III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

DIREITO PENAL E CIBERCRIMES I

D598
Direito penal e cibercrimes I [Recurso eletrônico on-line] organização III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet: Faculdade de Direito de Franca – Franca;

Coordenadores: Clóvis Alberto Volpe Filho, Helen Cristina de Almeida e Lucas Gonçalves da Silva – Franca: Faculdade de Direito de Franca, 2025.

Inclui bibliografia
ISBN: 978-65-5274-370-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: Governança, regulação e o futuro da inteligência artificial.
1. Direito. 2. Políticas Públicas. 3. Tecnologia. 4. Internet. I. III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet (1:2025 : Franca, SP).

CDU: 34

III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

DIREITO PENAL E CIBERCRIMES I

Apresentação

Entre os dias 30 de setembro e 3 de outubro de 2025, a Faculdade de Direito de Franca recebeu o III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet. O evento reuniu acadêmicos, profissionais, pesquisadores e estudantes, promovendo o debate interdisciplinar sobre o impacto das inovações tecnológicas no campo jurídico e nas políticas públicas. A programação envolveu Grupos de Trabalho (GTs) organizados para aprofundar temas específicos, abordando desde o acesso à justiça até as complexidades da regulação tecnológica, com ênfase na adaptação do sistema jurídico aos avanços da inteligência artificial e da automação.

O GT 9 examina as novas fronteiras do direito penal em meio à criminalidade virtual. As comunicações abordam o uso de reconhecimento facial, deepfakes e provas digitais, destacando riscos à privacidade e à integridade processual. O grupo busca construir parâmetros jurídicos que assegurem a proteção de direitos fundamentais diante dos desafios tecnológicos contemporâneos.

QUANDO O CÓDIGO PENAL SILENCIA E O ALGORITMO VIOLA: DEEPFAKE PORNOGRÁFICO COMO NOVA MÁQUINA DE HUMILHAÇÃO DE MULHERES

WHEN CRIMINAL LAW IS SILENT AND THE ALGORITHM VIOLATES: PORNOGRAPHIC DEEPFAKE AS A NEW MACHINE OF HUMILIATION AGAINST WOMEN

Ana Alice Oliveira Prado [1]
Maria Eduarda Santana Rodrigues [2]
Caio Augusto Souza Lara [3]

Resumo

O presente estudo analisa o uso de vídeos manipulados por inteligência artificial (deepfakes) como instrumento de violência de gênero digital. Tais práticas, que afetam majoritariamente mulheres, configuram formas contemporâneas de exposição não consensual e ataque à dignidade. Investiga-se a insuficiência da legislação penal brasileira diante dessa nova configuração de crime, propondo diretrizes para sua tipificação adequada. Com base em doutrinas jurídicas e experiências internacionais, a pesquisa visa contribuir para a atualização normativa e para a promoção de políticas públicas de proteção às vítimas.

Palavras-chave: Violência de gênero, Deepfake, Direito penal, Crimes digitais, Dignidade da mulher

Abstract/Resumen/Résumé

This study examines the use of AI-generated manipulated videos (deepfakes) as a tool of digital gender-based violence. These practices, which mainly affect women, represent a contemporary form of non-consensual exposure and dignity violation. It explores the insufficiency of Brazilian criminal law to address such crimes, proposing legislative updates. Based on legal doctrine and comparative international cases, this research aims to contribute to normative improvement and the development of public policies to protect affected women.

Keywords/Palabras-claves/Mots-clés: Gender violence, Deepfake, Criminal law, Digital crimes, Women's dignity

[1] Graduanda em Direito, modalidade integral, pelo Centro Universitário Dom Helder.

[2] Graduanda em Direito, modalidade integral, pelo Centro Universitário Dom Helder.

[3] Pró-Reitor de Pesquisa do Centro Universitário Dom Helder. Membro da Diretoria do CONPEDI.

1. CONSIDERAÇÕES INICIAIS

A presente pesquisa propõe uma análise crítica do uso de *deepfakes* pornográficos como forma emergente de violência de gênero, com ênfase em seus impactos simbólicos, jurídicos e sociais sobre a dignidade, a identidade e a privacidade das mulheres. Parte-se da compreensão de que a arquitetura tecnológica das imagens sintéticas, mediada por algoritmos de inteligência artificial, opera como instrumento sofisticado de dominação, manipulação e exposição pública. Nesse sentido, essas manipulações visuais não apenas falsificam rostos, mas reconfiguram narrativas de subjugação sobre corpos femininos, intensificando a lógica patriarcal sob o disfarce da inovação e do anonimato digital.

