

## DEEPPAKES E DIREITO PENAL

Bianca Caroline Rocha

Estela Gemignani Soares Más

Kerolen Bianca de Freitas Perly Netto

Resumo: O presente trabalho se propõe a analisar o fenômeno das deepfakes sob a perspectiva de seus impactos sociais e de suas implicações jurídico-penais no ordenamento brasileiro. As deepfakes consistem em mídias digitais manipuladas por meio de técnicas de inteligência artificial capazes de alterar imagens, vídeos e áudios com alto grau de realismo. O avanço e a popularização dessas tecnologias, inicialmente restritas a profissionais da área audiovisual, ampliaram significativamente sua utilização por usuários comuns, possibilitando tanto aplicações legítimas quanto usos maliciosos. Nesse contexto, observa-se a crescente utilização das deepfakes para a disseminação de desinformação, fraudes, manipulação política e produção de conteúdos íntimos não consensuais, especialmente contra mulheres, o que resulta em graves violações a direitos da personalidade, como honra, imagem, privacidade e dignidade sexual. Propõe-se, assim, examinar como a produção e a circulação de conteúdos adulterados maliciosamente contribuem para a fragilização da confiança da sociedade nas instituições e para o aumento da vulnerabilidade dos indivíduos no ambiente digital. Dessa forma, busca-se discutir o modo como o direito penal brasileiro tem enfrentado a problemática, atualmente por meio da aplicação de tipos penais já existentes diante da inexistência de uma tipificação específica para a prática de deepfakes.

Palavras-chave: Deepfake, Tecnologia, Direito Penal, Direitos da Personalidade, Tutela Jurídica, Insuficiência Normativa.

Abstract: This paper aims to analyze the phenomenon of deepfakes from the perspective of their social impacts and their criminal-law implications within the Brazilian legal system. Deepfakes consist of digital media manipulated through artificial intelligence techniques capable of altering images, videos, and audio with a high level of realism. The advancement and popularization of these technologies, initially restricted to professionals in the audiovisual field, have significantly expanded their use among ordinary users, enabling both legitimate applications and malicious uses. In this context, there has been a growing use of deepfakes for the dissemination of disinformation, fraud, political manipulation, and the production of non-consensual intimate content, especially against women, resulting in serious violations of personality rights such as honor, image, privacy, and sexual dignity. Thus, this study proposes to examine how the malicious production and circulation of altered content contribute to weakening society's trust in institutions and increasing individuals'

vulnerability in the digital environment. Therefore, the paper seeks to discuss how Brazilian criminal law has been addressing this issue, currently through the application of existing criminal provisions, given the absence of a specific legal classification for the practice of deepfakes.

Keywords: Deepfake, Technology, Criminal Law, Personality Rights, Legal Protection, Normative Insufficiency.

## **Introdução**

O notório avanço tecnológico ocorrido nas últimas décadas tem promovido transformações profundas na estrutura social, especialmente, nos meios de comunicação e difusão de informações nos meios digitais. Diante do desenvolvimento exponencial das ferramentas de manipulação de conteúdos audiovisuais com elevado grau de realismo e a consolidação da inteligência artificial (IA), encontra sua origem o fenômeno das *deepfakes*, produções que consistem na utilização de algoritmos e de recursos altamente acurados para a síntese e alteração de imagens, áudios ou vídeos com o objetivo de simular características humanas e causar danos à indivíduos e à coletividade.

Sob esta ótica, o uso indiscriminado das *deepfakes* passou a representar um desafio concreto ao ordenamento jurídico brasileiro. A criação e disseminação de conteúdos falsos difamatórios ou sexualmente explícitos sem o consentimento das vítimas, por meio das *deepfakes*, tem se mostrado atentatória a direitos fundamentais como a dignidade da pessoa humana, a honra, a imagem e a privacidade. Não obstante, o amplo acesso à tais ferramentas e a dificuldade de rastreamento da autoria intensificam a possibilidade de impunidade e revelam a insuficiência das normas penais tradicionais diante da alta velocidade no desenvolvimento das tecnologias de *deepfakes*, as quais revelam novas maneiras da prática delitiva no mundo digital.

Por conseguinte, o presente estudo propõe-se a examinar o fenômeno das *deepfakes* sob a ótica do Direito Penal brasileiro, analisando suas origens, formas de utilização e repercussões sociais, bem como a adequação ou a insuficiência das legislações vigentes para a responsabilização de condutas lesivas. Pretende-se, ainda, realizar uma abordagem comparada, considerando experiências internacionais relevantes, a fim de identificar possíveis parâmetros normativos e preventivos aplicáveis ao contexto nacional. Busca-se, por fim, contribuir para o debate acadêmico e jurídico acerca da necessidade de atualização do sistema penal frente aos desafios éticos, sociais e legislativos impostos pelas tecnologias emergentes de manipulação digital.

