

CENTRO UNIVERSITÁRIO BRASILEIRO - UNIBRA
CURSO DE GRADUAÇÃO EM DIREITO

LUIZ FERNANDO AGUIAR DE AQUINO
PEDRO ALYSSON GOMES DA SILVA
WAGNER PEREIRA XAVIER

**O fenômeno do *Deepfake* e seus impactos no ordenamento jurídico
brasileiro**

RECIFE/2024

LUIZ FERNANDO AGUIAR DE AQUINO
PEDRO ALYSSON GOMES DA SILVA
WAGNER PEREIRA XAVIER

O fenômeno do *Deepfake* e seus impactos no ordenamento jurídico brasileiro

Trabalho de conclusão de curso apresentado à Disciplina TCC II do Curso de Bacharelado em Direito do Centro Universitário Brasileiro - UNIBRA, como parte dos requisitos para conclusão do curso

Orientador(a): Espec. Eriane Curado de Souza Falcão Gurgel

RECIFE/2024

Folha reservada para a Ficha Catalográfica

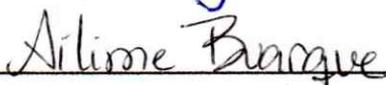
LUIZ FERNANDO AGUIAR DE AQUINO
PEDRO ALYSSON GOMES DA SILVA
WAGNER PEREIRA XAVIER

O FENÔMENO DO *DEEPPFAKE* E SEUS IMPACTOS NO ORDENAMENTO JURÍDICO BRASILEIRO

Artigo aprovado como requisito parcial para obtenção do título de Bacharelado em Direito, pelo Centro Universitário Brasileiro – UNIBRA, por uma comissão examinadora formada pelos seguintes professores:



Professor Orientador



Professor(a) Examinador(a)



Professor(a) Examinador(a)

Recife, 11 de DEZEMBRO de 2024.

NOTA: 9,5

RESUMO

Este artigo apresenta um estudo sobre a evolução dos crimes cibernéticos e o fenômeno das *deepfakes* no ordenamento jurídico brasileiro. Foi realizada revisão bibliográfica sobre o tema e análise da legislação vigente. Como objetivo geral, buscou-se analisar os impactos das *deepfakes* na sociedade e no direito, identificando lacunas na legislação perante esta ameaça emergente. Verificou-se que as *deepfakes*, embora ainda incipientes no Brasil, ganham notoriedade e disseminação por meio de aplicativos. Seu uso indevido pode gerar notícias falsas, ataques à honra e desinformação eleitoral. Contudo, a legislação brasileira carece de norma específica sobre o tema, dependendo apenas dos direitos da personalidade. Estudos de caso demonstram que tribunais pautam decisões pela analogia com casos semelhantes, todavia demarcam a necessidade de adaptação legal. Projetos de lei buscam regular fenômenos correlatos. Conclui-se que é imperiosa a promulgação de lei especial sobre *deepfakes*, definindo seus contornos, limites e sanções aplicáveis. Também se mostra imprescindível a conscientização social acerca da temática, diante do potencial impacto das *deepfakes* no ordenamento jurídico brasileiro.

Palavras Chave: Crimes cibernéticos; *Deepfakes*; Desinformação; Direitos da personalidade; Legislação Brasileira.

ABSTRACT

This article presents a study on the evolution of cybercrimes and the phenomenon of deepfakes in the Brazilian legal system. A bibliographic review was carried out on the topic and analysis of current legislation. As a general objective, we sought to analyze the impacts of deepfakes on society and law, identifying gaps in legislation in the face of this emerging threat. It was found that deepfakes, although still incipient in Brazil, are gaining notoriety and dissemination through applications. Its misuse can generate fake news, attacks on honor and electoral disinformation. However, Brazilian legislation lacks a specific rule on the subject, depending only on personality rights. Case studies demonstrate that courts base decisions on analogy with similar cases, however, they demonstrate the need for legal adaptation. Bills seek to regulate related phenomena. It is concluded that it is imperative to enact a special law on deepfakes, defining its contours, limits and applicable sanctions. Social awareness on the subject is also essential, given the potential impact of deepfakes on the Brazilian legal system.

Keywords: *Cybercrimes; Deepfakes; Disinformation; Personality rights; Brazilian legislation.*

SUMÁRIO

1. Introdução	6
2 Considerações iniciais sobre <i>deepfakes</i>	7
2.1 O que é <i>deepfakes</i>	8
2.2 Entendendo o conceito e aspecto técnicos	9
3 O <i>deepfakes</i> no brasil e o impacto na disseminação de informações falsas	10
3.1 Cenário panorâmico geral na legislação brasileira	11
3.2 Da honra no contexto das <i>deepfakes</i>	13
3.3 Da imagem no contexto das <i>deepfakes</i>	14
3.4 Projetos de lei e iniciativas regulatórias	14
3.5 Análise dos precedentes jurisprudenciais no contexto das <i>deepfakes</i>	15
4 Considerações finais	16
Referências	17

1. INTRODUÇÃO

A revolução tecnológica vivenciada nas últimas décadas trouxe consigo uma série de benefícios a sociedade, transformando profundamente a sociedade e moldando a forma como interagimos, comunicamos e conduzimos nossas atividades cotidianas. No entanto, essa era de avanços também desencadeou um aumento exponencial nos crimes cibernéticos, representando uma ameaça crescente à segurança e estabilidade do ciberespaço.

Este estudo visa analisar a Evolução dos Crimes Cibernéticos e os Desafios Enfrentados Pelo Ordenamento Jurídico Brasileiro, com um foco específico nos *deepfakes*, destacando sua importância como uma manifestação contemporânea dessa problemática. O ambiente virtual, marcado por sua natureza dinâmica e globalizada, impõe desafios singulares à aplicação da lei, demandando uma constante adaptação das estruturas jurídicas e políticas de segurança.

