FACULDADE SANTA LUZIA - FSL
CURSO DE BACHARELADO EM
DIREITO

# DEEPFAKES E O DIREITO À IMAGEM: O ORDENAMENTO JURÍDICO ESTÁ PREPARADO?

ORIENTANDA: MYRIAH RENATA DE JESUS TRINDADE FURTADO
PROFESSORA ESP.: MARIANA AZERÊDO RODRIGUES DE ALMEIDA

SANTA INÊS – MA
2025

MYRIAH RENATA DE JESUS TRINDADE FURTADO

# DEEPFAKES E O DIREITO À IMAGEM: O ORDENAMENTO JURÍDICO ESTÁ PREPARADO?

Trabalho apresentado à Faculdade Santa Luzia como requisito parcial para a obtenção do grau de Bacharel em Direito.

Orientadora Especalista: Prof.ª Mariana Azerêdo Rodrigues de Almeida

SANTA INÊS -MA

2025

# (19374) FACULDADE SANTA LUZIA – FSL

**MYRIAH RENATA DE JESUS TRINDADE FURTADO**

**DEEPFAKES E O DIREITO À IMAGEM: o ordenamento jurídico está preparado?**

**Data da Defesa:** 03 **de** Dezembro **de** 2025

**BANCA EXAMINADORA**

Mariana Azerêdo Rodrigues de Almeida.
**Orientador**

Elisângela Macedo Valentim
**Examinador 1**

Filipe da Silva Coelho
**Examinador 2**

**Nota:** 10,0 (Dez)

**Resumo:**

Este artigo analisa a capacidade do ordenamento jurídico brasileiro de enfrentar os desafios trazidos pela tecnologia de deepfakes, uma ferramenta baseada em inteligência artificial capaz de produzir manipulações audiovisuais extremamente realistas. O avanço e a crescente popularização dessa tecnologia criaram riscos à privacidade, à honra, à segurança e, sobretudo, ao direito à imagem, exigindo atenção do Direito e do Estado. O trabalho busca compreender se a legislação atual é suficiente para responder de maneira eficaz a essas violações, considerando a velocidade com que os deepfakes se desenvolvem e se difundem. Para isso, a pesquisa adota uma metodologia qualitativa e exploratória, fundamentada em análise bibliográfica e documental, examinando doutrina, legislação, jurisprudência, relatórios técnicos e casos emblemáticos nacionais e internacionais. O estudo organiza-se em três partes: a primeira apresenta o funcionamento e os impactos sociais dos deepfakes; a segunda discute a proteção jurídica do direito à imagem no Brasil, com base na Constituição Federal, no Código Civil, no Marco Civil da Internet e na Lei Geral de Proteção de Dados; e a terceira aborda a relação direta entre deepfakes e violações à imagem, apontando lacunas legais, dificuldades probatórias e desafios regulatórios. Conclui-se que, apesar de possuir um arcabouço jurídico robusto, o Brasil ainda não está plenamente preparado para lidar com esse fenômeno, sendo necessárias atualizações legislativas, investimentos em tecnologia e políticas públicas integradas que fortaleçam a proteção dos direitos fundamentais na era da inteligência artificial.

**Palavras-Chave:** Deepfake; Direito à Imagem; Inteligência Artificial; Responsabilidade Civil.

**Abstract:**
This article analyzes the ability of the Brazilian legal system to address the challenges posed by deepfake technology, an artificial intelligence tool capable of producing extremely realistic audiovisual manipulations. The advancement and increasing accessibility of this technology have created new risks to privacy, honor, security, and, above all, the right to one's image, demanding attention from both the law and the State. The study seeks to determine whether the current legal framework is sufficient to effectively respond to these violations, considering the speed at which deepfakes evolve and spread. To achieve this, the research adopts a qualitative and exploratory methodology, based on bibliographic and documentary analysis, including doctrine, legislation, case law, technical reports, and emblematic national and international cases. The study is structured into three parts: the first presents the functioning and social impacts of deepfakes; the second discusses the legal protection of the right to image in Brazil, grounded in the Federal Constitution, the Civil Code, the Marco Civil da Internet, and the General Data Protection Law; and the third examines the relationship between deepfakes and image violations, identifying legal gaps, evidentiary challenges, and regulatory obstacles. The conclusion is that, although Brazil has a relatively robust legal framework, it is still not fully prepared to deal with this phenomenon, requiring legislative updates, technological investment, and integrated public policies that strengthen the protection of fundamental rights in the age of artificial intelligence.