## **I. Deepfakes**

### *1.1. Contextualização histórica*

A ampliação da tecnologia nos últimos anos não só possibilitou o acesso aos meios digitais como o facilitou de maneira rápida e intuitiva, de modo que, recursos antes utilizados somente por

profissionais das áreas cinematográfica e de fotografia, passaram a ser acessíveis a usuários comuns. Nesse sentido, houve a criação de softwares como Photoshop, que permitem a edição e alteração de imagens de forma altamente acurada.

Desse modo, a popularização da ferramenta possibilitou que aqueles recursos fossem utilizados por indivíduos não necessariamente profissionais e para as mais diversas finalidades. É nesse contexto que, no ano de 2018, rede social *Reddit*, um usuário com o nome *deepfake* começou a publicar vídeos não consensuais com conteúdo pornográfico adulterado inserindo o rosto de celebridades do gênero feminino em vídeos de conteúdo sexual, utilizando-se de um algoritmo de inteligência artificial. O caso foi descoberto pela repórter do site *Motherboard*, Samantha Cole, que se tornou um expoente na discussão sobre o tema.

Ainda em 2019, um ano após as primeiras utilizações das *deepfakes*, como consequência da intensa velocidade e fluidez com que as informações se propagam no mundo digital, a ferramenta utilizada pelo usuário da plataforma de streaming já estaria disponível em aplicativos de edição de fotos e vídeos, fato que marcou uma onda de divulgação de imagens adulteradas de mulheres despidas realizando atos de conteúdo sexual.

Indubitavelmente, desde então, as *deepfakes* vêm sendo utilizadas das mais diferentes formas, abrangendo, atualmente, não só conteúdos danosos, mas também humorísticos, de estudos e, inclusive conteúdos políticos, o que suscitou nos meios sociais e, notadamente, no meio jurídico, debates sobre os limites de seu uso e sua regulamentação, ou a falta dela, quando utilizada de modo a lesar bens jurídicos tutelados pelo ordenamento jurídico.

### *I.II. Definição e utilização*

As *deepfakes* são mídias digitais (vídeos, áudios, imagens) manipuladas por meio de técnicas avançadas de inteligência artificial, especialmente redes neurais profundas (*deep learning*), capazes de substituir rostos, vozes ou expressões com alto grau de realismo. O termo vem da junção de “*deep*” (profundo, em referência ao *deep learning*, alusivo à capacidade da máquina em executar funções mais complexas de processamento de dados e produção de áudio, vídeos e imagens) e “*fake*” (falso). Essa tecnologia baseia-se em algoritmos que aprendem padrões de comportamento facial e vocal para gerar conteúdos praticamente indistinguíveis da realidade.

O principal problema atrelado às *deepfakes* está na manipulação maliciosa de informações, especialmente em contextos políticos, podendo gerar conteúdos mentirosos extremamente convincentes que podem manipular a percepção das pessoas quanto determinadas pessoas e fatos, e impactar a confiança pública nas instituições, ocasionando raciocínio e conjecturas equivocadas que, em momentos específicos e estratégicos, podem interferir nos resultados de eleições. Por essa razão, o Tribunal Superior de Justiça publicou a Resolução nº 23.732/2024 que proíbe terminantemente o

uso de mídias e conteúdos falsos e manipulados (*deepfakes*) em campanhas eleitorais que, no caso de descumprimento, pode acarretar na cassação do registro ou do mandato do malfeitor.

Além disso, *deepfakes* podem ser empregadas na esfera comercial objetivando a venda e divulgação de produtos controversos, a partir da simulação de vozes ou imagens de famosos, autoridades e empresas, visando transparecer confiança e atestar a funcionalidade do produto e induzindo os consumidores a aderir determinadas mercadorias propagadas por meios de divulgação fraudulentos e irregulares. Nessa esfera, o juiz de direito da 35ª Vara Cível do Foro Central da Comarca de São Paulo (Capital) determinou, em sede de tutela antecipada de urgência, a remoção imediata das *deepfakes* produzidos pela empresa Brites Corporation Ltda para promover cursos e divulgar produtos, envolvendo o nome, imagem e voz do médico Drauzio Varella sem a sua devida concordância ou autorização.

Enfim, no âmbito do direito penal, que é a esfera chave deste artigo, ainda não existe uma tipificação específica e adequada que enfrente diretamente o cerne da questão das *deepfakes* e, principalmente, os bens jurídicos violados pela produção desenfreada de conteúdos sintéticos falsos. Contudo, tal fato não impede a aplicação da lei penal vigente de acordo com cada caso concreto, visto que, em casos em que esses conteúdos são utilizados para aplicar golpes e fraudes, tais condutas são abrangidas pelo crime de estelionato. Considerando aspectos de violência de gênero contra as mulheres, em 2025 o art. 147-B do Código Penal foi alterado, acrescido de um parágrafo único que prevê o aumento de pena caso o crime descrito no caput (causar dano emocional grave à mulher) seja cometido com auxílio de conteúdos produzidos por ferramentas de inteligência artificial.

