Disponível em: <https://periodicos.capes.gov.br>. Acesso em: 08 out. 2025.

OLIVEIRA, Pedro Lucas Santos de. *As implicações do deepfakes no ordenamento jurídico brasileiro: questionamentos e soluções*. 2019. 22 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Estadual da Paraíba, Campina Grande, 2019.

SANTOS, Raphael Prieto; CARDIN, Valéria Silva Galdino; TENA, Lucimara Plaza. *Responsabilidade civil por revenge porn e image-based sexual abuse por deepfake e os direitos da personalidade da mulher vítima de violência digital*. **Cuadernos de Educación y Desarrollo**, v. 17, n. 4, p. e8116-e8116, 2025.

SILVA, Humberto Lúcio. *Deepfakes, pornografia de vingança e a proteção jurídica à imagem e à honra da mulher no Brasil*. In: MORAIS, Fausto Santos de; CARMO, Valter Moura do (org.). *Os direitos humanos na era tecnológica III*. Belo Horizonte: Skema Business School; CONPEDI, 2020. p. 4–10. ISBN 978-65-564