O objetivo central desta pesquisa é analisar a natureza desses delitos, desde suas origens até suas manifestações contemporâneas, contextualizando-os dentro do panorama jurídico nacional. Será empreendida uma análise criteriosa das lacunas existentes na legislação brasileira, compreendendo as dificuldades enfrentadas pelos órgãos responsáveis na persecução desses crimes, visando, assim, contribuir para o aprimoramento do arcabouço legal e das políticas públicas voltadas à prevenção e punição dos delitos cibernéticos.

A dinâmica e globalização do ambiente virtual apresentam desafios singulares à aplicação da lei, demandando uma adaptação constante das estruturas jurídicas e políticas de segurança. O cerne desta pesquisa é a análise da natureza dos crimes cibernéticos, desde suas origens até suas manifestações atuais, contextualizando-os no panorama jurídico brasileiro. A busca por uma compreensão aprofundada incluirá uma análise criteriosa das lacunas na legislação nacional, considerando as dificuldades enfrentadas pelos órgãos responsáveis no combate a esses crimes.

Ao longo do trabalho, serão abordadas a classificação e motivação por trás dos crimes cibernéticos, com especial atenção para a evolução dos *deepfakes* ao longo do tempo. Identificaremos as falhas na legislação vigente, propondo medidas concretas para seu aprimoramento. Além disso, examinaremos práticas de prevenção e combate, visando promover uma sociedade digital mais segura e resiliente diante das ameaças emergentes.

Este artigo não se limita a mapear e compreender crimes cibernéticos, mas também busca apresentar contribuições concretas para o fortalecimento do ordenamento jurídico brasileiro. Essas contribuições são essenciais para assegurar a integridade e a confiança no ambiente digital, fundamentais para o desenvolvimento sustentável de uma sociedade cada vez mais conectada.

A metodologia utilizada foi uma abordagem pesquisa exploratória descritiva, visando a compreensão sobre a evolução dos crimes cibernéticos, com destaque para o fenômeno do *deepfake* e os desafios enfrentados pelo ordenamento jurídico brasileiro. A escolha por uma abordagem descritiva

se justifica pela necessidade de mapear e compreender, de maneira abrangente, as nuances desse fenômeno complexo e em constante evolução.

Será realizada uma revisão bibliográfica abrangente sobre crimes cibernéticos, com foco primordial nos *deepfakes*. Essa revisão explorará a literatura acadêmica, revistas dos tribunais e documentos legislativos para estabelecer uma base teórica sólida que compreenda as diferentes facetas dos crimes cibernéticos e a evolução ao longo do tempo, priorizando a análise específica dos *deepfakes*.

Será analisadas decisões judiciais, desafios enfrentados pelos tribunais e a aplicação prática da legislação existente. Esses estudos de caso proporcionarão insights valiosos sobre as lacunas e desafios enfrentados no contexto jurídico.

Será realizada uma análise detalhada da legislação vigente no Brasil relacionada aos crimes cibernéticos, buscando identificar lacunas, em áreas que demandam aprimoramento. Documentos legais, como projetos de lei, serão examinados para compreender propostas de alterações e evolução normativa relacionadas aos *deepfakes*.

Dessa forma, com base nos resultados obtidos, a pesquisa apresentará propostas concretas para o aprimoramento da legislação e políticas públicas relacionadas aos crimes cibernéticos, destacando medidas específicas para lidar efetivamente com os desafios apresentados pelos *deepfakes* em constante evolução no contexto jurídico brasileiro.

2. CONSIDERAÇÕES INICIAIS SOBRE DEEPFAKES

O avanço tecnológico, inegavelmente, proporciona à sociedade oportunidades antes impensáveis, moldando a maneira como as pessoas se relacionam e interagem. No entanto, junto com essas possibilidades, surgem desafios jurídicos decorrentes de situações não contempladas pelo ordenamento vigente. Nesse contexto, destacam-se as *deepfakes*.

Assim como muitas inovações tecnológicas, as *deepfakes* podem ser utilizadas tanto de maneira bem-intencionada quanto mal-intencionada. Contudo, a disseminação generalizada de programas e aplicativos capazes de criar *deepfakes* levanta preocupações, pois alguns indivíduos podem explorar essa tecnologia para fins imorais, antiéticos ou até mesmo ilícitos. *Deepfakes* já foram usadas para dar veracidade a falsos sequestros, com a exigência de pagamento de resgates. Já foram utilizadas, da mesma forma, para confundir funcionários de empresas, fazendo-os executar ordens de pagamento inexistentes, gerando a perda de grandes quantidades de dinheiro¹.

Uma empresa multinacional perdeu US\$ 26 milhões (ou R\$ 129 milhões) nesta semana depois que golpistas enganaram seu funcionário em Hong Kong com uma chamada de vídeo em grupo falsa criada usando tecnologia deepfake, segundo o *South China Morning Post*. Os golpistas simularam uma videoconferência com a participação do diretor financeiro da empresa e de outros colaboradores. Só que ninguém na chamada de vídeo era real – exceto a vítima, um funcionário da empresa.

No fim das contas, o único participante de carne e osso que participava da reunião foi convencido a fazer um total de 15 transferências para cinco contas bancárias de Hong Kong.²

Ainda não é possível afirmar com certeza se os benefícios decorrentes da disseminação dessa inovação serão suficientes para compensar os prejuízos que sua popularização pode acarretar no futuro. No entanto, já se observa que as *deepfakes* podem se tornar uma preocupação significativa para a sociedade. Quando utilizadas de maneira inadequada, essas tecnologias têm o potencial de imputar comportamentos reprováveis a indivíduos, facilitar a prática de fraudes e até influenciar resultados eleitorais ¹.

As *deepfakes* representam um desafio para a imprensa que precisa sempre buscar a verdade sobre os fatos que noticia, para a persecução penal que pode estar diante de crimes praticados pelas pessoas que aparecem nos vídeos ou por aqueles que manipularam de forma criminosa os vídeos e também para cidadãos comuns que precisam de meios para discernir o que é real e o que é fictício no ambiente tecnológico, principalmente se o vídeo envolve pessoas públicas, políticos ou celebridades ³.