**Keywords:** Deepfake; Right to Image; Artificial Intelligence; Civil Liability.

## INTRODUÇÃO

A sociedade contemporânea vivencia uma transformação digital acelerada, na qual a inteligência artificial (IA) emerge como uma força motriz de inovações e, simultaneamente, de complexos desafios sociais e jurídicos. Dentre as múltiplas aplicações da IA, a tecnologia conhecida como deepfake tem se destacado por sua capacidade de gerar conteúdo audiovisual sintético com um nível de realismo sem precedentes. Originado da fusão dos termos deep learning (aprendizado profundo) e fake (falso), o fenômeno consiste na criação de vídeos, imagens ou áudios manipulados que podem fazer uma pessoa parecer dizer ou fazer algo que, na realidade, nunca ocorreu. Essa capacidade de fabricar realidades alternativas de forma convincente e cada vez mais acessível lança uma sombra sobre a confiabilidade da informação e coloca em xeque direitos fundamentais consolidados, notadamente o direito à imagem.

O direito à imagem, consagrado como direito fundamental no artigo 5º, inciso X, da Constituição Federal de 1988, e detalhado no Código Civil, representa a prerrogativa de todo indivíduo de controlar o uso e a representação de sua própria aparência e identidade. Contudo, a proteção jurídica tradicional, concebida para uma era de mídias analógicas e manipulações digitais rudimentares, é agora confrontada por uma tecnologia que não apenas reproduz, mas sintetiza e recria a imagem humana, desafiando os próprios conceitos de autenticidade e prova.

Diante deste cenário, emerge o problema de pesquisa que norteia este trabalho: o ordenamento jurídico brasileiro está preparado para enfrentar os desafios impostos pelos deepfakes à proteção do direito à imagem? Esta questão desdobra-se em indagações sobre a suficiência das normas existentes, a eficácia dos mecanismos de tutela jurisdicional, a complexidade da responsabilização de criadores e plataformas, e a necessidade de novas abordagens regulatórias.

O objetivo geral deste trabalho é, portanto, consolidar uma análise abrangente sobre a intersecção entre a tecnologia de deepfakes e o direito à imagem, avaliando a adequação do arcabouço jurídico brasileiro para lidar com os conflitos emergentes. Para alcançar este fim, foram traçados os seguintes objetivos específicos: a) conceituar e detalhar a tecnologia de deepfakes, sua evolução histórica e seus impactos sociais; b) sistematizar o tratamento do direito à imagem no ordenamento jurídico brasileiro, explorando seus fundamentos constitucionais, legais e sua proteção na doutrina e jurisprudência; c) analisar criticamente as lacunas e inadequações da legislação vigente frente aos desafios específicos dos deepfakes.

O trabalho foi estruturado em três capítulos de desenvolvimento. O Capítulo 1 oferece uma imersão no universo dos deepfakes, explicando seu funcionamento técnico e impactos sociais. O Capítulo 2 dedica-se a uma análise dogmática do direito à imagem no Brasil. O Capítulo 3 realiza a síntese analítica, confrontando a tecnologia com o direito para identificar os desafios jurídicos e lacunas legislativas.

## METODOLOGIA

A presente pesquisa foi desenvolvida com o objetivo de analisar a capacidade de resposta do ordenamento jurídico brasileiro aos desafios impostos pela tecnologia de deepfakes no que tange à proteção do direito à imagem. Para alcançar tal propósito, adotou-se uma abordagem metodológica de natureza qualitativa, que se mostra mais adequada para a compreensão de fenômenos sociais complexos, como a intersecção entre tecnologia, direito e sociedade.

Quanto aos seus fins, o estudo classifica-se como uma pesquisa exploratória. O caráter relativamente recente e a rápida evolução do fenômeno dos deepfakes demandam uma investigação inicial que vise a familiarizar-se com o problema, esclarecer conceitos, identificar as principais variáveis e desenvolver uma compreensão mais precisa do tema.