A escolha do tema justifica-se pelo crescimento expressivo de casos envolvendo a disseminação de conteúdos pornográficos manipulados, com destaque para o ocorrido em 2025 no Colégio Santa Maria, em Belo Horizonte, no qual alunas adolescentes foram vítimas da inserção não consentida de seus rostos em vídeos de teor sexual. O episódio expôs não apenas a gravidade do trauma psíquico sofrido, mas também a insuficiência da resposta institucional frente à complexidade técnica da agressão. Mesmo diante da instauração de inquérito pelo Ministério Público, a ausência de legislação penal específica dificultou a tipificação adequada da conduta, refletindo uma invisibilização estrutural da violência de gênero no ambiente digital.

Sob a ótica jurídico-social, a relevância da pesquisa reside na constatação da incapacidade do ordenamento penal brasileiro em lidar com práticas como os *deepfakes* pornográficos, que escapam às previsões da Lei nº 12.737/2012 (Lei Carolina Dieckmann), da Lei nº 13.718/2018 (Importunação Sexual) e do artigo 218-C do Código Penal. Essa lacuna normativa favorece a perpetuação da violência e revela o descompasso entre o avanço das tecnologias de manipulação e a estagnação do sistema punitivo. Torna-se, portanto, imperativo repensar o papel do Direito Penal na proteção das mulheres frente às novas dinâmicas da agressão digital, incorporando uma perspectiva de gênero e uma compreensão crítica da violência algorítmica.

Do ponto de vista metodológico, adota-se uma abordagem jurídico-sociológica, conforme a classificação de Gustin, Dias e Nicácio (2020), articulando elementos do Direito Penal, da Teoria Feminista e da Criminologia Crítica. Trata-se de uma pesquisa qualitativa, de natureza teórica e exploratória, orientada por raciocínio crítico e sustentada em revisão

bibliográfica especializada. Serão mobilizadas autoras como Judith Butler (2003), Silvia Federici (2018) e Enaura de Paula Bastos (2021), além de relatórios técnicos de organizações como SaferNet e InternetLab. O objetivo é oferecer uma reflexão aprofundada sobre os limites da legislação vigente e propor diretrizes jurídicas e políticas públicas capazes de enfrentar, com a urgência e complexidade que o tema exige, a violência de gênero no contexto digital.

2. LEGISLAÇÃO COMPARADA E O ENFRENTAMENTO JURÍDICO DA VIOLÊNCIA POR *DEEPFAKES*

O avanço acelerado da inteligência artificial tem impactado de forma significativa os sistemas jurídicos ao redor do mundo, gerando novos dilemas no campo da proteção de direitos fundamentais. Entre as tecnologias emergentes, os *deepfakes* se destacam por sua capacidade de manipular imagens, vídeos e áudios com altíssimo grau de realismo, produzindo conteúdos potencialmente lesivos à honra, à imagem e à privacidade das pessoas. Essa técnica tem sido amplamente utilizada como instrumento de violência de gênero, especialmente em sua vertente pornográfica, configurando uma forma contemporânea de agressão simbólica que desafia os instrumentos clássicos de regulação penal.

Sob a perspectiva comparada, os Estados Unidos têm adotado medidas legislativas mais incisivas no enfrentamento dessa prática. Em 2025, foi promulgado o *Take It Down Act*, uma legislação federal que criminaliza a criação e disseminação de conteúdos íntimos manipulados por inteligência artificial sem o consentimento da vítima. A norma prevê penas agravadas para casos que envolvem menores de idade e determina que as plataformas digitais removam o conteúdo denunciado em até 48 horas, sob pena de sanção. Essa obrigatoriedade visa mitigar os efeitos danosos da exposição e promover uma responsabilização mais ágil dos agentes envolvidos.

