

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

DIREITO PENAL E CIBERCRIMES II

D598

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

Coordenadores: Renan Posella Mandarino, Fábio Cantizani Gomes e Ana Carolina de Sá Juzo – Franca: Faculdade de Direito de Franca, 2025.

Inclui bibliografia

ISBN: 978-65-5274-364-0

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 II

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 foca nos crimes digitais e na responsabilização penal de condutas praticadas em ambiente virtual. As pesquisas discutem pornografia não consentida, cyberbullying, discursos de ódio e a eficácia das investigações digitais. O grupo ressalta a necessidade de adequação legislativa e de políticas públicas voltadas à prevenção e repressão dos cibercrimes.

DEEPFAKES COMO MECANISMO DE VIOLÊNCIA VIRTUAL CONTRA MULHERES: A UTILIZAÇÃO DA INTELIGÊNCIA ARTIFICIAL COMO FERRAMENTA DE FOMENTO À DISCRIMINAÇÃO

**DEEPFAKES AS A MECHANISM OF ONLINE VIOLENCE AGAINST WOMEN:
THE USE OF ARTIFICIAL INTELLIGENCE AS A TOOL FOR PROMOTING DISCRIMINATION**

**Marcela Coimbra Machado
Rafaela Rodrigues de Oliveira Freitas**

Resumo

O estudo analisa de que maneira o uso de ferramentas de inteligência artificial pode contribuir para a discriminação de mulheres no ambiente virtual. Com ênfase na tecnologia de deepfake, a pesquisa tem como objetivo compreender como esse recurso pode ser instrumentalizado como forma de violência digital e quais os caminhos legais possíveis para o enfrentamento desse fenômeno. Busca-se contribuir para a mitigação do problema apresentado por meio do método científico dedutivo, com base em pesquisa bibliográfica em fontes digitais.

Palavras-chave: Deepfake, Inteligência artificial, Discriminação, Violência de gênero

Abstract/Resumen/Résumé

The study analyzes how the use of artificial intelligence tools can contribute to the discrimination of women in virtual environments. With an emphasis on deepfake technology, the research aims to understand how this resource can be instrumentalized as a form of digital violence and what legal approaches are possible to confront this phenomenon. The study seeks to contribute to the mitigation of the identified issue through the deductive scientific method, based on bibliographic research using digital sources.

Keywords/Palabras-claves/Mots-clés: Deepfake, Artificial intelligence, Discrimination, Gender-based violence

INTRODUÇÃO

Com o avanço da tecnologia e o fácil acesso à internet, a utilização da inteligência artificial (IA) tornou-se parte do cotidiano das pessoas. Ferramentas desenvolvidas por grandes empresas como Google, OpenAi, Microsoft dentre outras, são capazes de simular a inteligência humana através de algoritmos treinados com um grande acúmulo de dados, ou seja, é através do comportamento humano que as máquinas aprendem a reproduzir condutas e corresponder às demandas de quem as procura de maneira rápida e eficaz, seja para responder questões, auxiliar em tarefas no dia a dia e até mesmo a criar elementos visuais.

Entretanto, com a facilidade de acesso à essas máquinas treinadas, um perigo surge a partir de seu uso na modificação de imagens de indivíduos com a intenção de prejudicar sua reputação, principalmente de mulheres. O chamado “*deepfake*”, expressão que surge da união dos termos “deep” – extraída da tecnologia deep learning, “aprendizado profundo” – e “fake”, que significa “falso”, em inglês, é que denomina essas falsas imagens elaboradas com base em técnicas de inteligência artificial que possuem um alto grau de realismo.

Essas imagens alteradas, com o único objetivo de afetar a reputação de mulheres é um ato de opressão, portanto, se enquadram como um tipo de violência, e como ocorrem por meio da internet, o seu ambiente de atuação é o virtual. Ao lesar bens jurídicos tutelados pelo o Direito como um todo, como a honra e a vida dessas que acabam sendo vítimas dos abusos da utilização desse tipo de inteligência, nota-se a relevância do tema proposto, uma vez que, combate esse reforço à discriminação que mulheres vivenciam dentro das redes sociais, já que a menoridade feminina continua a se propagar na utilização desse meios ao reforçar padrões de opressão.