A existência desse potencial de danos evidencia a necessidade de uma análise aprofundada dos impactos sociais e jurídicos das *deepfakes*. Neste estudo específico, o foco recai sobre o conflito entre a legislação brasileira aplicáveis as *deepfakes* e as proteções legais da honra e imagem das pessoas retratadas através dessa forma de mídia.

Dado o caráter relativamente recente dessa tecnologia, é prudente iniciar esta monografia contextualizando o que são *deepfakes*, destacando suas diferenças em relação a outros vídeos falsos e apresentando a situação atual dessa inovação no Brasil. Esse estudo também abordará as diversas finalidades para as quais as *deepfakes* vêm sendo empregadas, incluindo casos emblemáticos de compartilhamento desse tipo de mídia. Por fim, serão exploradas as perspectivas futuras de uso das *deepfakes*, visando demonstrar seu potencial impacto ao ordenamento jurídico brasileiro.

2.1 O QUE É DEEPFAKES

Definir o termo *deepfake* é uma tarefa complexa, tendo em vista sua evolução ao longo do tempo. A evolução da tecnologia, em especial das inteligências artificiais, culminou na criação de *deepfakes* os quais consistem na distorção de vídeos e imagens de modo a mascarar a verdade e a simular acontecimentos nunca ocorridos, o que por muitas vezes acaba por violar a honra e a imagem dos indivíduos que tem sua imagem utilizada sem consentimento ⁴.

O TSE ⁵, ‘complementa definindo *deepfake* como um “conteúdo sintético em formato de áudio, vídeo ou combinação de ambos, que tenha sido gerado ou manipulado digitalmente, ainda que mediante autorização, para criar, substituir ou alterar imagem ou voz de pessoa viva, falecida ou fictícia’.

O aperfeiçoamento das ferramentas de inteligência artificial levou ao surgimento do fenômeno dos *deepfakes*, quando a imagem e a voz de uma pessoa são manipuladas para a produção de informações falsas, tornando praticamente impossível distinguir entre uma mensagem manipulada digitalmente de uma mensagem gravada na realidade. Enquanto na seara política, as preocupações estão relacionadas à manipulação de mensagens com intuito de alterar o resultado das eleições, colocando em risco a lisura do processo eleitoral, na seara do direito

privado crescem as denúncias de personalidades que têm seu nome, voz e imagem vinculados a produtos e serviços, muitos dos quais de qualidade e segurança duvidosas. Normalmente os infratores recorrem à manipulação da imagem e voz de pessoas conhecidas do público: médicos, jornalistas, esportistas, atores e atrizes. Geralmente usam figuras respeitadas em seu campo de atuação e o objetivo daqueles que, de má-fé, fazem uso desses artifícios, é aproveitar-se da reputação ou do carisma da pessoa para comercializar um produto ou serviço⁶.

O termo *deepfake* resulta da combinação das palavras “*deep*” – referente à tecnologia *deep learning*, ou aprendizado profundo – e “*fake*”, que significa “falso” em inglês. Embora não haja uma palavra equivalente em português, o conceito pode ser traduzido livremente como “falsidade profunda”, referindo-se a conteúdos falsos criados com elevado grau de sofisticação.

Assim, englobando essas definições, *deepfakes* podem ser entendidos como conteúdos audiovisuais (imagens ou áudios) manipulados digitalmente mediante inteligência artificial de maneira extremamente realista, capazes de representar pessoas em situações inexistentes da realidade¹⁻⁶.

2.2 ENTENDENDO O CONCEITO E ASPECTOS TÉCNICOS

No final de 2017, um usuário da plataforma virtual *Reddit* introduziu a expressão *deepfake* ao divulgar vídeos pornográficos forjados, criados por meio de inteligência artificial com base em algoritmos de troca de faces. O termo *deepfake* sugere, em tradução livre, uma “falsificação profunda”, representando vídeos digitalmente manipulados de forma extremamente realista, nos quais pessoas são retratadas falando palavras que nunca proferiram e realizando ações que nunca executaram.

O termo *deepfake* apareceu em dezembro de 2017, quando um usuário do *Reddit* com esse nome começou a postar vídeos de sexo falsos com famosas. Com softwares de *deep learning*, ele aplicava os rostos que queria a clipes já existentes. Os casos mais populares foram os das atrizes Gal Gadot e Emma Watson. A expressão *deepfake* logo passou a ser usada para indicar uma variedade de vídeos editados com machine learning e outras capacidades da IA⁶.

“A tecnologia inovadora por trás dos *deepfakes* permite “costurar” uma cópia do rosto de uma pessoa em um vídeo original, substituindo o rosto original pelo desejado”⁷. Essa técnica cria a ilusão de que a pessoa está presente no vídeo. ‘É relevante notar que, embora a definição inicial seja esclarecedora sobre a ideia central das *deepfakes*, ela carece de detalhamento sobre os aspectos técnicos fundamentais para diferenciar essa forma de manipulação digital de outros vídeos falsos’⁷.

Ao utilizar algoritmos de *machine learning* para inserir rostos e vozes em gravações de vídeo e áudios reais, tecnologias de *deepfakes* possibilitam a criação de personificações extremamente realistas, cujo resultado final é uma mídia dotada de tamanha verossimilhança que se torna impossível distinguir o que é real daquilo que foi digitalmente produzido. Colocando em termos mais simples, uma *deepfake* é um tipo de “mídia sintética”, o que significa dizer que se trata de uma mídia – incluindo-se imagens, áudio e vídeo – que é ou manipulada ou inteiramente gerada por uma inteligência artificial⁸.