Além da legislação federal, medidas estaduais complementam o marco regulatório estadunidense. O *Elvis Act*, aprovado no Tennessee, visa garantir o controle individual sobre dados biométricos, como imagem e voz, impedindo seu uso não autorizado em conteúdos sintéticos. Já na Califórnia, a legislação AB-602/730 estabelece penalidades civis e criminais para a manipulação de imagem com finalidade sexual ou difamatória. Essas medidas demonstram que os Estados Unidos têm construído uma estrutura normativa integrada, sensível aos riscos da inteligência artificial e comprometida com a proteção da integridade

digital dos indivíduos.

No Brasil, por outro lado, a resposta legislativa ainda se mostra fragmentada e pouco efetiva. A promulgação da Lei nº 15.123/2025 foi um passo inicial ao reconhecer o uso da manipulação de imagens como agravante da violência psicológica contra a mulher, mas a norma não tipifica diretamente a conduta de manipulação digital. Projetos de lei como o PL 3821/2024, que propõe a criminalização da criação de imagens falsas de nudez ou ato sexual, e o PL 3608/2023, que exige autorização para uso da imagem de pessoas falecidas em ambientes digitais, ainda tramitam sem coordenação sistêmica, dificultando a construção de um marco penal robusto.

Além das lacunas penais, o Brasil também enfrenta limitações na responsabilização civil. A Lei Geral de Proteção de Dados (LGPD) tem sido apontada como um instrumento possível de resposta, principalmente em casos de uso indevido de dados pessoais na criação de *deepfakes*. No entanto, sua estrutura normativa é voltada à proteção de dados e à regulação de tratamentos lícitos, o que reduz sua eficácia frente à gravidade e à especificidade da violência de gênero digital. Ainda que útil para fins indenizatórios, a LGPD não substitui a urgência de tipificações penais que contemplem o dano simbólico e a violação do consentimento.

Outro desafio importante diz respeito à responsabilização das plataformas digitais. Enquanto nos Estados Unidos já existem previsões legais obrigando as empresas a removerem conteúdos nocivos em prazos curtos, no Brasil a discussão ainda é incipiente. A tramitação do projeto de lei das Fake News levanta questões sobre anonimato, dever de moderação e responsabilização de intermediários, mas ainda carece de uma abordagem que incorpore a perspectiva de gênero e a especificidade da violência algorítmica. Sem mecanismos eficazes de controle e cooperação com o Poder Público, as plataformas seguem operando com impunidade estrutural.

A tensão entre liberdade de expressão e proteção contra abusos digitais é outro ponto sensível. Nos Estados Unidos, essa tensão é agravada por uma tradição jurídica fortemente liberal, que muitas vezes se opõe a qualquer forma de regulação de conteúdo. Já no Brasil, prevalece uma abordagem baseada na ponderação de princípios, como a vedação ao anonimato, a dignidade da pessoa humana e a função social da internet. Nesse sentido, é essencial que as propostas legislativas sejam tecnicamente consistentes e democraticamente legitimadas, sem ceder ao populismo punitivista ou ao liberalismo desregulador.

Diante desse cenário, conclui-se que o enfrentamento jurídico à manipulação digital de imagens íntimas exige mais do que respostas pontuais: requer uma estratégia normativa abrangente, interseccional e compatível com os valores constitucionais. É preciso integrar a proteção penal com a regulação civil, a governança digital e as políticas públicas de prevenção, acolhimento e reparação. O combate à violência algorítmica só será efetivo se for capaz de articular tecnologias, instituições e direitos, reconhecendo o impacto desproporcional dessas práticas sobre a dignidade das mulheres e a urgência de uma proteção jurídica condizente com a complexidade do século XXI.

3. VIOLÊNCIA ALGORÍTMICA E GÊNERO: O *DEEPFAKE* COMO TECNOLOGIA DE DOMINAÇÃO

A consolidação dos ambientes digitais como espaços de sociabilidade, exposição e disputa simbólica tem intensificado a emergência de novas formas de violência baseadas em gênero. No centro desse fenômeno, destaca-se a ascensão dos *deepfakes* como ferramentas de manipulação de identidades visuais, atuando em uma zona nebulosa entre o virtual e o real. Por meio da simulação hiper-realista de rostos, vozes e gestos, essas tecnologias forjam narrativas audiovisuais falsas, mas socialmente devastadoras. Trata-se de um tipo de violência que opera não com base em contato físico, mas na reconfiguração simbólica da imagem da vítima, desestabilizando reputações, afetando vínculos sociais e corroendo o senso de realidade.