## II. Impactos Sociais

A crescente nos casos de produção e proliferação de *deepfakes* e sua perpetuação como fenômeno no mundo digital nos últimos anos resultou em inúmeros impactos sociais que reverberam nas mais diversas ramificações da coletividade e, nesse sentido, gerou danos significativos à valores fundamentais outrora consagrados por aquela atrelado à uma quebra de confiança de forma generalizada, tanto nas instituições vigentes, quanto nas plataformas digitais e na própria sociedade como coletividade.

Nesse sentido, o início da onda de propagação de *deepfakes* no Brasil foi marcada pela vergonha e pelo medo, uma vez que as primeiras manipulações de fotos e vídeos foram realizadas em conteúdos de mulheres com alto índice de visibilidade em uma clara tentativa - e efetivação - de violação da intimidade. Não obstante, aquelas vítimas enfrentaram rigorosos desafios jurídicos, legislativos e diante das plataformas a fim de conseguir a interrupção da circulação do conteúdo adulterado e a responsabilização dos autores, fatores que, em muitos dos casos, não se concretizaram.

Ao longo do tempo e com o avanço da tecnologia utilizada nas *deepfakes*, o alvo passou a ser não somente os indivíduos com visibilidade, mas também o “cidadão comum”, de sorte que o medo de ter fotos e vídeos públicos ou pessoais adulterados maliciosamente, sem a possibilidade de remoção do conteúdo ou reparação do dano de forma ágil, passou a ser um temor comum.

Mariana de Siqueira e Ester Jerônimo de Andrade corroboram que:

A despeito de ser um problema recorrente na vida das personalidades públicas, sejam atrizes, cantoras, jornalistas ou até mesmo figuras políticas, com a popularização da pornografia de vingança, qualquer um com o mínimo de presença digital é uma potencial vítima.<sup>1</sup>

Esse momento de tensão culminou na gradual degradação das referências de valores morais essenciais para o funcionamento de uma comunidade. Valores humanos como o respeito, a honestidade, o senso de justiça, a ética, entre tantos outros, passaram a ser intensa e reiteradamente subjugados e violados, ocasionando a banalização desses valores e, por conseguinte, uma coletividade desorientada e desconectada de alguma referência moral.

Como bem pontuou Renato de Oliveira Pereira, refletindo as lições de Hannah Arendt:

“O problema com Eichmann era exatamente que muitos eram como ele, e muitos não eram nem pervertidos, nem sádicos, mas eram e ainda são terrível e assustadoramente normais. Do ponto de vista de nossas instituições e de nossos padrões morais de julgamento, essa normalidade era muito mais apavorante do que todas as atrocidades juntas” (ARENDR, 1999, p. 299), pois indicava o surgimento de um novo tipo de criminoso, incapaz de avaliar a desproporção entre o que aspiravam e a magnitude da devastação que ajudavam a promover para atingir seus objetivos.<sup>2</sup>

Nesse sentido, atualmente, o “espírito do tempo” passou a ser o sentimento de temor no que tange a normatização e a banalização de conteúdos manipulados. A utilização de imagens adulteradas passou a ter aplicação ampla e, praticamente, irrestrita, de modo que a foto pornográfica “vazada” de uma atriz mundialmente renomada é prontamente descredibilizada e reconhecida popularmente pelo jargão “é IA (Inteligência Artificial)”.

Dessa forma, aquela insegurança na certeza de proteção pelo Poder Estatal e a dúvida do que é conteúdo verdadeiro e do que é falso, despertou na população o sentimento de desconfiança nas instituições que outrora eram aparato de segurança e assistência a direitos fundamentais e a valores humanos. Aliados a isso, constata-se a morosidade do estado em solucionar esses conflitos, por meio de seus poderes, seja o Judiciário, o Executivo ou o Legislativo que são essenciais para a manutenção da vida social da coletividade.

---

<sup>1</sup> SIQUEIRA, Mariana de; ANDRADE, Ester Jerônimo de. **Deepfake e privacidade**: uma análise jurídica acerca da manipulação da imagem dos usuários. Revista Foco, 2024.

<sup>2</sup> PEREIRA, Renato de Oliveira. **Eichmann e a incapacidade de pensar**: alienação do mundo e do pensamento em Hannah Arendt. Marília: Cultura Acadêmica, 2021.

### III.1. Violação aos bens jurídicos tutelados

Os principais impactos sociais relacionados à produção, uso e compartilhamento ilimitado das *deepfakes* incidem diretamente sobre valores consagrados e bens jurídicos tutelados tanto pela legislação constitucional, quanto pelas normas infraconstitucionais. A luz do Código Civil de 2002, nos artigos 11 ao 21, encontra-se a previsão da proteção expressa dos direitos da personalidade, especificamente, a honra, a imagem, a integridade, a privacidade e o direito ao próprio corpo. Nesta seara, a violação concretiza-se desde o momento da manipulação não consentida da imagem, e encontra seu ápice no momento em que a pessoa natural, alvo do conteúdo fraudulento, encontra-se desprovida do controle sobre a produção e o alcance daquele tipo de mídia sintetizada a partir de fragmentos de sua existência física (imagem física, voz, trejeitos, etc.).