As *deepfakes*, além de serem comumente associadas à manipulação de imagens, podem igualmente ser utilizadas para a falsificação de áudios.

as deepfakes mais sofisticadas são produzidas com o uso de redes generativas adversárias (também conhecida como GAN, (*GENERATIVE ADVERSARIAL NETWORKS*)). Em uma GAN, dois algoritmos competem entre si: o primeiro com a função de gerar conteúdos falsos indetectáveis, e o segundo com a função de descobrir e apontar falhas do primeiro. Dessa maneira, o primeiro algoritmo é constantemente aprimorado, conseguindo produzir resultado cada vez mais real ¹.

Diante do exposto, o termo "*deepfake*" pode ser definido como um vídeo ou áudio falsificado, notavelmente realista, manipulado digitalmente por meio de inteligência artificial para retratar pessoas em situações que não ocorreram. O uso de arquivos de imagem, vídeo ou áudio da pessoa retratada é inerente à criação de *deepfakes*, ressaltando o potencial de violação dos direitos à imagem e à honra do indivíduo retratado durante a elaboração, reprodução e compartilhamento desses conteúdos ^{6,7}.

3. O DEEPFAKES NO BRASIL E O IMPACTO NA DISSEMINAÇÃO DE INFORMAÇÕES FALSAS

No contexto brasileiro ⁴, “as *deepfakes* têm ganhado popularidade como meio de entretenimento e criação de sátiras humorísticas”. ‘Notavelmente, o jornalista Bruno Sartori se destaca ao compartilhar *deepfakes* de figuras políticas, utilizando essa tecnologia para criar paródias e vídeos satíricos. Ao contrário da propagação de desinformação, Sartori adota uma abordagem transparente, evidenciando a falsidade do conteúdo ⁹.

A manipulação da realidade audiovisual por meio de *deepfakes* representa um sério desafio à confiabilidade das informações, especialmente em contextos sensíveis como o político e o eleitoral.

Diante desse cenário, o Tribunal Superior Eleitoral (TSE) adotou medidas regulatórias visando proteger o processo democrático dessas ameaças digitais.

Por meio da Resolução 23.610/2019, e sua subsequente alteração pela Resolução 23732/2024, o TSE estabeleceu normas específicas para o uso de IA na criação e propagação de conteúdo durante as eleições.

Essas regulamentações buscam assegurar a integridade da propaganda eleitoral, limitando o uso de tecnologias que possam deturpar a informação entregue aos eleitores ⁹.

Em março de 2020, o aplicativo *Impressions App* revelou que os brasileiros constituíam a segunda maior nacionalidade na plataforma, representando 20% dos usuários. Entretanto, até o momento, carecemos de estudos conclusivos sobre o conteúdo das *deepfakes* compartilhadas no Brasil. Além das produções de Bruno Sartori, destaca-se o caso do vídeo vazado envolvendo o governador de São Paulo, João Dória, em 2018, onde supostamente estava participando de uma orgia, evidentemente violando a sua imagem e honra, gerando incertezas sobre a possibilidade de ter sido uma *deepfake* ¹⁰.

O episódio de João Dória ressalta a urgência de conscientização sobre as *deepfakes* e suas potenciais ramificações no Brasil. A capacidade de enganar as pessoas, aliada à forte polarização política, destaca o potencial danoso das *deepfakes*, contribuindo para a disseminação de informações falsas em um cenário já marcado por esse desafio.

Em setembro de 2020, o Tribunal Superior Eleitoral ¹¹ “divulgou em seu portal on-line um vídeo protagonizado pelo pesquisador e biólogo Átila Lamarino, explicando o conceito de *deepfakes* e associando-os diretamente às *fake News*.” Esse evento reflete uma crescente preocupação jurídica sobre o possível uso de *deepfakes* na produção de notícias falsas no Brasil.

Dessa forma, foi criado o "PL das *Fake News*", surge como uma resposta legislativa ao crescente problema da desinformação na internet no Brasil, propondo a criação da Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Este projeto visa regular as plataformas digitais com o objetivo de combater a disseminação de notícias falsas ¹².

O PL impõe às plataformas digitais a responsabilidade de adotar medidas contra a propagação de conteúdo falso, exigindo a identificação de contas automatizadas e maior transparência nas políticas de moderação de conteúdo ¹².

No âmbito jurídico brasileiro, embora não exista legislação específica sobre *deepfakes*, os indivíduos retratados são protegidos pelos direitos à imagem e à honra, conforme previsto na Constituição Federal, em seu art. 5º, inciso X, da Carta Magna Pátria¹³ e no artigo 20 do Código Civil/2002. No entanto, há uma colisão iminente entre essas tutelas e a liberdade de expressão dos disseminadores de *deepfakes*, demandando cuidado na tomada de decisões judiciais

A popularização das *deepfakes*, ainda em estágio inicial no Brasil, representa uma ameaça à sociedade devido ao seu potencial para condutas ilícitas contra a honra e imagem de indivíduos, além de agravar o problema das fake News no contexto eleitoral. No contexto brasileiro, esse fenômeno pode intensificar os desafios relacionados à disseminação de informações falsas, exigindo uma abordagem cautelosa por parte dos operadores do direito.

3.1 CENÁRIO PANORÂMICO GERAL NA LEGISLAÇÃO BRASILEIRA

A ascensão dos *Deepfakes* representa um marco significativo no campo das inovações tecnológicas, apresentando desafios únicos que ainda não foram abordados de forma específica pela legislação brasileira; No ordenamento jurídico brasileiro atual, não se encontram leis específicas que abordem a questão da legalidade na disseminação de *deepfakes* criminalizando, a análise da legalidade dessas ações deve considerar o contexto específico em que o compartilhamento ocorre, bem como a mensagem ou intenção por trás do ato em questão.

Apesar da lacuna normativa existente, os operadores do direito buscam criminalizar, de maneira indireta, através de outras legislações atualmente em vigor no ordenamento jurídico brasileiro.

