Cognitio Juris
ISSN 2236-3009

A RESPONSABILIDADE CIVIL E PENAL PELO USO DE INTELIGÊNCIA ARTIFICIAL NA MANIPULAÇÃO DE IMAGENS COM FINS ILÍCITOS

CIVIL AND CRIMINAL LIABILITY FOR THE USE OF ARTIFICIAL INTELLIGENCE IN THE MANIPULATION OF IMAGES FOR ILLICIT PURPOSES

Artigo submetido em 01 de dezembro de 2025
Artigo aprovado em 02 de dezembro de 2025
Artigo publicado em 02 de dezembro de 2025

Cognitio Juris
Volume 15 – Número 58 – 2025
ISSN 2236-3009

.

Autor(es):
Lucas Lima Gomes[1]
Rosana Reis de Melo Silva[2]
Leda Mourão Domingos[3]

RESUMO: O avanço acelerado das tecnologias digitais, especialmente da inteligência artificial (IA) e das técnicas de manipulação de imagens como o *deepfake*, tem provocado profundas transformações sociais, ao mesmo tempo em que amplia as possibilidades de prática de ilícitos no ambiente virtual. O objetivo deste artigo é analisar a responsabilidade civil e penal decorrente do uso de IA na manipulação de imagens com fins ilícitos, destacando lacunas

normativas, desafios interpretativos e dificuldades na identificação de autores. A metodologia utilizada consistiu em pesquisa bibliográfica e documental, com enfoque na legislação brasileira, como o Código Civil, Código Penal, Marco Civil da Internet e Resoluções do Tribunal Superior Eleitoral. Os resultados apontam que, embora existam mecanismos normativos capazes de responsabilizar os agentes, ainda há fragilidades significativas na produção de provas, na tipificação penal específica e na capacidade investigativa das autoridades. A análise do caso envolvendo a deputada federal Tabata Amaral evidencia a gravidade dos danos causados por imagens manipuladas e a dificuldade de identificar e punir os responsáveis. Conclui-se que o ordenamento jurídico brasileiro possui instrumentos para enfrentar a questão, porém necessita de maior atualização normativa, aprimoramento técnico dos órgãos de investigação e políticas públicas voltadas à educação digital e à proteção da honra e imagem no meio virtual.

Palavras-chave: Inteligência Artificial; Manipulação de Imagens; Responsabilidade Civil; Responsabilidade Penal.

ABSTRACT: The rapid advancement of digital technologies, especially artificial intelligence (AI) and image manipulation techniques such as deepfake, has caused profound social changes, while expanding the possibilities for illegal activities in the virtual environment. The objective of this article is to analyze the civil and criminal liability arising from the use of AI in the manipulation of images for illegal purposes, highlighting regulatory gaps, interpretative challenges, and difficulties in identifying perpetrators. The methodology used consisted of bibliographic and documentary research, focusing on Brazilian legislation, such as the Civil

Code, Penal Code, Civil Rights Framework for the Internet, and Resolutions of the Superior Electoral Court. The results indicate that, although there are regulatory mechanisms capable of holding agents accountable, there are still significant weaknesses in the production of evidence, specific criminal classification, and the investigative capacity of the authorities. The analysis of the case involving federal deputy Tabata Amaral highlights the seriousness of

the damage caused by manipulated images and the difficulty of identifying and punishing those responsible. It can be concluded that the Brazilian legal system has the tools to address the issue, but it needs further regulatory updates, technical improvements in investigative bodies, and public policies focused on digital education and the protection of honor and image in the virtual environment.

Keywords: Artificial Intelligence; Image Manipulation; Civil Liability; Criminal Liability.

1 INTRODUÇÃO

O surgimento de novas tecnologias é constante, abrangendo desde soluções para facilitar tarefas cotidianas até ferramentas voltadas ao entretenimento e lazer, à medida que essas tecnologias se popularizam e se integram ao cotidiano das pessoas, também surgem novos tipos de delitos, especialmente no meio digital. Um exemplo marcante são os crimes chamado “deepfake” (termo em inglês que significa “falsificação profunda” refere-se a conteúdo audiovisual manipulado por inteligência artificial para simular o rosto, a voz ou o corpo de uma pessoa real, criando uma aparência altamente convincente, mas falsa), em que criminosos manipulam ou criam imagens, para colocar vítimas em situações falsas, atingindo diretamente sua imagem, honra e dignidade.

Em abril de 2014 entrou em vigor no Brasil a Lei nº 12.965, também conhecida como Marco Civil da Internet, sendo a primeira legislação brasileira que buscou regulamentar o desenvolvimento da internet em todo o território nacional, bem como estabelecer os direitos e deveres dos internautas (Brasil, 2014).