Considerando que o principal objetivo da produção de *deepfakes* envolve ocasionar o engano, falsificar, desacreditar e manipular a realidade, na esfera do direito penal, é cada vez mais comum o uso desse tipo de conteúdo da prática de crimes patrimoniais, contra a honra e contra a dignidade sexual. No caso do primeiro, as *deepfakes* são usadas para compartilhar conteúdos alarmantes que prejudicam a percepção da vítima, tornando-a vulnerável a atentados contra o seu patrimônio, por exemplo, por meio de fraudes e estelionatos. Na seara dos direitos contra a honra, as *deepfakes* visam constranger, incriminar e ridicularizar a vítima, seja atribuindo-lhe alguma conduta questionável ou ilícita, incluindo-a em situações vexatórias ou manipulando imagens ao acrescentar traços enfadonhos e caricatos. Essas e outras condutas são comumente enquadradas nos crimes de calúnia, difamação e injúria.

Na esfera dos crimes contra a dignidade sexual, a violação é mais complexa e severa, já que as *deepfakes* são utilizadas, principalmente, para a produção de conteúdo pornográfico sintético, sem o consentimento da vítima (a maioria é composta por mulheres) com o objetivo de violentar, constranger e ultrajar a sua intimidade e privacidade. Especificamente, nesse caso, a *deepfake* toma a forma de uma ferramenta de perpetuação de opressão e violência contra as mulheres, as quais se veem cada vez mais encurraladas e desprotegidas, já que, dado o fácil e livre acesso à essas ferramentas, podem a qualquer momento ter sua imagem e intimidade expostas e incluídas em conteúdos pornográficos sem qualquer forma de controle ou lastro.

Assim, a produção e uso indiscriminado de *deepfakes* representam um fenômeno perverso que coloca em xeque a tutela de direitos rigorosamente protegidos pelo ordenamento jurídico brasileiro. Nas mais diversas esferas, a ofensa aos bens jurídicos é cada vez mais qualificada e específica, e as consequências avassaladoras já que o controle e rastreamento desse tipo de conteúdo é quase impossível.

### III. Implicações Jurídicas Penais

#### III.1. Análise das legislações vigentes

Na esfera do direito penal, especificamente, a produção, uso e compartilhamento *deepfakes* não estão enquadrados em um tipo próprio, isto é, essas condutas não são censuradas pelo Código Penal de 1940. Ainda assim, tais condutas comumente são enquadradas em outros crimes, em que as *deepfakes* atuam como instrumento viabilizador da prática criminosa. Nos crimes contra a honra, artigos 138 a 140 do Código Penal, o conteúdo sintético figura apenas como uma das formas de praticar o crime, isto é, dos vários meios, em que o criminoso poderia utilizar para cometer o crime o uso de *deepfakes* é apenas mais um.

Na esfera dos crimes patrimoniais, especificamente no artigo 171 do Código Penal, o crime de estelionato, abrange uma gama de situações em que as *deepfakes* podem configurar de forma diferente e, de certa forma, mais direta ainda que implicitamente. No caput do referido artigo, a conduta é caracterizada pela obtenção de vantagem financeira indevida mediante erro de outrem, artifício, ardil ou qualquer meio fraudulento, o conteúdo sintético manipulado é facilmente enquadrado como apetrecho de induzimento ao erro e engano, e até mesmo, meio fraudulento já que, produção de imagens irreais e manipuladas configura a fraude.

Nos §§ 2º-A e B do artigo 171, existe a menção específica da fraude eletrônica, uma qualificadora do crime de estelionato, que prevê penas mais graves se o crime é cometido por meio de recursos eletrônicos, logo, as *deepfakes* são exatamente enquadradas nesse tipo de crime, caso sejam utilizadas para cometê-lo. Assim, ainda que de maneira implícita e esteja ausente a menção expressa e clara quanto ao conteúdo sintético, não restam dúvidas que esse tipo de conteúdo seja repudiado no diploma legal.

Na seara dos crimes contra a dignidade sexual, a Lei 13.718/2018 incluiu no Código Penal o artigo 218-C, que instituiu o crime de divulgação de cena de estupro, de sexo ou de pornografia, outro caso em que não existe a menção expressa das *deepfakes*, mas, a partir dos verbos que compõem o tipo, ainda assim é possível que o seu manejo e compartilhamento sejam enquadrados no artigo supracitado. É valoroso destacar que o cerne do crime é a ausência de consentimento da vítima especificamente quanto à divulgação do material íntimo, ainda que em determinados casos a produção e o registro sejam consentidos, a antijuridicidade versa sobre o compartilhamento e exploração econômica não consentidos pela vítima. Nesses casos, o maior desafio a ser enfrentado pelo Poder Judiciário é o rastreamento específico dos autores do crime, já que, por meio de uma interpretação literal do artigo, nota-se que um novo crime é cometido a cada vez que o material é compartilhado, além disso, é praticamente impossível a delimitação exata do conteúdo e, principalmente, a quantificação exata dos danos à imagem e dignidade da vítima.