Ao contrário das agressões tradicionais, os *deepfakes* não requerem proximidade física nem violação direta do corpo da vítima. A violência é mediada por código, disseminada por redes e amplificada por algoritmos de recomendação. A vítima, muitas vezes adolescente ou figura pública, vê-se exposta em contextos de nudez simulada, inserida em conteúdos pornográficos sem jamais ter consentido com tal representação. A eficácia simbólica dessa prática está justamente na sua verossimilhança: quanto mais "crível" a falsificação, maior o impacto social, o dano psicológico e o constrangimento jurídico. O algoritmo, nesse caso, torna-se arma.

Estudos do Oxford Internet Institute e da *MIT Technology Review* demonstram que mais de 95% dos *deepfakes* em circulação têm conteúdo sexual, sendo a maioria esmagadora voltada contra mulheres. Essa estatística não apenas revela um padrão de gênero sistemático,

mas também escancara a reprodução digital da misoginia estrutural. As vítimas são expostas não por acaso, mas porque seus corpos são historicamente objeto de vigilância, controle e consumo. A tecnologia apenas moderniza esse controle, transformando imagens públicas como postagens, selfies e vídeos em matéria-prima para a violência algorítmica.

Nesse contexto, a expressão *revenge porn* mostra-se inadequada para descrever a natureza complexa desse fenômeno. O termo reduz a violência à esfera interpessoal, sugerindo vingança afetiva ou ruptura íntima como motivação. No entanto, a realidade dos *deepfakes* é marcada por anonimato, mercado e cultura. Em substituição, o conceito de *image-based sexual abuse* tem sido adotado por organismos internacionais e pesquisadores críticos, por englobar não apenas a exposição de conteúdo íntimo real, mas também a criação e disseminação de imagens falsas, ameaças, chantagens e usos não autorizados da imagem pessoal.

O cerne do problema reside na violação do consentimento digital. Ao contrário do consentimento físico, que se dá em atos presenciais e tangíveis, o consentimento digital diz respeito ao controle contínuo que cada indivíduo deve ter sobre sua imagem, dados biométricos e representações em ambientes virtuais. Quando algoritmos capturam feições, inserem rostos em vídeos de sexo ou espalham essas manipulações por redes sociais, o que se observa é uma total anulação desse consentimento. A identidade digital da vítima torna-se propriedade de terceiros, e sua reconstrução simbólica passa a servir a fins de humilhação e espetáculo.

A literatura feminista tem desempenhado papel central na denúncia e análise desse tipo de violência. Clare McGlynn e Erika Rackley demonstram como o ambiente digital reatualiza os mecanismos históricos de controle patriarcal, punindo mulheres por sua autonomia, voz ou visibilidade pública. O *deepfake* pornográfico funciona como uma ferramenta de coerção silenciosa, uma punição simbólica para aquelas que ousam existir de forma autônoma na esfera pública. Nesse sentido, a violência algorítmica não é aleatória: ela possui um alvo socialmente definido — as mulheres — e um propósito normativo — reforçar estruturas de submissão.

A complexidade desse fenômeno exige respostas que articulem técnica, política e cultura. Do ponto de vista tecnológico, já existem algoritmos que detectam essas falsificações digitais, marcas digitais invisíveis (*watermarking*) e canais de denúncia automatizada em redes sociais. Mas tais recursos são frequentemente insuficientes diante da velocidade de

disseminação e da lógica de viralização das redes. Por isso, é urgente consolidar um marco normativo que reconheça explicitamente a violência algorítmica como violação dos direitos fundamentais à privacidade, à dignidade e à identidade. Tipificações penais, regulamentações para plataformas e garantias de reparação às vítimas são medidas indispensáveis.

Além do aspecto normativo, o combate ao *deepfake* como violência de gênero exige políticas públicas voltadas à educação digital, ao acolhimento das vítimas e à responsabilização de agentes envolvidos. É preciso também reconhecer que muitas plataformas lucram com a viralização de conteúdos sensacionalistas, inclusive os marcados por violência simbólica. Romper com essa lógica significa desarmar uma engrenagem que lucra com a vulnerabilização sistemática das mulheres.