No que concerne aos procedimentos técnicos, a pesquisa fundamenta-se em uma combinação de pesquisa bibliográfica e documental. A pesquisa bibliográfica consistiu no levantamento, seleção e análise de materiais já publicados sobre o tema, incluindo livros de doutrina jurídica, artigos científicos de periódicos especializados em direito e tecnologia, teses, dissertações e monografias.

A pesquisa documental, por sua vez, envolveu a análise de fontes primárias que não receberam tratamento analítico prévio ou que foram reexaminadas sob uma nova perspectiva. Este procedimento incluiu o estudo aprofundado da legislação pertinente, como a Constituição Federal de 1988, o Código Civil de 2002, o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

O procedimento de análise dos dados coletados seguiu uma abordagem crítico-analítica. As informações obtidas foram sistematicamente organizadas, comparadas e interpretadas à luz do problema de pesquisa. A análise buscou não apenas descrever o estado da arte da tecnologia e da legislação, mas também identificar tensões, lacunas, contradições e convergências.

## DESENVOLVIMENTO

### 1 DEEPFAKES: TECNOLOGIA, EVOLUÇÃO E IMPACTOS

A compreensão dos desafios jurídicos impostos pelos deepfakes exige, primeiramente, uma imersão em sua natureza tecnológica, sua trajetória histórica e suas profundas implicações sociais.

#### 1.1 Conceito, Definição e Tecnologia Subjacente

O termo 'deepfake' é um neologismo que amalgama as expressões 'deep learning' (aprendizado profundo) e 'fake' (falso), encapsulando a essência de sua origem e propósito. Tecnicamente, um deepfake é um conteúdo audiovisual (imagem, vídeo ou áudio) que foi alterado ou inteiramente gerado por algoritmos de IA para representar uma pessoa dizendo ou fazendo algo que nunca ocorreu na realidade, com um grau de realismo que pode torná-lo indistinguível do conteúdo autêntico para o olho humano.

A tecnologia central por trás da maioria dos deepfakes são as Redes Generativas Adversariais, ou Generative Adversarial Networks (GANs), uma arquitetura de aprendizado de máquina proposta pelo pesquisador Ian Goodfellow (em 2014). As GANs operam por meio de uma competição entre duas redes neurais: o Gerador e o Discriminador. O Gerador tem a tarefa de criar conteúdo falso, enquanto o Discriminador, treinado com um vasto conjunto de dados reais, atua como um crítico, tentando distinguir o conteúdo autêntico do conteúdo manipulado. Esse processo adversarial continua por milhares de iterações, até que o Gerador produza conteúdo tão realista que o Discriminador não consiga mais diferenciá-lo do real.

### 1.2 Tipos, Aplicações e Evolução Histórica

Diversas são as espécies de deepfakes, cada uma com suas particularidades e potenciais de uso. A categoria mais conhecida é a de deepfakes de vídeo, que inclui a substituição de rosto, onde o rosto de uma pessoa é sobreposto ao de outra, técnica notória pelo seu uso em pornografia não consensual; A reencenação facial, que transfere as expressões e movimentos labiais de uma pessoa para o rosto de outra, e a geração de rostos, que cria imagens de pessoas inteiramente fictícias. Os deepfakes de áudio, ou clonagem de voz, que permitem a síntese de falas com a voz de qualquer pessoa. Já os deepfakes de imagem estática permitem trocas de rosto e manipulação de atributos como idade e gênero.

A trajetória histórica dos deepfakes revela uma aceleração tecnológica exponencial. A manipulação de imagens é tão antiga quanto a própria fotografia, com exemplos notórios como as fotografias alteradas na era stalinista. No entanto, a era digital marcou um ponto de inflexão. Em 1997, o projeto acadêmico 'Video Rewrite' da Universidade de Stanford demonstrou a possibilidade de alterar digitalmente os movimentos labiais em um vídeo. O marco decisivo ocorreu em 2014, com a publicação do artigo científico de Ian Goodfellow sobre as GANs. Em 2017, o fenômeno explodiu na esfera pública com o surgimento do termo no Reddit.

O ano de 2018 foi crucial para a conscientização pública, com o lançamento do aplicativo FakeApp e a produção de um vídeo de alerta pela BuzzFeed mostrando um deepfake convincente do ex-presidente Barack Obama. Em 2022, durante a invasão da Ucrânia, um deepfake do presidente Zelensky demonstrou seu potencial como arma de guerra informacional. O caso da cantora Taylor Swift, em janeiro de 2024, gerou indignação global e impulsionou discussões legislativas.