Por fim, a Lei 15.123/2025 incluiu o parágrafo único no artigo 147-B do Código Penal, que agrava a penalidade do crime de violência psicológica contra a mulher, caso o delito seja cometido “mediante uso de inteligência artificial ou de qualquer outro recurso tecnológico que altere imagem ou som da vítima”. Diferentemente dos demais dispositivos supramencionados, este é o único que não depende de uma interpretação extensiva, encarando explicitamente o manejo de *deepfakes* como uma conduta reprovável e que deve ser enfrentada de forma ampla e rigorosa.

### III.II. Insuficiência normativa

A elaboração e a proliferação das *deepfakes* levantam questões sobre a necessidade de limitação da atuação e da autorregulação das plataformas digitais, uma vez que esta já não é mais eficiente, e a complexidade de se estabelecer limites normativos frente à uma tecnologia em constante transformação. É nesse contexto em que o encontro de um sistema jurídico deficitário combinado com um processo legislativo extremamente moroso e uma tecnologia fugaz dão origem a um vácuo normativo que carece, com urgência, de atenção.

As plataformas digitais são regidas por uma governança algorítmica extremamente eficiente e acurada que não só determina e individualiza a entrega de conteúdos, como também se beneficia de sua propagação ao oferecer ao usuário um aparato totalmente personalizado, constituindo, assim, um sistema que se retroalimenta e que favorece a reprodução de conteúdo e a descentralização de sua origem, de modo que a responsabilização de agentes que elaboram conteúdos de manipulação maliciosos, como as *deepfakes*, torna-se insatisfatória, quando não impossível.

Dessa forma, mostra-se evidente a necessidade de articulação de normas limitadoras que regulem o exercício desenfreado e inconsequente do uso de tecnologias de manipulação de imagem, o que tem se mostrado uma medida de alta complexidade. Não obstante, a aplicação extensiva da legislação penal já existente sem a previsão de um tipo penal específico dificulta a caracterização e a limitação do ilícito, não sendo possível combater as *deepfakes* com eficiência ou responsabilizar o agente com assertividade, uma vez que não existem critérios objetivos de responsabilização tanto das plataformas quanto dos usuários.

Nesse sentido, destaca Paulo Alexandre Rodrigues de Siqueira que:

Parte da doutrina, especialmente, os garantistas afirmam que tais inovações legislativas não poderiam ser aplicadas, eis que não há previsão expressa sobre o tipo penal ‘Deep Fake’, o que poderia causar analogia *in mala parte*, que é vedada pelo direito penal.<sup>3</sup>

Além disso, a insuficiência normativa dificulta a proteção do bem jurídico tutelado que está sendo ameaçado ou lesionado nos meios digitais, de modo que uma conduta lesiva permanece em uma “zona cinzenta”, na qual existe uma ofensa grave à honra, à imagem, à personalidade do

<sup>3</sup> SIQUEIRA, Paulo Alexandre Rodrigues de. **O “deep fake” e a legislação brasileira**: utilização de instrumentos legais para a proteção à imagem. Brasília-DF, 2021.

indivíduo causada por uma conduta específica, qual seja, a manipulação de sua imagem por meio das *deepfakes*, porém a conduta em si não é considerada pelo ordenamento jurídico vigente um ato ilícito, como elabora Diniz:

Esse vácuo contribui para a erosão da confiança no sistema de proteção jurídica, especialmente diante da complexidade probatória envolvida na demonstração da falsidade do conteúdo e na identificação dos responsáveis. Além disso, a inexistência de uma abordagem legislativa sistematizada impossibilita a construção de jurisprudência estável e coerente, aumentando a imprevisibilidade nas decisões judiciais e comprometendo a segurança jurídica dos indivíduos expostos.

A normatização insuficiente se revela também no campo da proteção coletiva, onde a ausência de regras claras enfraquece a atuação dos órgãos públicos frente à proliferação de conteúdos manipulados.<sup>4</sup>

Fato incontroverso é que o sistema penal brasileiro vem adotando medidas de prevenção e de tentativa de responsabilização pela criação e propagação das *deepfakes*, notadamente pela alteração do artigo 147-B, do Código Penal, dada pela Lei nº 15.123/25, que fixou como causa de aumento de pena pela metade, no crime de violência psicológica contra a mulher, a utilização da Inteligência Artificial ou outro recurso tecnológico que altere a imagem ou o som da vítima. A alteração no referido artigo demonstra uma clara atenção por parte do legislador no que tange à manipulação dos conteúdos digitais e à gravidade de sua utilização para fins que atinjam bens jurídicos tutelados pelo ordenamento jurídico. Entretanto, o dispositivo, ainda que compreenda a problemática, é mero instrumento simbólico diante da fragmentária normatização vigente, uma vez que regula uma pequena fração da responsabilização dos autores de *deepfake* e não contempla todos os espectros dos danos causados por eles.