A norma apelidada de Lei Carolina Dieckmann foi criada após o furto de 36 fotos íntimas do computador da atriz, seguido de tentativa de extorsão e divulgação das imagens na internet. A Lei nº 12.737/2012 alterou o Código Penal ao incluir os artigos 154-A e 154-B, que tipificam a invasão de dispositivos informáticos e a divulgação de dados pessoais. Além disso, essa lei passou a prever regras para a interrupção ou perturbação de serviço informático, telemático

ou de informação de utilidade pública, bem como a equiparação do cartão de crédito ou débito a documento particular (Brasil, 2012).

Diante desse cenário, surge a seguinte problemática: Quais são os limites e desafios enfrentados pelo ordenamento jurídico brasileiro na responsabilização civil e penal de agentes que utilizam ferramentas de inteligência artificial para manipular imagens e lesar direitos de terceiros?

Apesar da lei, ainda se praticam e aumentam o crimes contra a imagem e honra da pessoa na internet justamente por não ser algo falado nas mídias sociais, e acaba contribuindo para a impunidade dos agentes que manipulam imagens com o uso de inteligência artificial, uma vez que os magistrados ainda precisam se basear em legislações elaboradas antes do surgimento dessas tecnologias.

A escolha do tema justifica-se diante da necessidade de compreender como o uso indevido da inteligência artificial tem gerado novas formas de violação de direitos fundamentais, especialmente o direito à imagem, e como o ordenamento jurídico brasileiro ainda encontra dificuldades em acompanhar essas transformações tecnológicas. Diante do crescimento das inteligências artificiais, capazes de manipular conteúdo, observou-se um cenário preocupante em que reputações são destruídas e vidas são afetadas por montagens praticamente indetectáveis.

Dessa forma, o presente trabalho tem como objetivo analisar a responsabilidade civil e penal decorrente do uso da inteligência artificial na manipulação de imagens com fins ilícitos, e como objetivos específicos: Avaliar os impactos sociais e jurídicos do uso de tecnologias como os *deepfakes*, na reputação e dignidade das vítimas;Verificar como a legislação brasileira atual trata os crimes digitais relacionados à violação de imagem por meio de inteligência artificial; Identificar os principais desafios enfrentados pelos operadores do direito na responsabilização dos agentes que utilizam ferramentas de IA para práticas ilícitas;

Propor reflexões sobre a necessidade de atualização normativa e de novos mecanismos legais para garantir maior proteção aos direitos da personalidade frente aos avanços tecnológicos.

2 A INTELIGÊNCIA ARTIFICIAL E A MANIPULAÇÃO DE IMAGENS DIGITAIS

Para compreender o funcionamento das tecnologias contemporâneas de manipulação de imagens produzidas por inteligência artificial, é necessário retomar alguns conceitos essenciais da ciência da computação.

O primeiro deles é o processamento de linguagem natural (*Natural Language Processing – NLP*), também chamado de linguística computacional. Esse campo surgiu para permitir que computadores consigam interpretar e gerar textos em línguas humanas como português e inglês já que as máquinas não utilizam linguagem natural, mas sim linguagens de programação, tais como *Windows Powershell, JavaScript ou Python.* Como explica Grishman (1986), o NLP foi desenvolvido justamente para traduzir comandos em linguagem humana para códigos operacionais compreensíveis pelos sistemas computacionais, e vice-versa.

Outro conceito relevante é o de redes neurais artificiais, cuja pesquisa teve início ainda na década de 1940, com McCulloch e Pitts, e evoluiu significativamente nos anos seguintes. Segundo Russell e Norvig (2003), as redes neurais podem ser compreendidas a partir de duas abordagens principais: (a) a matemática, que se concentra na criação de arquiteturas e algoritmos complexos, e (b) a biológica, que busca modelar características semelhantes ao funcionamento dos neurônios humanos. Ambas convergem para sistemas computacionais capazes de processar grandes volumes de dados com maior profundidade e rapidez, permitindo conexões e cruzamentos cada vez mais sofisticados.

Com a evolução dessas redes foi possível desenvolver o aprendizado de máquina (*machine learning*), um dos pilares da inteligência artificial moderna. Trata-se de sistemas que aprendem com experiências anteriores, reconhecem padrões e adaptam seu comportamento

a novas situações sem depender de instruções explícitas. Como afirmam Russell e Norvig (2003, p. 2), algoritmos de aprendizado de máquina são capazes de “detectar e extrapolar padrões originalmente atribuídos a eles”, ampliando continuamente sua capacidade de análise.

A partir desses avanços tecnológicos processamento de linguagem natural, redes neurais e aprendizado de máquina chegamos ao conceito contemporâneo de inteligência artificial (IA). Historicamente, o termo foi proposto pela primeira vez por John McCarthy, em 1956, na conferência de Dartmouth, considerado o marco inaugural da área.

Stuart Russell, um dos principais pesquisadores do campo, explica que a IA pode ser estudada sob quatro enfoques: pensamento humano, pensamento racional, comportamento humano e comportamento racional. Para o autor, a IA consiste em uma ciência experimental voltada ao estudo da representação do conhecimento (cognição), raciocínio, aprendizagem, percepção de problemas e solução dos mesmos (Russell; Norvig, 2003, p. 7).