### 1.3 Casos Emblemáticos e Impactos Sociais

A análise de casos concretos é fundamental para dimensionar o impacto real dos deepfakes. Internacionalmente, casos como os de Barack Obama, Volodymyr Zelensky e Taylor Swift demonstram o quão indistinguível da realidade a tecnologia pode se tornar. Estudos apontam que 96% dos deepfakes online são de natureza pornográfica e 99% destes vitimizam mulheres.

No Brasil, o fenômeno se manifesta com contornos próprios. Figuras públicas como o médico Drauzio Varella e o apresentador Marcos Mion tiveram suas imagens clonadas para promover produtos fraudulentos. No campo político, âncoras do Jornal Nacional foram alvo de um deepfake que invertia resultados de pesquisas eleitorais durante o período eleitoral de 2022.

Talvez a faceta mais sombria seja a infiltração no ambiente escolar. Um levantamento da SaferNet Brasil identificou múltiplos casos de deepfakes sexuais em escolas de pelo menos dez estados, envolvendo dezenas de vítimas, majoritariamente meninas adolescentes. Os impactos sociais são vastos. Na esfera individual, causam danos psicológicos, reputacionais e financeiros. Na esfera coletiva, os deepfakes corroem a confiança nas instituições e fomentam o dividendo do mentiroso: a capacidade de qualquer pessoa acusada com base em um vídeo autêntico alegar que se trata de um deepfake, minando a responsabilização.

## 2 O DIREITO À IMAGEM NO ORDENAMENTO JURÍDICO BRASILEIRO

Para avaliar a capacidade do sistema jurídico brasileiro de enfrentar os desafios impostos pelos deepfakes, é imprescindível primeiro compreender em profundidade o arcabouço normativo que protege o direito à imagem.

## 2.1 Fundamentos Constitucionais e Legais

A proteção ao direito à imagem no Brasil encontra seu alicerce mais sólido na Constituição Federal de 1988, que o elevou à categoria de direito fundamental. O dispositivo central é o artigo 5º, inciso X, que estabelece a inviolabilidade da 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. Complementarmente, o inciso V assegura o direito de resposta, e o inciso XXVIII, alínea 'a', garante a proteção à reprodução da imagem e voz humanas.

Essa proteção constitucional é densificada no Código Civil de 2002, que dedicou um capítulo aos Direitos da Personalidade (artigos 11 a 21). O art. 20 é a norma chave, estipulando que, salvo se autorizadas ou necessárias à administração da justiça, a divulgação de escritos, transmissão da palavra, ou publicação da imagem de uma pessoa poderão ser proibidas, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.

Com o advento da internet, o Marco Civil da Internet (Lei nº 12.965/2014) estabeleceu o regime de responsabilidade dos provedores. Seu artigo 21 prevê que, em casos de divulgação não autorizada de imagens de nudez ou atos sexuais, a remoção pode ser exigida por notificação extrajudicial. A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) classificou a imagem como dado pessoal, e quando processada para reconhecimento facial, pode ser dado pessoal sensível.

O uso de inteligência artificial (IA) para adulterar, criar ou manipular fotos, vídeos e áudios com a finalidade de constranger e prejudicar mulheres poderá ser tipificado como crime no Brasil, conforme o Projeto de Lei n.º 5.695/2023, em tramitação na Câmara dos Deputados. A proposta inclui essa conduta na Lei Maria da Penha e prevê pena de até quatro anos de reclusão para quem utilizar sistemas de IA com o objetivo de causar constrangimento, humilhação, assédio, ameaça ou qualquer outra forma de violência contra a mulher, no contexto doméstico ou familiar.

O texto original, de autoria do deputado federal Fred Linhares (Republicanos-DF), previa pena de um a dois anos de reclusão, além de multa. Contudo, o substitutivo apresentado pela relatora Dayany Bittencourt (União-CE) ampliou a punição, elevando a pena mínima para dois anos e dobrando o máximo inicialmente proposto. O projeto já foi aprovado na Comissão de Defesa dos Direitos da Mulher e ainda precisa ser analisado pela Comissão de Constituição e Justiça e de Cidadania para, então, ser submetido ao plenário da Câmara e, em caso de aprovação, ao Senado.