Diante do exposto, justifica-se a necessidade do presente estudo como forma de ampliar o conhecimento acerca dos *deepfakes* como ferramenta que contribui para a prática de crimes virtuais podendo ser penalizado pelo Direito Penal e também de sua capacidade em distorcer a realidade de maneira a fomentar a discriminação contra indivíduos mais vulneráveis, sobretudo de mulheres. Tendo como tema principal, a análise da violência virtual promovida pelo mal uso dessas máquinas treinadas por algoritmos na alteração de imagens fomentando a opressão contra mulheres.

O trabalho desenvolve-se a partir da seguinte indagação: de que maneira as ferramentas de inteligência artificial, em especial os *deepfakes*, vêm sendo utilizadas como mecanismos de fomento à discriminação contra mulheres no ambiente virtual, e quais estratégias podem ser adotadas para combater essa prática?

Em razão do que foi demonstrado, almeja-se analisar de que maneira a utilização indevida de sistemas inteligentes pode fomentar a violência de gênero no ambiente virtual. Ademais, objetiva-se examinar de maneira crítica como a falta de ética nos meios digitais contribui para um tratamento discriminatório, julgar como a legislação brasileira pode reprimir esse mal uso da tecnologia, ilustrar por meio da Lei 15.123/25 um possível meio eficaz de combate à essa prática criminosa que norteia o estudo em questão e explanar maneiras de mitigação de conteúdo sintéticos manipulados.

Nesse contexto parte-se da hipótese de que a falta de rigorosidade de plataformas de inteligência artificial frente ao uso descontrolado de suas ferramentas contribui para a discriminação de mulheres no meio digital, por outro lado, com uma legislação específica e medidas de sanções severas, mulheres poderão ser respeitadas e mesmo na ocorrência desse tipo de crime virtual poderão encontrar amparo na justiça brasileira.

A fim de responder a questão apresentada, o estudo em questão se utilizará do método científico dedutivo, uma vez que, a conclusão partirá da obtenção de dados gerais já constatados e aplicáveis a uma verdade individual aos crimes cometidos com base no uso de *deepfakes* contra mulheres no ambiente virtual.

DESENVOLVIMENTO

A inteligência artificial pode ser usada em diversos contextos e possui como objetivo produzir conhecimento para auxiliar na resolução de problemas, dentre suas funções está a manipulação de imagens, útil para diferentes finalidades, como a própria diversão do usuário. Porém, o seu uso vem sendo deturpado para fins ilícitos, ao modificar imagens e vídeos como se fossem verdadeiros, usuários, em sua maioria homens, têm-se utilizado de soluções inteligentes para constranger, humilhar, ameaçar e expor mulheres, sejam elas presentes em seu convívio social ou até mesmo figuras públicas, como ocorreu nas últimas eleições, em outubro do ano passado, segundo o G1, independentemente da posição política da candidata, seja ela de direita ou esquerda, a manipulação de vídeos e fotos ocorre contra qualquer uma delas, de acordo com o mesmo portal de notícias só em 2023 circularam na internet quase 100 mil vídeos falsos e em sua grande maioria tem mulheres como alvo¹.

Para fazer o uso de ferramentas algorítmicas ofertadas por grandes empresas tecnológicas basta fornecer dados básicos como nome e e-mail, dessa forma, cria-se uma conta. É evidente que, o aproveitamento desses mecanismos pode ser realizado por qualquer indivíduo de maneira facilitada, já que não é necessário pagamento, salvo nos casos que se

deseje uma versão evoluída da plataforma com recursos especiais que a versão original não tenha, e muito menos um número de documento oficial que identifique com precisão quem está por trás das solicitações e perguntas. Sendo assim, há uma dificuldade em localizar e punir aquele que produz *deepfakes* e os dissemina através de publicações em redes sociais.