Além disso, é possível observar um avanço do poder Legislativo frente ao tema abordado diante da criação de projetos de lei que visam tipificar o crime de adulteração maliciosa de vídeos ou áudios, como o Projeto de Lei nº 1272, de 2023, de autoria do Senador Jorge Kajuru (PSB/GO). O PL propõe alterar o Código Penal para a criação do artigo 308 - A, na medida em que visa a criminalização da produção das denominadas *deepfakes* e reconhece que a legislação já prevê a punição de crimes contra a honra cometidos com a utilização de conteúdos adulterados, porém carece de especificação. Atualmente, o projeto tramita no Senado Federal e foi recentemente encaminhado para análise nas devidas comissões.

Não obstante, apesar de trativas esporádicas sobre o tema, em uma tentativa de avanço gradual de regulamentação, o Poder Legislativo caminha vagarosamente na busca por uma solução fática e eficaz para o problema diante do ritmo frenético e desenfreado com que as informações circulam no

---

<sup>4</sup> DINIZ, Pedro. **Os desafios regulatórios e a necessidade de tutela jurídica frente à proliferação de deepfakes**. Revista Tópicos, v. 3, n. 22, 2025. ISSN:2965-6672.

mundo digital, sendo necessários diversos “remendos” a fim de reparar os danos causados pelas *deepfakes* por meio de precárias equiparações a outros tipos penais.

Dessa forma, na maioria dos casos, as vítimas das *deepfakes* arcam com as consequências dos danos causados desamparadas e com proteção deficitária do ordenamento que goza de competência e de jurisdição para tutelar seus direitos e punir efetivamente, com instrumentos preventivos e repressivos, condutas que firam tais direitos, visto que é direito exclusivo do Estado o *ius puniendi* (poder punitivo estatal).

Sob esse prisma, ainda, garante a Constituição Federal a dignidade da pessoa humana, sendo que, em seu artigo 5º, inciso X, dispõe que são invioláveis “a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.”, e nesse sentido deve zelar o Estado. Ainda, determina o texto constitucional o dever do Poder Judiciário de garantir a apreciação de lesão ou ameaça de lesão a direitos.

### *III.III. Experiência internacional*

#### *União Europeia*

Nos últimos anos, a União Europeia, em atenção ao rápido avanço das tecnologias de Inteligência Artificial (IA), elaborou frentes de estudo para a regulamentação e utilização da mais variada gama de IAs, com o objetivo claro de tornar o seu uso seguro e confiável. Nesse sentido, houve a criação do Gabinete da Comissão Europeia para IA na UE, um grupo de trabalho formado por deputados europeus para contribuir para o desenvolvimento do setor digital no Bloco.

Em junho de 2024, a União Europeia promulgou a Lei de Inteligência Artificial, denominada “AI Act”, que conta com prazos diferentes para que determinados trechos entrem em vigor, sendo que possui expectativa de aplicação completa no ano de 2026. O dispositivo legal conta com classificações das IAs com base no risco que apresentam, sujeitando-os a requisitos específicos de funcionamento baseado em sua categoria, disposições acerca da governança e fiscalização por autoridades nacionais competentes e de Conselhos de IA, de modo a garantir supervisão humana para sistemas de alto risco e condições de transparência e responsabilidade na utilização do algoritmo.

De forma geral, a Lei de IA da UE tem como finalidade essencial a regulação da utilização da IA com foco em suas nuances, de sorte que não visa coibir o manuseio das IAs, mas possibilitar o uso consciente e transparente para aplicação em variadas esferas da sociedade atrelada ao seu desenvolvimento pleno e adaptação do mundo digital às noções de ética e de coletividade de que o mundo Ocidental compartilha.

#### *China*

Em 2023, a Administração de Ciberespaço da China (CAC - departamento ligado ao governo chinês) implementou as “Disposições sobre a Administração de Síntese de Profundidade de Serviços de Informações Baseados na Internet”, uma série de dispositivos normativos que instituem deveres específicos e explícitos dos provedores de serviços de inteligência artificial, em especial as que realizam aprendizado profundo, processamento massivo de dados e produção de conteúdo sintético. O texto legal conta com a vedação total e expressa do uso desses mecanismos para atentar contra a imagem da nação chinesa, bem como da produção e compartilhamento de notícias falsas. Além disso, institui o dever de retratação e transparência das empresas provedoras, obrigando-as a esclarecer rumores e boatos causados por seus conteúdo gerados e compartilhados em suas plataformas, assim como elaborar espaços digitais públicos, seguros e intuitivos para os usuários opinarem e denunciarem, garantindo-lhes transparência e eficiência na resolução de problemas.

A principal disposição alusiva às *deepfakes* trata-se da obrigatoriedade imposta às empresas provedoras de incluir selos e avisos visíveis de que o conteúdo em questão é sintético e produzido por inteligência artificial, proibindo terminantemente qualquer instituição ou usuário de manipular, esconder ou retirar esses avisos. Ademais, o texto estende seus efeitos e disposições para as lojas de aplicativos digitais que devem notificar, verificar e, se for o caso, suspender a oferta e disponibilidade de produtos que violem os parâmetros estabelecidos em lei.