## 2.2 Proteção Jurídica: Natureza, Características e Tutela

O direito à imagem é classificado como um direito da personalidade, essencial à dignidade humana. Essa natureza lhe confere características especiais, definidas no artigo 11 do Código Civil: são direitos intransmissíveis e irrenunciáveis. A intransmissibilidade significa que o direito não pode ser alienado permanentemente; permite-se apenas a concessão de autorizações específicas e temporais. A

irrenunciabilidade impede que uma pessoa abdique de forma geral de seu direito à imagem.

A tutela ressarcitória visa reparar o dano, geralmente por indenização. A jurisprudência do STJ, na Súmula 403, estabeleceu que independe de prova do prejuízo a indenização pela publicação não autorizada de imagem com fins econômicos ou comerciais, configurando dano moral in re ipsa. A fixação do valor é feita pelo juiz com base em razoabilidade e proporcionalidade.

A tutela preventiva ou inibitória, fundamentada no artigo 497 do CPC, permite requerer ordem para impedir a prática ou continuação de ato ilícito. É concedida independentemente de culpa ou dano, bastando a ameaça de lesão. No contexto digital, obter medida liminar para remoção imediata é frequentemente o mecanismo mais eficaz.

### 2.3 Jurisprudência Relevante e Doutrina Brasileira

O Superior Tribunal de Justiça (STJ) tem desempenhado papel central na interpretação das normas. O tribunal tem refinado a aplicação do direito à imagem ponderando-o com a liberdade de imprensa, admitindo uso jornalístico em fatos de interesse público, mas condenando sensacionalismo e exposição vexatória.

O Supremo Tribunal Federal (STF), no julgamento da ADI 4815, declarou inconstitucional a exigência de autorização prévia para publicação de biografias, entendendo que configuraria censura prévia. A decisão estabeleceu que eventuais abusos devem ser reparados a posteriori, privilegiando a liberdade de expressão.

A doutrina brasileira forneceu bases teóricas. Carlos Alberto Bittar foi pioneiro na sistematização, defendendo a autonomia do direito à imagem. Roxana Borges aprofunda a disponibilidade relativa dos direitos da personalidade. Autores como Anderson Schreiber e Gustavo Tepedino trazem perspectiva civil-constitucional.

## 3 DEEPFAKES E DIREITO À IMAGEM: A INTERSECÇÃO E OS DESAFIOS

Após a exploração da tecnologia de deepfakes e do arcabouço de proteção ao direito à imagem no Brasil, este capítulo se aprofunda na intersecção crítica entre ambos.

### 3.1 A Intersecção e os Desafios Jurídicos Específicos

A colisão entre deepfakes e o direito à imagem gera desafios que transcendem as categorias tradicionais. O primeiro é o desafio probatório. O sistema de justiça depende da confiabilidade das provas, e mídias audiovisuais sempre foram consideradas evidências robustas. Os deepfakes corroem essa confiança, criando uma crise epistemológica. Como um juiz pode validar um vídeo quando a tecnologia permite a fabricação de qualquer cena? Isso gera o dividendo do mentiroso. A situação é agravada pela escassez de peritos forenses especializados no Brasil.

O segundo grande desafio é o da autoria e responsabilização. A criação e disseminação de um deepfake envolve múltiplos atores: o criador original, as plataformas digitais e os usuários que compartilham. Identificar o criador é uma tarefa hercúlea. A responsabilização das plataformas é limitada pelo art. 19 do Marco Civil, que as isenta de responsabilidade prévia à ordem judicial.

O terceiro desafio é jurisdicional. Deepfakes são um fenômeno globalizado: podem ser criados em um país, hospedados em servidores de outro e ter como vítima um cidadão de um terceiro. Essa dinâmica transnacional choca-se com o princípio da territorialidade. A ausência de adesão do Brasil à Convenção de Budapeste sobre o Crime Cibernético dificulta a obtenção de provas e a persecução de criminosos no exterior.