Dentre essas legislações, algumas se destacam pela sua relevância e impacto, como a Convenção sobre crimes cibernéticos ¹⁴, “firmada em Budapeste em novembro de 2001, foi promulgado no Brasil pelo Decreto 11.491/2023”, é um tratado internacional que visa combater os crimes

cibernéticos, promovendo a colaboração entre diferentes países, ela serve como um referencial importante para a formulação de legislações nacionais e para o fortalecimento da cooperação internacional na luta contra a criminalidade digital ¹⁴.

Existe ainda a Lei Federal n.º 12.735 de 2012, conhecida como Lei Azeredo ¹⁵, que estabelece diretrizes fundamentais para a prevenção, investigação e repressão de delitos cibernéticos. O foco principal dessa lei é a segurança da informação, criando um ambiente mais seguro para os usuários da internet e desencorajando práticas ilícitas;

Por sua vez, a Lei Federal n.º 12.737 de 2012, chamada de Lei Carolina Dieckmann ¹⁶, criminaliza a invasão de dispositivos eletrônicos com o intuito de obter dados sem autorização. Ao tipificar esse tipo de crime, a legislação representou um avanço significativo na proteção contra abusos e invasões de privacidade no ambiente digital.

O Marco Civil da Internet, instituído pela Lei Federal n.º 12.965 de 2014, estabelece um conjunto de direitos e deveres que regem o uso da internet no Brasil. Essa norma enfatiza a proteção da privacidade dos usuários e a segurança dos dados pessoais, refletindo a necessidade de um equilíbrio entre a liberdade de expressão e a proteção da privacidade ¹⁷.

Além disso, a Lei Federal n.º 13.772 de 2018, introduz no Código Penal o artigo 216-B, a criminalização de atos de importunação sexual e a divulgação não autorizada de cenas de estupro. Essa legislação amplia a proteção à dignidade sexual, evidenciando a crescente preocupação com a segurança e o respeito aos direitos individuais ¹⁸.

Por fim, a Lei Federal n.º 13.709 de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD) ¹⁹, “é um dos pilares fundamentais na regulamentação do tratamento de dados pessoais no Brasil.” Esta lei estabelece direitos para os titulares e responsabilidades para os agentes que realizam o tratamento de dados. A LGPD foi parcialmente alterada pela Lei Federal n.º 13.853 de 2019 e é essencial para garantir a privacidade e a proteção dos dados dos cidadãos em um contexto digital cada vez mais complexo ¹⁹.

Diante do crescente fenômeno dos *Deepfakes*, essas legislações oferecem uma base inicial para a defesa dos direitos fundamentais relacionados à imagem e à privacidade, embora ainda haja um longo caminho a percorrer para uma regulamentação específica e eficaz.

Na ausência de uma legislação dedicada ao tema, os aspectos envolvidos no compartilhamento de tais conteúdos podem determinar se tal prática é legal ou não. Isso porque o compartilhamento pode, em certas circunstâncias, constituir uma violação dos direitos protegidos de uma pessoa, ou estar sob a proteção de direitos constitucionalmente garantidos, como o direito à honra e à imagem.

Apesar de existir a inclusão de imagens manipuladas ou conteúdos sintéticos no contexto da violação sexual (artigo 216-B, parágrafo único, Código Penal), a ausência de uma lei que trate das *deepfakes* em outras áreas específicas, deixando desprotegidos os sujeitos representados nessas produções, que são amparados pelos direitos à honra e à imagem, como estabelece a Constituição Federal no artigo 5º, inciso X, e o Código Civil de 2002, no artigo 20. Contudo, existe um conflito

evidente entre a proteção desses direitos e a liberdade de expressão daqueles que divulgam *deepfakes*, o que requer uma abordagem criteriosa nas decisões judiciais.

No que tange à legislação brasileira, não existe norma específica sobre as *deepfakes*. Fidelis²⁰ ressalta que, “todos esses dispositivos não abarcam todas as possibilidades de crimes que as *deepfakes* podem causar à toda sociedade, sendo necessário criar medidas que previnam, controlem, e combatam as consequências danosas que elas podem causar”

3.2 Da honra no contexto das *deepfakes*

A relevância do direito à honra no contexto do estudo advém da capacidade das *deepfakes* de comprometer a dignidade do indivíduo representado. Isso se manifesta especialmente em casos de *deepfakes* que geram notícias falsas com conteúdo difamatório ou vexatório, ou até mesmo em situações que expõem indevidamente a pessoa, servindo como instrumento para o *cyberbullying* ou para a divulgação de pornografia de vingança (*revenge porn*). Diante desse cenário se faz necessário uma análise desse direito jurídico e sua interação com o fenômeno das *deepfakes* no âmbito legal.

A Honra é um bem jurídico tutelado por diversos textos legais, a começar pela Declaração Universal dos Direitos Humanos, em seu artigo 12(ONU), passando pela Constituição Federal em seu artigo 5º, X e pelo Código Civil nos artigos 17 e 20, finalizando no Código Penal.

A tutela penal dos crimes contra a honra encontra previsão nos artigos 138, 139 e 140 do Código Penal, que tratam respectivamente de calúnia, difamação e injúria, com suas disposições gerais do artigo 141 ao 145²¹.

Antes de 2019, o artigo 141, inciso III do Código Penal, diz que se aumenta a pena em um terço se o crime for cometido na presença de várias pessoas, ou por meio que facilite a sua divulgação²¹.

Este inciso prevê, como majorante, uma situação de perigo e não de dano, que pode ser caracterizada de duas formas: na presença de várias pessoas ou por meio que facilite a divulgação da ofensa. Qualquer dessas formas possibilita a ocorrência de maior dano ao ofendido pela maior facilidade de divulgação da ofensa irrogada. Não é necessário que a ofensa seja divulgada, sendo suficiente que qualquer das formas empregadas seja idônea para divulgá-la, pois, como dissemos, estas configuram situação de perigo, e não de dano²².

Em 2019 foi instituído pela Lei 13.964/19²³, o parágrafo 2º, ‘que acrescentou, se o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, aplicando-se o triplo da pena, sendo este parágrafo vetado em 2021 pelo presidente Jair Messias Bolsonaro.’