Estados Unidos

Os Estados Unidos também apresentam dedicação ao tema do enquadramento legal, principalmente na seara penal, das *deepfakes*. Em decorrência da descentralização da estrutura federativa do país, a adoção de legislação específica acontece de forma autônoma, de modo que cada estado lida com os efeitos dos danos dos conteúdos manipulados individualmente. Dessa forma, além das leis estaduais que tangenciam conteúdos adulterados, notadamente em relação a crimes sexuais, os congressistas norte-americanos recentemente incluíram em suas discussões propostas de alcance federal.

O projeto de lei de 2023, denominado “*Deepfakes Accountability Act*”, que tramita na casa do Congresso Americano, visa “proteger a segurança nacional contra as ameaças representadas pela tecnologia de *deepfake* e providenciar recurso legal de vítimas de *deepfakes* danosas”, enquanto o projeto “*Malicious Deep Fake Prohibition Act*” (2018), “estabelece um novo tipo penal relacionado à criação ou à distribuição de mídia eletrônica falsa que parece realista”. Esses projetos demonstram avanço sobre a regulamentação da problemática.

## Conclusão

A análise desenvolvida pelo presente artigo abordou o fenômeno das *deepfakes*, pontuando os desafios jurídicos e sociais. A produção sintética de mídias digitais (imagens, sons e vídeos),

propiciada por aplicativos de inteligência artificial, ultrapassa a seara tecnológica e atinge profundamente as estruturas fundamentais da convivência humana, incidindo diretamente sobre a coletividade, os valores consagrados e bens jurídicos definitivamente tutelados, por exemplificação, a honra, a imagem, a dignidade sexual, liberdade e a privacidade. Ao tornar praticamente indistinguível o real do artificial, as *deepfakes* são aparatos poderosos que propiciam desestabilização da confiança coletiva e corroem valores egrégios essenciais à vida em sociedade, demandando ao Direito a urgente tarefa de responder, atualizar e adaptar seus instrumentos de controle, de proteção e de tutela.

Quanto ao ordenamento jurídico brasileiro, existem dispositivos penais que permitem o enquadramento de determinadas condutas associadas ao mau uso de ferramentas de inteligência artificial, contudo, inexistente, até o presente momento, uma tipificação penal específica capaz de abranger com precisão e efetividade, as múltiplas consequências da não regulamentação dessa problemática. A recente alteração do artigo 147-B do Código Penal representa um avanço explícito, mas apenas simbólico e insuficiente diante da complexidade e da dimensão dos efeitos danosos produzidos por esse tipo de conteúdo.

A experiência internacional demonstra que a regulamentação das *deepfakes* demanda uma abordagem específica e integrada, que combine mecanismos repressivos contra práticas abusivas, a transparência algorítmica e responsabilização tanto de usuários quanto de plataformas. Modelos como o AI Act da União Europeia, as normas restritivas chinesas e as iniciativas legislativas norte-americanas revelam caminhos distintos, porém convergentes, no reconhecimento da necessidade de limitação e controle do uso dessas tecnologias.

Em suma, as *deepfakes* impõem ao Direito brasileiro contemporâneo o desafio de reafirmar seus fundamentos diante de uma realidade em contínua transformação. A defesa e proteção da integridade da verdade, da honra e da dignidade das pessoas não deve ser mantida refém de interpretações expansivas, de generalidades e de insuficiências legislativas. As crescentes evoluções tecnológicas exigem uma resposta regulamentadora rápida e eficiente do ordenamento jurídico, em que exista a reafirmação dos princípios constitucionais e do comprometimento do Poder Judiciário objetivando a tutela e eficácia dos direitos de seus jurisdicionados.

### Referências bibliográficas

CALIFORNIA. **Assembly Bill No. 602**: Civil Code – Deepfake Pornography. California State Legislature, Sacramento, 2019. Disponível em: [https://leginfo.ca.gov/faces/billNavClient.xhtml?bill\\_id=201920200AB602](https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB602). Acesso em: 30 out. 2025.

CALIFORNIA. **Assembly Bill No. 730**: Political Deepfakes. California State Legislature, Sacramento, 2019. Disponível em:

[https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill\\_id=201920200AB730q](https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB730q). Acesso em: 30 out. 2025.

DA. **Deepfakes**: O desafio jurídico da influência que persiste - Migalhas. Disponível em: <<https://www.migalhas.com.br/depeso/422806/deepfakes-o-desafio-juridico-da-influencia-que-persiste>>. Acesso em: 30 out. 2025.

DINIZ, Pedro. **Os desafios regulatórios e a necessidade de tutela jurídica frente à proliferação de deepfakes**. Revista Tópicos, v. 3, n. 22, 2025. ISSN:2965-6672.

**Disposições sobre a Administração de Serviços de Informação da Internet de Síntese Profunda**. Disponível em: <https://www.chinalawtranslate.com/en/deep-synthesis/#gsc.tab=0>. Acesso em: 5 nov. 2025.