### 3.2 Lacunas Legislativas e a Inadequação do Ordenamento Atual

A análise crítica revela que, apesar de sua robustez teórica, o ordenamento possui lacunas significativas. O Código Civil, em seu artigo 20, pressupõe a existência de uma imagem real que é captada. A norma não foi projetada para lidar com imagens inteiramente sintéticas que nunca existiram. Além disso, a proteção é condicionada ao atingimento da honra ou fins comerciais, deixando zona cinzenta.

No âmbito penal, a ausência de tipo específico obriga aplicação analógica de crimes existentes como calúnia, difamação e estelionato. Essa abordagem é problemática sob a ótica da legalidade estrita.

### 3.3 Responsabilidade Civil

Do ponto de vista civil, a responsabilidade pode ser abordada tanto na modalidade subjetiva quanto objetiva. Na responsabilidade civil subjetiva, conforme o artigo 186 do Código Civil, aquele que violar direito e causar dano a outrem fica obrigado a repará-lo.

Por outro lado, a responsabilidade objetiva, prevista no § único, art. 927, Código Civil, dispensa a comprovação de culpa quando a atividade desenvolvida implicar risco.

A questão da prova no processo civil inverte a lógica tradicional: não se trata de provar que um fato ocorreu com base em um vídeo, mas sim de provar que um vídeo é falso ou autêntico. Isso demanda perícia técnica altamente especializada, envolvendo análise forense de metadados, detecção de artefatos de compressão e análise de movimentos oculares.

A complexidade representa um obstáculo significativo ao acesso à justiça. Do ponto de vista do Direito Penal, a tipificação dos deepfakes enfrenta o princípio da legalidade estrita, consagrado no art. 5º, inciso XXXIX, da Constituição Federal, e no artigo 1º do Código Penal: não há crime sem lei anterior que o defina.

Os crimes de calúnia (artº 138, Código Penal), difamação (artº 139, CP) e injúria (artº 140, CP) podem ser aplicáveis, contudo as penas previstas são brandas, variando de três meses a dois anos, não refletindo a gravidade dos deepfakes.

O Marco Civil da Internet e a LGPD também mostram limitações. O modelo de responsabilidade de plataformas é reativo e lento. A LGPD, focada no tratamento de dados pessoais, pode não abranger claramente a criação de conteúdo inteiramente sintético.

Do ponto de vista do Direito Administrativo, a Autoridade Nacional de Proteção de Dados (ANPD), criada pela LGPD, possui competências relevantes no combate aos deepfakes. A ANPD pode editar normas sobre proteção de dados pessoais e privacidade, fiscalizar o cumprimento da legislação e aplicar sanções.

Dado que a imagem é dado pessoal, e seu uso para criar deepfakes pode configurar tratamento ilícito, a ANPD poderia atuar de forma preventiva e repressiva. No entanto, a autoridade ainda está em estruturação. A questão da competência jurisdicional apresenta complexidades.

O artº 53 do CPC, estabelece que é competente o foro de domicílio do réu, mas em caso de dano, é competente o foro do lugar do ato. No contexto digital, onde o deepfake pode ser criado em uma localidade, hospedado em outra e ter vítima em uma terceira, com repercussões em todo território nacional, a determinação do foro competente é um desafio.

A jurisprudência tem admitido a competência do foro de domicílio da vítima. Do ponto de vista processual, o instituto da tutela de evidência, disciplinado no artº 311 do Código de Processo Civil, que permite a concessão de tutela provisória quando houver prova documental suficiente, enfrenta dificuldades. A própria natureza dos deepfakes cria dúvida sobre autenticidade, dificultando o enquadramento. A vítima precisa provar que o conteúdo é falso, o que exige perícia, criando paradoxo onde a proteção rápida depende de demonstração que não pode ser rápida.

A complexidade da perícia representa obstáculo significativo ao acesso à justiça. A maioria dos tribunais brasileiros não dispõe de peritos com formação específica em análise de deepfakes, e a contratação de expertise externa pode ser proibitivamente cara. A detecção de deepfakes é uma corrida armamentista constante entre criadores e detectores. Os métodos de detecção baseiam-se em inconsistências no piscar de olhos, artefatos de compressão, descontinuidades temporais, anomalias na sincronização labial e padrões de iluminação impossíveis. Ferramentas forenses utilizam análise de metadados, verificação de assinaturas digitais e comparação com bases de dados.