De acordo com Alves⁴ “é possível a aplicação de lei penal ao crime praticado no âmbito da *deepfake*”:

Caso alguém edite um vídeo de modo a fazer parecer que determinada pessoa está praticando um crime, o editor do conteúdo terá praticado o crime de calúnia (art. 138, CP). Se, por outro lado, no vídeo falsificado, o indivíduo não estiver praticando um crime, mas estiver praticando um ato desabonador de sua conduta, será o criador do “deep fake” responsabilizado pelo crime

de difamação (art. 139, CP). Na hipótese de injuriar alguém através dessa tecnologia, terá praticado o crime de injúria (art. 140, CP) ⁴.

3.3 Da imagem no contexto das *deepfakes*

As primeiras indagações acerca do direito à imagem surgiram com a invenção da fotografia. Anteriormente a reprodução de imagens exigia a participação ativa da pessoa retratada, o que implicava um consentimento implícito. Inicialmente, as discussões se concentravam nas condições sob as quais as imagens poderiam ser capturadas, enfrentando limitações técnicas e materiais significativamente mais restritas do que as atuais ¹⁰.

Hoje, a preocupação se ampliou para abranger as vastas possibilidades de reprodução e distribuição de imagens pessoais e de terceiros. Este contexto é reflexo direto do progresso tecnológico, especialmente com a proliferação de smartphones capazes de registrar fotos e vídeos de alta qualidade e a cultura de compartilhamento massivo nas redes sociais ¹⁰.

A garantia do direito à imagem é um princípio fundamental estabelecido na Constituição Federal brasileira, no artigo 5º, inciso X. Esse dispositivo legal assegura a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas ¹³. Além disso, a Lei de Direitos Autorais, nº 9.610/98, também reforça a proteção legal das obras visuais, como fotografias e representações gráficas. “O direito de imagem é essencial para preservar a dignidade e a privacidade das pessoas, garantindo que elas tenham controle sobre o uso e divulgação de suas imagens ²⁴.”

Os dilemas modernos do direito à imagem se concentram, portanto, no potencial de exploração das imagens divulgadas online, em especial quando tal uso ocorre sem o consentimento do proprietário ou de maneira divergente ao propósito originalmente estabelecido pelo mesmo. Esse panorama cria um terreno fértil para a criação de *deepfakes* com objetivos diversos, afetando tanto figuras públicas quanto indivíduos privados.

3.4 PROJETOS DE LEI E INICIATIVAS REGULATÓRIAS

Diante dos desafios apresentados, diversos projetos de lei têm sido propostos visando a adaptação da legislação brasileira ao fenômeno das *deepfakes*.

O Projeto de Lei no 2.630 de 2020, conhecido como "PL das *Fake News*", “propõe a criação da Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet ¹²”.

Seus principais pontos originais são: dever das plataformas de vetar contas inautênticas; divulgação de relatórios trimestrais de transparência sobre moderação de conteúdos; criação do Conselho de Transparência e Responsabilidade na Internet; possibilidade de provedores criarem instituição de autorregulação, certificada pelo conselho; e multa de até 10% do faturamento do grupo econômico no Brasil em caso de descumprimento na lei ¹².

O Projeto de Lei nº 145 de 2024 ⁶, “objetiva estabelecer normas de proteção contra disseminação não autorizada de *deepfakes*”. O autor aponta que normalmente os infratores recorrem a manipulação de imagens de pessoas conhecidas do público.

Enquanto na seara política, as preocupações estão relacionadas à manipulação de mensagens com intuito de alterar o resultado das eleições, colocando em risco a lisura do processo eleitoral, na seara do direito privado crescem as denúncias de personalidades que têm seu nome, voz e imagem vinculados a produtos e serviços, muitos dos quais de qualidade e segurança duvidosas ⁶.

Existe o Projeto de Lei nº146/2024 ⁸, ‘que pretende alterar o Código Penal (Lei 2.648/1940)’ para prever causas de aumento de pena nos crimes contra a honra quando envolverem o uso de tecnologias de inteligência artificial para fazer alteração a imagem de pessoa ou som humano, podendo ter a pena quintuplicada’. “A medida visa qualificar esses delitos quando realizados por meio de manipulação digital profunda proporcionada pelas *deepfake* ⁸.”

Visando coibir o uso de *deepfakes* para desinformação eleitoral, o TSE editou a Resolução nº 23.610/2019 para regular a utilização de inteligência artificial na propaganda. Determinando:

proibição das *deepfakes*; obrigação de aviso sobre o uso de IA na propaganda eleitoral; restrição do emprego de robôs para intermediar contato com o eleitor (a campanha não pode simular diálogo com candidato ou qualquer outra pessoa); e responsabilização das *big techs* que não retirarem do ar, imediatamente, conteúdos com desinformação, discurso de ódio, ideologia nazista e fascista, além dos antidemocráticos, racistas e homofóbicos ¹¹.

Assim, apesar das iniciativas, permanece a necessidade de um marco legal que brinde proteção adequada às pessoas e promova o uso ético das *deepfakes*.

3.5 ANÁLISE DOS PRECEDENTES JURISPRUDENCIAIS NO CONTEXTO DAS DEEPFAKES

Na ausência de uma legislação específica sobre *deepfakes* no Brasil, os tribunais têm se baseado nos princípios constitucionais e na analogia com casos semelhantes para julgar questões envolvendo essa tecnologia. Alguns precedentes já estabelecidos podem nortear a atuação do Poder Judiciário e a edição de novas leis diante de demandas relativas a *deepfakes*.

No julgamento da AP 1021/DF do Supremo Tribunal Federal ²⁵, a ementa destaca a configuração do crime de difamação quando houve a publicação de um vídeo editado, atribuindo-lhe conteúdo racista inexistente na fala original. Nessa decisão, o tribunal rejeitou a preliminar de inépcia da queixa-crime e reconheceu a comprovação da materialidade e da autoria, além da presença do *animus diffamandi*.