Outro problema enfrentado no combate às mídias digitais falseadas por IA, é por parte das vítimas, que além de sofrerem impactos psicológicos severos como ansiedade e isolamento social, lidam com dificuldades em remover o conteúdo das plataformas, já que cada rede social possui sua própria diretriz, que podem conflitarem entre si. Ainda assim, pode-se denunciar a publicação, função que é disponibilizada em todas as redes sociais, mas se a publicação continuar se perpetuando cabe ação judicial, sendo necessário provas claras, outro obstáculo para as pessoas lesadas. Em outras palavras, é preciso provar que estão sendo vítimas de *deepfakes* e que aquelas imagens e vídeos não foram realizados por conta própria, mas que foram fruto de manipulação gerada a partir de ferramentas algorítmicas.

Diante da proposta da inteligência artificial, de servir para ajudar na busca de respostas e no auxílio a questões emblemáticas, cabe às pessoas utilizá-la de maneira ética, já que as plataformas são disponibilizadas democraticamente a qualquer indivíduo sem distinção e com um propósito legítimo para sua funcionalidade. À vista disso, ressalta-se a importância da conscientização realizada pelas próprias plataformas desde seu primeiro uso em relação aos usuários, além de outras medidas preventivas e de repressão. Como aponta o autor do estudo sobre *deepfakes*, Will Hawkins, produzido na Universidade de Oxford:

Existe uma necessidade urgente de proteções técnicas mais robustas, políticas de plataforma mais claras e aplicadas de forma mais proativa, além de novas abordagens regulatórias para lidar com a criação e a distribuição desses modelos de IA prejudiciais².

Os *deepfakes* são feitos exclusivamente para criar narrativas falsas focando em danos à reputação, dignidade e vida das vítimas. Nesse sentido, o mesmo estudo revela que em 15 minutos com base em 20 fotos de referência, mais de 35 mil softwares podem gerar imagens de pessoas de modo desenfreado já que estão disponíveis para download de forma pública². Em decorrência dessa facilidade de criação e de disseminação, amplia-se o alcance e a intensidade da violência perpetuando vieses e a impunidade de quem os produz.

Um dos principais obstáculos enfrentados na mitigação do uso indevido de I.A, é a falta de legislação específica para lidar com os *deepfakes* promovidos contra as mulheres. A maioria das leis atuais não contempla diretamente essa tecnologia, tornando difícil punir quem cria ou distribui esses conteúdos, principalmente quando há intenção de prejudicar terceiros. Além disso, os marcos legais muitas vezes esbarram em questões de liberdade de expressão,

dificultando a delimitação clara entre uso ilícito e uso legítimo. Na legislação brasileira, há leis que defendem a mulher e que podem ser usadas no combate a esse tipo de violência virtual, como a Lei Maria da Penha, com mecanismos para coibir a violência doméstica e familiar contra a mulher, a lei Carolina Dieckmann que também pode ser utilizada no mesmo contexto, pois visa a proteção da segurança e privacidade dos dados pessoais no meio digital, tipificando crimes cibernéticos, por exemplo invasão de dispositivos tecnológicos pessoais da vítima, punindo o criminoso.

Ademais, a única lei que aborda o tema discutido é a Lei 15.123/25, que relaciona o Direito Penal Brasileiro e a tecnologia, reconhecendo o impacto dos *deepfakes* na prática de crimes de violência psicológica contra a mulher. Mesmo que a lei seja um avanço na regulação de conteúdos digitais na justiça brasileira, ela ainda é ampla e insuficiente, visto que, não contempla as particularidades e desafios impostos pelos *deepfakes*, exigindo, assim, interpretações jurídicas mais aprofundadas. A necessidade de mudanças na legislação é de extrema urgência, para assim tipificar, ainda mais detalhadamente, os crimes relacionados ao uso indevido das inteligências artificiais contra as mulheres, aumentando a gravidade de acordo com o uso pretendido pelo criminoso do *deepfake*.