4. CONSIDERAÇÕES FINAIS

A presente pesquisa demonstrou que os *deepfakes* pornográficos configuram uma nova forma de violência de gênero digital, marcada por alta complexidade técnica, baixa visibilidade institucional e graves repercussões sobre a integridade psíquica, social e jurídica das vítimas. Trata-se de uma prática que combina elementos de agressão simbólica, exposição pública e manipulação algorítmica, desafiando os parâmetros tradicionais de proteção penal e evidenciando a necessidade de um redesenho normativo que leve em consideração as especificidades da violência baseada em imagem e gênero.

A análise comparada revelou que, embora o Brasil tenha avançado pontualmente em iniciativas legislativas, ainda carece de um marco regulatório robusto e integrado para enfrentar essa modalidade de crime. A ausência de tipificação penal específica, aliada à lentidão na responsabilização de plataformas e agressores, perpetua um cenário de impunidade e normalização da violência digital. A experiência de países como os Estados Unidos indica caminhos possíveis de regulamentação, mas também evidencia os riscos de tensionamento com a liberdade de expressão, o que demanda soluções equilibradas e contextualmente ajustadas à realidade brasileira.

Conclui-se que a construção de um ambiente digital justo, seguro e democrático exige mais do que inovações legislativas. Requer uma atuação coordenada entre o Direito Penal, as políticas públicas e os mecanismos técnicos de prevenção e resposta. É urgente reafirmar que o respeito ao consentimento, à privacidade e à dignidade das mulheres deve ser

um imperativo ético da era digital. Proteger os corpos simbólicos e identidades femininas diante das novas tecnologias é um desafio civilizatório que interpela o compromisso coletivo com a liberdade, a justiça e a equidade em sua forma mais concreta.

REFERÊNCIAS BIBLIOGRÁFICAS

BASTOS, Enaura de Paula. *Feminismo, poder e direitos fundamentais*. Belo Horizonte: D'Plácido, 2021.

BRASIL. *Lei nº 12.737, de 30 de novembro de 2012*. Dispõe sobre a tipificação criminal de delitos informáticos. *Diário Oficial da União*: seção 1, Brasília, DF, 3 dez. 2012.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais – LGPD. *Diário Oficial da União*: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. *Lei nº 13.718, de 24 de setembro de 2018*. Altera o Decreto-Lei nº 2.848/40 (Código Penal), para prever crimes contra a dignidade sexual. *Diário Oficial da União*: seção 1, Brasília, DF, 25 set. 2018.

BRASIL. *Lei nº 15.123, de 10 de março de 2025*. Agrava penas de violência psicológica praticada por meio de tecnologias de manipulação de imagem. *Diário Oficial da União*: seção 1, Brasília, DF, 11 mar. 2025.

BUTLER, Judith. *Problemas de gênero: feminismo e subversão da identidade*. Tradução de Renato Aguiar. Rio de Janeiro: Civilização Brasileira, 2003.

FEDERICI, Silvia. *O ponto zero da revolução: trabalho doméstico, reprodução e lutas feministas*. Tradução de Verena Glass. São Paulo: Elefante, 2018.

GUSTIN, Miracy; DIAS, Cristiana Fortini; NICÁCIO, Karine. *Metodologia da pesquisa jurídica*. 2. ed. Belo Horizonte: Fórum, 2020.

INTERNETLAB. *Violência de gênero online: uma abordagem interseccional*. São Paulo: InternetLab, [s.d.]. Disponível em: https://www.internetlab.org.br. Acesso em: jul. 2025.

MCCLYNN, Clare; RACKLEY, Erika. *Image-based sexual abuse: reforming criminal laws*. Oxford Journal of Legal Studies, Oxford, v. 38, n. 2, p. 285-305, 2018.

MIT TECHNOLOGY REVIEW. *The state of deepfakes: 2023 report*. Cambridge, MA: MIT, 2023. Disponível em: https://www.technologyreview.com. Acesso em: jul. 2025.

OXFORD INTERNET INSTITUTE. *Deepfakes and synthetic media: threats and countermeasures*. Oxford: University of Oxford, 2022. Disponível em: https://www.oii.ox.ac.uk. Acesso em: jul. 2025.

SAFERNET BRASIL. *Relatório anual sobre crimes de ódio e violência online*. São Paulo: SaferNet, 2024. Disponível em: https://www.safernet.org.br. Acesso em: jul. 2025.