No entanto, à medida que os algoritmos evoluem, as técnicas de detecção precisam evoluir continuamente.

A proposta de criação de um Registro Nacional de Identificação de Conteúdo Sintético, análogo a sistemas de hash utilizados para combater a pornografia infantil, tem sido discutida. Esse sistema funcionaria mediante atribuição de identificadores únicos (hashes criptográficos) a conteúdos identificados como deepfakes maliciosos, permitindo que plataformas bloqueiem automaticamente tentativas de repostagem.

A implementação levanta questões sobre centralização de poder, riscos de censura e desafios técnicos de manter eficácia contra técnicas de evasão. O papel das plataformas de redes sociais na disseminação de deepfakes e sua responsabilização civil é tema de intenso debate.

O modelo de responsabilidade estabelecido pelo Marco Civil da Internet foi concebido em contexto tecnológico diferente. As plataformas argumentam que são meras intermediárias sem obrigação de monitorar proativamente o conteúdo postado por usuários.

Contudo, críticos apontam que essas empresas possuem recursos técnicos e financeiros para implementar sistemas de detecção de deepfakes, e que sua inação é motivada por interesses econômicos, já que conteúdo controverso gera engajamento e receitas publicitárias. A análise do direito comparado oferece lições valiosas.

A necessidade de atualização legislativa no Brasil é urgente. Propõe-se a criação de um tipo penal específico que criminalize a criação, alteração ou disseminação de deepfakes com finalidades ilícitas, abrangendo a pornografia de vingança sintética, a fraude, a difamação e a interferência em processos eleitorais.

A pena deve ser proporcional à gravidade do dano, com agravantes para casos envolvendo menores de idade. Paralelamente, faz-se necessária a reforma do Marco Civil da Internet para introduzir um regime diferenciado de responsabilidade para deepfakes.

Sugere-se a criação de um procedimento de notificação e remoção acelerado, no qual a vítima possa exigir remoção imediata pela plataforma. A educação digital emerge como componente essencial. A alfabetização midiática, que capacita cidadãos a reconhecer manipulações, questionar fontes e verificar autenticidade, deve ser integrada aos currículos escolares. Campanhas públicas de conscientização são fundamentais.

A cooperação internacional é absolutamente essencial. A adesão do Brasil à Convenção de Budapeste sobre o Crime Cibernético, ou a negociação de acordos bilaterais de cooperação com países-chave, é medida indispensável para superar o desafio jurisdicional. A vitimologia dos deepfakes revela padrões preocupantes de vulnerabilidade.

Mulheres, especialmente jovens, são desproporcionalmente vitimizadas por deepfakes pornográficos não consensuais, refletindo estruturas de violência de gênero. Figuras públicas, incluindo políticos, jornalistas e ativistas, são alvos frequentes de deepfakes difamatórios que visam minar sua credibilidade.

Minorias étnicas e religiosas também têm sido vitimizadas por deepfakes que disseminam estereótipos e incitam ódio. Essa distribuição desigual dos danos demanda que as políticas de enfrentamento incorporem uma perspectiva de justiça social, priorizando a proteção de grupos vulneráveis.

## CONSIDERAÇÕES FINAIS

Ao final desta jornada investigativa, é possível retornar à questão central: o ordenamento jurídico brasileiro está preparado para enfrentar os desafios impostos pelos deepfakes? A síntese dos achados aponta para uma resposta complexa: o PBrasil não está plenamente preparado, mas também não se encontra inteiramente desarmado. O diagnóstico revela um sistema com fundamentos sólidos, porém com ferramentas desatualizadas.

Os capítulos demonstraram que os deepfakes representam uma ameaça multifacetada. Não se trata apenas de nova violação do direito à imagem, mas de fenômeno que corrói a confiança na informação, potencializa a violência de gênero, viabiliza fraudes sofisticadas e ameaça a integridade democrática. A tecnologia impõe desafios probatórios, jurisdicionais e de responsabilização que a legislação atual não consegue endereçar satisfatoriamente.

A resposta é que o ordenamento jurídico brasileiro, em sua configuração atual, não está adequadamente preparado. As lacunas são evidentes: falta legislação específica que criminalize a criação e disseminação de deepfakes maliciosos; o

modelo de moderação de conteúdo depende excessivamente da intervenção judicial; e a infraestrutura técnica e humana do sistema de justiça é insuficiente para lidar com a complexidade do fenômeno.