No campo tecnológico, a detecção de *deepfakes* ainda enfrenta grandes desafios. Os algoritmos de criação de mídias estão cada vez mais sofisticados, enquanto os mecanismos de identificação nem sempre conseguem acompanhar essa evolução. Detectar um *deepfake* com precisão requer tecnologias avançadas, muitas das quais ainda estão em desenvolvimento e nem sempre acessíveis a governos, empresas ou cidadãos comuns. A detecção se torna difícil, pois as tecnologias capazes de identificar estão concentradas somente para as grandes produtoras de IA, limitando o seu uso. A partir disso, percebe-se a necessidade da educação midiática, para assim a população saber e identificar a disseminação de conteúdo falso, e juntamente com a tipificação da conduta, não produzir *deepfakes*. O problema do presente estudo, não causa prejuízos somente em âmbito nacional, mas também em âmbito internacional, portanto deve ser estimulado um cooperação internacional que combata esses crimes.

O combate aos *deepfakes*, especialmente aqueles usados para atacar, expor ou difamar mulheres, exige uma abordagem multifacetada. As principais frentes de enfrentamento incluem: educação digital, promover a alfabetização digital é essencial para que as mulheres e a sociedade em geral saibam identificar conteúdos manipulados. Campanhas educativas em escolas, redes sociais e comunidades ajudam a prevenir a disseminação de *deepfakes* e reduzem a vulnerabilidade das vítimas. A conscientização, é

fundamental conscientizar o público sobre os impactos dos *deepfakes* na vida das mulheres, especialmente aqueles usados para fins sexuais ou de violência simbólica. Iniciativas que denunciem o uso dessas tecnologias para perpetuar misoginia, controle e humilhação contribuem para mudar a cultura de permissividade. A responsabilidade das plataformas, das redes sociais e das plataformas digitais precisam adotar políticas rigorosas para remover rapidamente conteúdos falsos e punir usuários que compartilham ou produzem *deepfakes* abusivas, a transparência nos algoritmos e canais eficazes de denúncia são passos importantes também. Por fim, ferramentas de detecção, o desenvolvimento de tecnologias que detectam automaticamente *deepfakes* é essencial. Softwares baseados em inteligência artificial podem identificar manipulações em imagens e vídeos, ajudando tanto na prevenção quanto na responsabilização legal dos agressores.

CONCLUSÃO

O uso de *deepfakes*, tecnologia baseada em inteligência artificial capaz de criar imagens e vídeos hiper-realistas, tornou-se uma grave ferramenta de violência digital contra mulheres. Essa prática vem sendo usada para constranger, expor, humilhar e ameaçar mulheres, frequentemente de forma sexualizada, com o objetivo de destruir reputações e perpetuar a desigualdade de gênero. O fácil acesso às ferramentas de IA, somado à ausência de regulamentação rígida, facilita a criação e disseminação dessas mídias manipuladas, tornando a punição dos agressores extremamente difícil.

A violência por *deepfakes* se insere em um contexto mais amplo de misoginia digital, onde a exposição virtual agrava impactos psicológicos como ansiedade, depressão e isolamento. A resposta a essa nova forma de violência precisa ser urgente e multidisciplinar, visto que, afeta direitos fundamentais como a honra, dignidade, imagem e segurança das vítimas. Entre os principais desafios estão, a falta de legislação específica, vale salientar que as leis mencionadas, Lei Maria da Penha, Lei Carolina Dieckmann e principalmente a Lei 15.123/25, são de extrema importância, pois ajudam na preservação e garantia dos direitos das mulheres ao serem violentadas de forma física, mental ou emocional, caso tenham sua privacidade digital invadidas e impactadas por *deepfakes*. A responsabilidade das plataformas digitais que falham na verificação das postagens também é um desafio, que deve ser desenvolvido. Dentre os impedimentos citados, destaca-se como o mais grave a dificuldade em punir os agentes que cometem esses crimes, uma vez que, em geral, atuam de forma anônima e em escala global.