European Commission. **European AI Office** | Shaping Europe's Digital Future. Digital-Strategy.ec.europa.eu, 8 Mar. 2024, [digital-strategy.ec.europa.eu/en/policies/ai-office](https://digital-strategy.ec.europa.eu/en/policies/ai-office).

FACILITA JURÍDICO. **Deepfake, IA e prática de crimes**: Entenda o Caso Drauzio Varella e Seus Impactos Jurídicos. Disponível em: <https://facilitajuridico.com.br/blog/deepfake-direito-imagem-caso-drauzio-varella-129>. Acesso em: 30 out. 2025.

**Lei Da UE Sobre IA**: Primeira Regulamentação de Inteligência Artificial. Temas | Parlamento Europeu, 12 June 2023, [www.europarl.europa.eu/topics/pt/article/20230601STO93804/lei-da-ue-sobre-ia-primeira-regulamentacao-de-inteligencia-artificial](https://www.europarl.europa.eu/topics/pt/article/20230601STO93804/lei-da-ue-sobre-ia-primeira-regulamentacao-de-inteligencia-artificial).

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.

MIÃO, A. **China torna obrigatória identificação de conteúdo gerado por IA**. Disponível em: <https://www.poder360.com.br/poder-china/china-torna-obrigatoria-identificacao-de-conteudo-gerado-por-ia>. Acesso em: 10 nov. 2025.

OLIVEIRA, G. A. G.; ÁVILA, G. N. **Deep fake, direitos da personalidade e o direito penal**: uma análise dos impactos tecnológicos na era digital. Revista Eletrônica do Curso de Direito da UFSM. Santa Maria, v. 19, e85239, p. 1-19, 2024. Disponível em: <https://doi.org/10.5902/1981369485239>. Acesso em: 8 out. 2025.

PEREIRA, Renato de Oliveira. **Eichmann e a incapacidade de pensar: alienação do mundo e do pensamento em Hannah Arendt**. Marília: Cultura Acadêmica, 2021.

REINA, E. Consultor Jurídico. Disponível em: <https://www.conjur.com.br/2023-abr-08/china-cria-lei-informacoes-falsas-meio-deepfakes>. Acesso em: 31 out. 2024.

REUTERS. **UE Estabelece Diretrizes Sobre Uso Indevido de IA**. CNN Brasil, 4 Feb. 2025, [www.cnnbrasil.com.br/economia/macroeconomia/ue-estabelece-diretrizes-sobre-uso-indevido-de-ia/](https://www.cnnbrasil.com.br/economia/macroeconomia/ue-estabelece-diretrizes-sobre-uso-indevido-de-ia/).

SIQUEIRA, M. de, & Andrade, E. J. de. (2024). **Deepfake e privacidade**: uma análise jurídica acerca da manipulação da imagem dos usuários. Revista Foco, 17(8), e5679. <https://doi.org/10.54751/revistafoco.v17n8-014>.

SIQUEIRA, Paulo Alexandre Rodrigues de. **O “deep fake” e a legislação brasileira**: utilização de instrumentos legais para a proteção à imagem. Brasília-DF, 2021.

THE ECONOMIST. **What is a deepfake?** The Economist Explains, 07 ago. 2019. Disponível em: [https://www.economist.com/the-economist-explains/2019/08/07/what-is-a-deepfake?utm\\_medium=cpc.adword.pd&utm\\_source=google&ppccampaignID=19495686130&ppcadID=&utm\\_campaign=a.22brand\\_pmax&utm\\_content=conversion.direct-response.anonymous&gclid=aw.ds&gad\\_source=1&gad\\_campaignid=19495464887&gbraid=0AA AADBbuq3IFZXF3-PGXm8EBfp0KZARuJ&gclid=Cj0KCCQjw15jHBhDHARIsAB0YqjwmHOZ-6ygNCvDU57tm2eLun-Oz1heCpG7Lu98\\_JUtY-sDcF3JY0z8aAsylEALw\\_wcB](https://www.economist.com/the-economist-explains/2019/08/07/what-is-a-deepfake?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=19495686130&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gclid=aw.ds&gad_source=1&gad_campaignid=19495464887&gbraid=0AA AADBbuq3IFZXF3-PGXm8EBfp0KZARuJ&gclid=Cj0KCCQjw15jHBhDHARIsAB0YqjwmHOZ-6ygNCvDU57tm2eLun-Oz1heCpG7Lu98_JUtY-sDcF3JY0z8aAsylEALw_wcB). Acesso em: 8 out. 2025.

UNITED STATES. **DEEPPAKES Accountability Act. 116th Congress**, Washington D.C., 2019. Disponível em: <https://www.congress.gov/bill/116th-congress/house-bill/3230>. Acesso em: 30 out. 2025.

UNITED STATES. **Malicious Deep Fake Prohibition Act of 2018 (S.3805)**. 115th Congress, Washington D.C., 2018. Disponível em: <https://www.congress.gov/bill/115th-congress/senate-bill/3805>. Acesso em: 30 out. 2025.