Já no mandado de segurança julgado pelo Tribunal Regional Eleitoral de Minas Gerais (MSCiv 0600808-47.2024.6.13.0000), a corte considerou vedada a utilização de *deepfakes* em período pré-eleitoral, independentemente de o conteúdo ser claramente identificado como manipulado por inteligência artificial. Isso se deu em razão do potencial dessas práticas para desequilibrar o pleito ou comprometer a integridade do processo eleitoral, conforme as normas eleitorais vigentes, especialmente

a Resolução TSE nº 23.610/2019, com as modificações introduzidas pela Resolução nº 23.732/2024, dispondo sobre a propaganda eleitoral.

Adicionalmente em uma sentença proferida pela Vara Única da Comarca de Jardim de Piranhas/RN (0800988-84.2022.8.20.5142) ²⁷, o juízo condenou uma instituição financeira por falha na prestação de serviço ao permitir a contratação fraudulenta de empréstimo mediante o uso de *deepfake*. O tribunal entendeu que a mera coleta de biometria facial não é suficiente para comprovar a legitimidade da contratação, considerando os riscos inerentes a essa tecnologia ²⁷.

Esses precedentes demonstram que, diante da ausência de legislação específica, os tribunais têm buscado solucionar as questões envolvendo *deepfakes* por meio da aplicação analógica de dispositivos relacionados a crimes contra a honra e a regulamentação eleitoral. Essa abordagem, no entanto, denota a necessidade de uma adaptação legal mais adequada para lidar com os desafios trazidos por essa tecnologia.

4. CONSIDERAÇÕES FINAIS

O cenário atual demonstra que a disseminação das *deepfakes* vem assumindo uma importância crescente no ordenamento jurídico brasileiro. No entanto, essa tecnologia também coloca em evidência a urgência de revisões legislativas que garantam a proteção dos direitos individuais e a segurança do ambiente digital.

Como bem apontado no contexto desta pesquisa, o ordenamento jurídico brasileiro carece de uma normativa específica para lidar com as particularidades do fenômeno das *deepfakes*. Somente legislação genérica aplicável aos direitos da personalidade, sobretudo à imagem e à honra, tem servido como referência jurídica nesses casos.

Além disso, percebe-se que a disseminação de *deepfakes* no Brasil é incipiente, mas apresenta tendência de crescimento. Isso se manifesta pela maior adesão dos brasileiros a aplicativos de criação dessas mídias falsas, representando riscos futuros de uso deturpado para produção de notícias falsas ou ataques à honra.

Destaca-se, também, a preocupação do TSE em regular o emprego das *deepfakes* no contexto eleitoral, em virtude do elevado potencial de manipulação das eleições mediante a disseminação de informações falsas por esse mundo tecnológico digital. Entretanto, regulamentações pontuais como essa são insuficientes para coibir todo o leque de condutas ilícitas passíveis de serem cometidas.

O presente estudo evidenciou a crescente importância do fenômeno das *deepfakes* no ordenamento jurídico brasileiro, demonstrando a urgência de revisões legislativas para garantir a adequada proteção dos direitos individuais e segurança do ambiente digital.

O encaminhamento mais acertado para os problemas mapeados consiste na proposição de uma legislação específica, no âmbito penal sobre *deepfakes* no Brasil. Essa normativa deve contemplar definições claras sobre o termo, delimitar os casos em que sua manipulação é proibida e estabelecer

parâmetros para a responsabilização dos infratores, garantindo-se a indenização aos atingidos. Sendo imperativo que o ordenamento jurídico brasileiro acompanhe a evolução tecnológica, adaptando-se para oferecer respostas eficazes aos desafios impostos pelas deepfakes, garantido a proteção dos direitos fundamentais, salvaguardando a confiança da sociedade em um cenário de constante transformação.

Faz-se necessário um esforço conjunto entre o poder público, empresas de tecnologia e a sociedade para sensibilizar a população sobre a veracidade duvidosa dessas mídias manipuladas.

Espera-se que este estudo se torne referência relevante para futuros profissionais do Direito, fornecendo subsídios teóricos e práticos para lidar de maneira mais eficaz com as questões envolvendo as *deepfakes* e ao preencher lacunas de conhecimento este artigo busca contribuir para o fortalecimento do ordenamento jurídico brasileiro.

REFERÊNCIAS

1. Barroso LR, Fachin LE, Mendes GF, Rocha CL. Guia Ilustrado Contra as Deepfakes [Internet]. Data Privacy Brasil Research. 2024 [citado 09 de dezembro de 2024]. Disponível em: [https://portal.stf.jus.br/desinformacao/doc/Guia%20ilustrado%20Contra%20DeepFakes_ebook%20\(1\).pdf](https://portal.stf.jus.br/desinformacao/doc/Guia%20ilustrado%20Contra%20DeepFakes_ebook%20(1).pdf)
2. Giovanni B, Mato Grosso MP do E. Ministério Público do Estado de Mato Grosso. 2024 [citado 10 de dezembro de 2024]. ‘DEEPFAKE’: Golpistas usam Inteligência Artificial e criam reunião falsa com diretor financeiro de multinacional. Disponível em: <https://mpmt.mp.br/conteudo/1217/134964/deepfake-golpistas-usam-inteligencia-artificial-e-criam-reuniao-falsa-com-diretor-financeiro-de-multinacional-que-transfere-r-129-milhoes-a-criminosos>
3. Bezerra C da S, Agnoletto GC. Combate às Fake News. 1º ed. Vol. 1. São Paulo, SP: Editora Posteridade; 2020. 266 p.
4. Alves BM, Araújo AKV, Cavalcante JF, Galdino Júnior FE, Rodrigues LHL, Oliveira PHS de. Análise da responsabilização criminal dos criadores e propagadores de “deep fakes” no ordenamento jurídico brasileiro. Cad. Pedagógico [Internet]. 10º de junho de 2024 [citado 09 de dezembro de 2024];21(6):e4348. Disponível em: <https://ojs.studiespublicacoes.com.br/ojs/index.php/cadped/article/view/4348>
5. Brasil. Tribunal Superior Eleitoral [Internet]. [citado 10 de dezembro de 2024]. Tse Proíbe uso de inteligência artificial para criar e propagar conteúdos falsos nas eleições. Disponível em: <https://www.tse.jus.br/comunicacao/noticias/2024/Fevereiro/tse-proibe-uso-de-inteligencia-artificial-para-criar-e-propagar-conteudos-falsos-nas-eleicoes>.
6. Brasil. PL 145/2024 - Senado Federal [Internet]. 2024 [citado 10 de dezembro de 2024]. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/161946>
7. Oliveira SR de. Sorria, você está sendo filmado! 1º ed. Vol. 1. São Paulo, SP: Editora Revista dos Tribunais; 2021. Disponível em: <https://www.jusbrasil.com.br/doutrina/sorria-voce-esta-sendo-filmado-ed-2021/1233936808>. Acesso em: 17 out. 2024.
8. Brasil. PL 146/2024 - Senado Federal [Internet]. 2024 [citado 09 de dezembro de 2024]. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/161947>