No atual cenário dos *deepfakes*, é indispensável a tentativa de reverter todos os danos causados, baseados em quatro pilares, o primeiro é a educação, voltada para o ambiente digital para assim promover críticas à população para identificar *deepfakes*. A partir disso, a conscientização pública para haver mais denúncias, tendo assim um respaldo por uma regulamentação legal como a Lei 15.123/25. A gravidade do problema demanda cooperação entre setores jurídicos, tecnológicos, educacionais e sociais, bem como articulação internacional para combater a disseminação transfronteiriça desses conteúdos. Apenas com uma abordagem ética, rigorosa e multidisciplinar será possível proteger efetivamente as mulheres dessa nova forma de violência digital.

Diante do avanço contínuo da inteligência artificial e da crescente sofisticação dos *deepfakes*, torna-se essencial investir em pesquisas que aprimorem os mecanismos de detecção, bem como aprofundem a compreensão dos impactos sociais e psicológicos dessa tecnologia sobre as mulheres. A criação de marcos regulatórios mais específicos e eficazes deve caminhar lado a lado com o desenvolvimento tecnológico, garantindo que o uso indevido da IA seja responsabilizado com agilidade e justiça. Além disso, é urgente promover uma colaboração ativa entre governos, plataformas digitais, sociedade civil e comunidade científica para formular políticas públicas que priorizem a segurança digital e a proteção dos direitos fundamentais das mulheres. Somente com ações coordenadas, éticas e multidisciplinares será possível enfrentar os riscos associados aos *deepfakes* e construir um ambiente digital mais seguro, inclusivo e igualitário.

REFERÊNCIAS

¹ DEEP nudes: fotos e vídeos são manipulados por IA para produzir conteúdo erótico. **G1**, 06 de out. de 2024. Disponível em: <https://g1.globo.com/fantastico/noticia/2024/10/06/deep-nudes-fotos-e-videos-sao-manipulados-por-ia-para-produzir-conteudo-erotico.ghtml>. Acesso em: 30 de jun. de 2025.

² CHRIST, Giovana. IA aumenta a criação de deepfakes de pornografia com mulheres, diz estudo. **CNN Brasil**, 16 de jun. de 2025. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/ia-aumenta-a-criacao-de-deepfakes-de-pornografia-com-mulheres-diz-estudo/>. Acesso em: 01 de jul. de 2025.

Brasil. Guia Ilustrado Contra as Deepfakes. Supremo Tribunal Federal; Data Privacy Brasil. Brasília: STF, Coordenadoria de Combate à Desinformação, 2024.

ANTONIOSI, Isabela. Deepfake é crime? Entenda a nova Lei nº 15.123/25. **JusBrasil**, 01 de mai. de 2025. Disponível em: <https://www.jusbrasil.com.br/artigos/deepfake-e-crime-entenda-a-nova-lei-n-15123-25/3538560848>. Acesso em: 01 de jul. de 2025.

VIEIRA, Juliana Rust Batista Felício. Violência digital: Deepfakes o novo rosto da opressão contra mulheres. **Migalhas**, 21 de mai. de 2025. Disponível em: <https://www.migalhas.com.br/depeso/430699/violencia-digital-deepfakes-o-novo-rosto-da-opressao-contra-mulheres>. Acesso em: 01 de jul. de 2025.

ALBIANI, Christine et al. Como deepfakes se tornaram armas de violência de gênero e o que fazer a respeito. **JOTA**, 28 de jun. de 2025. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/como-deepfakes-se-tornaram-armas-de-violencia-de-genero-e-o-que-fazer-a-respeito>. Acesso em: 02 de jul. de 2025.

MARTINS, Giulia Nascimento. **A violência contra a mulher nas redes sociais no contexto da desinformação: uma perspectiva da Ciência da Informação**. 2025. 70 f. Dissertação (Mestrado em Ciência da Informação) – Universidade Estadual Paulista (Unesp), Faculdade de Filosofia e Ciências, Marília, 2025.

BARROSO, Luís Roberto; MELLO, Patrícia Perrone Campos. Inteligência artificial: promessas, riscos e regulação. Algo de novo debaixo do sol. **Revista Direito e Práxis**, Rio de Janeiro, v. 15, n. 4, 2024. Disponível em: <https://www.scielo.br/j/rdp/a/n89PjvWXTdthJKwb6TtYXy/>. Acesso em: 04 de jul. de 2025.