Contudo, seria impreciso afirmar que o país está inerte. A Constituição Federal oferece base principiológica robusta que permite interpretações evolutivas. A jurisprudência já consolidou entendimentos valiosos. A existência da LGPD, do Marco Civil e de projetos de lei em tramitação demonstra consciência crescente do problema.

Diante do exposto, conclui-se com as seguintes recomendações: é urgente a aprovação de legislação específica; é necessária reforma do Marco Civil para criar mecanismo de remoção rápida; é fundamental investimento em capacitação de peritos forenses digitais; e a resposta deve incluir amplas campanhas de educação digital. Em última análise, a proteção do direito à imagem na era dos deepfakes é uma batalha pela preservação da dignidade, da verdade e da confiança. O ordenamento jurídico brasileiro possui os alicerces, mas precisa urgentemente construir as ferramentas adequadas. A tecnologia não irá esperar.

## REFERÊNCIAS

BITTAR, Carlos Alberto. **Os Direitos da Personalidade.** ed. São Paulo: Saraiva, 2015.

BORGES, Roxana Cardoso Brasileiro. **Direitos da personalidade e autonomia privada.** 2. ed. São Paulo: Saraiva, 2007.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 nov. 2025.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002. Código Civil.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 12 nov. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12 nov. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 nov. 2025.

BRASIL. **Lei nº 15.123, de 8 de abril de 2025**. Agrava penas para crimes contra mulheres com uso de IA. Disponível em: https://www.camara.leg.br/noticias/1040554. Acesso em: 12 nov. 2025.

BRASIL. S**uperior Tribunal de Justiça. Súmula 403.** Independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais. Brasília, DF: Superior Tribunal de Justiça, 2009.

BRASIL. **Supremo Tribunal Federal.** Ação Direta de Inconstitucionalidade 4.815. Relatora: Min. Cármen Lúcia. Julgamento em 10 jun. 2015.

CNN BRASIL. **Saiba o que é deepfake:** técnica de inteligência artificial que foi apropriada para produzir desinformação. 2024. Disponível em: https://www.cnnbrasil.com.br/noticias/. Acesso em: 12 nov. 2025.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro:** Teoria Geral do Direito Civil. São Paulo: Saraiva, 2023.

FORBES BRASIL. Deepfake: **Golpes e Desinformação** - Os efeitos colaterais dos vídeos de IA ultrarrealistas. 2025. Disponível em: https://forbes.com.br/. Acesso em: 12 nov. 2025.

G1. O que é deepfake e como ele é usado para distorcer realidade. 2024. Disponível em: https://g1.globo.com/tecnologia/. Acesso em: 12 nov. 2025.

KASPERSKY. Protect Yourself from Deep Fake. Resource Center. 2024. Disponível em: https://www.kaspersky.com.br/resource-center/. Acesso em: 12 nov. 2025.

MINISTÉRIO PÚBLICO FEDERAL. **Deepfake e Inteligência Artificial:** saiba o que pode e o que é proibido nas campanhas eleitorais. 2024. Disponível em: https://www.mpf.mp.br/. Acesso em: 12 nov. 2025.

LEMOS, Ronaldo. Direito, **Tecnologia e Cultura.** Rio de Janeiro: FGV Editora, 2020.

MULHOLLAND, Caitlin. **Dados Pessoais Sensíveis e Consentimento na Lei Geral de Proteção de Dados.** In: TEPEDINO, Gustavo et al. (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019.

RODOTÁ, Stefano. **A Vida na Sociedade da Vigilância: a privacidade hoje.** Rio de Janeiro: Renovar, 2008.

SCHREIBER, Anderson. **Direitos da Personalidade.** 3. ed. São Paulo: Atlas, 2014.

TEPEDINO, Gustavo. **A Tutela da Personalidade no Ordenamento Civil-Constitucional Brasileiro.** In: TEPEDINO, Gustavo. Temas de Direito Civil. 3. ed. Rio de Janeiro: Renovar, 2004.

UNIÃO EUROPEIA. **Regulamento (UE) 2024/1689** do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas em matéria de inteligência artificial. Jornal Oficial da União Europeia, 2024.