9. Cyrineu, RT, Melón R. Consultor Jurídico. [citado 09 de dezembro de 2024]. IA e deep fakes nas eleições: desafio da tecnologia à integridade eleitoral (parte 1). Disponível em: <https://www.conjur.com.br/2024-abr-15/ia-e-deep-fakes-nas-eleicoes-desafio-da-tecnologia-a-integridade-eleitoral-parte-1/>
10. Medon FJA. O direito à imagem na era das deep fakes. RBDCivil [Internet]. 9º de abril de 2021;27(01):251. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/438>
11. Justiça Eleitoral [Internet]. [citado 09 de dezembro de 2024]. Nova campanha do TSE contra a desinformação vai ao ar a partir desta terça-feira (1º). Disponível em: <https://www.tse.jus.br/comunicacao/noticias/2020/Setembro/nova-campanha-do-tse-contra-a-desinformacao-vai-ao-ar-a-partir-desta-terca-feira-1o>
12. Brasil. PL 2630/2020 - Senado Federal [Internet]. 2020 [citado 09 de dezembro de 2024]. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/141944>
13. Brasil. Constituição da República Federativa do Brasil, Brasília: Senado Federal
14. Brasil. Decreto-lei nº 11.491 de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste [Internet]. Disponível em: <https://legislacao.presidencia.gov.br/atos/?tipo=DEC&numero=11491&ano=2023&ato=7a7kXWU10MZpWT0be>
15. Brasil. Lei Federal nº 12.735, de 30 de novembro de 2012. Para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares [Internet]. Brasília, DF: Presidência da República [citado 09 de dezembro de 2024]. Disponível em: <https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=12735&ano=2012&ato=0baoXUq1kM VpWT8d3>
16. Brasil. Lei Federal nº 12.737 de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos [Internet]. Brasília, DF: Presidência da República. Disponível em: <https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=12737&ano=2012&ato=7e2ETUq1kM VpWTb9b>
17. Brasil. Lei Federal nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil [internet]. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm.
18. Brasil. Lei nº 13.772 de 19 de dezembro de 2018. para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar e para criminalizar o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado. [Internet]. Brasília, DF: Presidência da República. Disponível em: <https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=13772&ano=2018&ato=6ecgXVE5UeZ pWT0f7>
19. Brasil. Lei Federal nº 13.709 de 14 de agosto de 2018. Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade [Internet]. Brasília, DF: Presidência da República. Disponível em: <https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=13709&ano=2018&ato=293QzZ61UeZ pWT79e>

20. Fidelis VC, Soares DV. Os desafios do ordenamento jurídico brasileiro frente às deepfakes. Revista Pensamento Jurídico [Internet]. 18 de setembro de 2023 [citado 09 de dezembro de 2024];17(1). Disponível em: <https://ojs.unialfa.com.br/index.php/pensamentojuridico/article/view/711>
21. Brasil. Decreto-lei no 2.848, de 7 de dezembro de 1940. Código Penal (1940) – Lex: coletânea de legislação: Edição Federal: [Internet]. [citado 09 de dezembro de 2024]. Disponível em: <https://www.lexml.gov.br/urn/urn:lex:br:federal:decreto.lei:1940-12-07;2848>
22. Bitencourt CR. Tratado de Direito Penal - volume 2 - parte especial - dos crimes contra a pessoa - 23 edição - 2023. 23º ed. São Paulo, SP: SaraivaJur; 2022. 720 p.
23. Brasil. Lei Federal nº 13.964 de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal [Internet]. [citado 09 de dezembro de 2024]. Disponível em: <https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=13964&ano=2019&ato=8cfATVE5keZpWT929>
24. Brasil. Lei nº 9.610 de 19 de fevereiro de 1998. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. [Internet]. [citado 09 de dezembro de 2024]. Disponível em: <https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=9610&ano=1998&ato=02dMTRE1EeNpWT89a>
25. BRASIL. STF. AP 1021, Brasília, DF: Superior Tribunal de Federal, 2020[Internet]. [citado 09 de dezembro de 2024]. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur434530/false>. Acesso em: 18 out. 2024.
26. Jusbrasil. Tribunal Regional Eleitoral de Minas Gerais. Mandado de Segurança Cível: msciv 0600808-47.2024.6.13.0000. [Internet]. [citado 09 de dezembro de 2024]. Belo Horizonte - Mg jurisprudência. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tre-mg/2534403173>
27. Jusbrasil. Tribunal Justiça Rio Grande do Norte. Procedimento Comum Cível 0800988-84.2022.8.20.5142. Vara Única da Comarca de Jardim de Piranhas tjrj. Jurisprudência [Internet]. [citado 09 de dezembro de 2024]. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-rrn/1757166566/inteiro-teor-1757166589>