Atualmente, diversas formas de inteligência artificial (IA) são empregadas em diferentes áreas, desde algoritmos que personalizam conteúdos em redes sociais e plataformas de streaming até sistemas capazes de emular processos de pensamento humano. A classificação da IA é feita com base em sua capacidade operacional e funcionalidade, sendo possível identificar três categorias principais. Destaca-se, entre elas, a Inteligência Artificial Limitada — também chamada de Inteligência Artificial Fraca que, embora incapaz de realizar raciocínios autônomos, possui a capacidade de armazenar vastos volumes de dados e executar funções específicas para as quais foi programada. Dentro desta categoria, distinguem-se ainda as máquinas reativas e aquelas dotadas de memória limitada (Salesforce, 2024).

Em razão da novidade que representa para o Direito, o ordenamento jurídico brasileiro ainda carece de uma regulamentação específica voltada ao desenvolvimento, comercialização e,

consequentemente, à atribuição de responsabilidade penal no contexto da inteligência artificial. A primeira iniciativa legislativa relevante é o Projeto de Lei nº 21/2020, atualmente em tramitação no Congresso Nacional, cujo objetivo é estabelecer princípios e fundamentos para o desenvolvimento e a aplicação de sistemas de IA no Brasil (Câmara dos Deputados, 2020).

De acordo com o referido projeto, considera-se sistema de inteligência artificial aquele baseado em processos computacionais que, a partir de objetivos definidos por humanos, seja capaz de processar dados, interpretar o ambiente externo, interagir com ele e realizar predições, recomendações, classificações ou decisões. Para tanto, utiliza-se de técnicas como aprendizagem de máquina (supervisionada, não supervisionada e por reforço), sistemas baseados em conhecimento ou lógica, abordagens estatísticas, inferência bayesiana, métodos de pesquisa e otimização (Brasil, 2023).

É importante destacar que o projeto de lei ressalva a exclusão dos processos de automação que sejam rigidamente orientados por parâmetros fixos de programação, ou seja, que não contemplem a capacidade de aprendizado e interação autônoma com o ambiente, conforme definido no parágrafo único do artigo 2º. Dessa forma, observa-se a importância da criação de um marco regulatório que não apenas conceitue a inteligência artificial de maneira adequada, mas também ofereça instrumentos normativos capazes de disciplinar sua utilização e prever mecanismos de responsabilização em caso de danos provocados por sistemas automatizados.

2.1 O MARCO CIVIL DA INTERNET

A popularização da internet no Brasil teve início em 1995, ano em que se consolidou o seu comércio no país (Arruda, 2011). Desde então, os brasileiros passaram a ter acesso às múltiplas possibilidades oferecidas pelo ambiente digital. Essa expansão impulsionou o desenvolvimento de diversas tecnologias, como novas ferramentas, softwares, redes sociais,

moedas digitais e, mais recentemente, sistemas de inteligência artificial.

Em resposta às transformações advindas da crescente utilização da internet, foi sancionada, em abril de 2014, a Lei nº 12.965 conhecida como Marco Civil da Internet, a primeira legislação brasileira destinada a regulamentar o uso da internet em todo o território nacional, estabelecendo direitos e deveres para os utilizadores (Brasil, 2014). O Marco Civil representa uma resposta legislativa que busca conferir maior segurança jurídica às relações virtuais.

Segundo Teffé (2015, p. 45), "o Marco Civil da Internet, composto por 32 artigos, trata da proteção de registros, dados pessoais e comunicações privadas, da neutralidade da rede, da responsabilidade civil dos provedores e da guarda de registros, prevendo ainda sua requisição por autoridades". Além disso, destaca-se a proteção à privacidade e a promoção da liberdade de expressão como princípios centrais do diploma normativo, visando garantir um ambiente digital livre e plural, sem interferências indevidas ou censura prévia.

Entre os pontos de maior relevância, destaca-se o Capítulo II, que reforça direitos fundamentais já consagrados na Constituição Federal de 1988, como a inviolabilidade da intimidade, da vida privada e das comunicações privadas. No tocante à responsabilidade civil, o artigo 18 do Marco Civil estabelece que os provedores de conexão à internet não podem ser responsabilizados por conteúdos gerados por terceiros (Brasil, 2014).

De acordo com Queiroz (2018), a responsabilidade civil, em regra, é atribuída diretamente a quem realiza o ato ilícito, geralmente pessoas físicas, sendo a responsabilização de terceiros exceção, aplicável apenas nos casos em que não forem tomadas providências após ordem judicial, conforme previsto no artigo 19 da mesma lei.

Portanto, embora o Marco Civil da Internet tenha como foco assegurar direitos fundamentais no uso da rede mundial de computadores e disciplinar a reparação civil de danos causados no ambiente virtual, a norma não trata de forma expressa da responsabilidade penal dos utilizadores ou dos provedores de internet. Diante disto, evidencia a necessidade de

evolução legislativa para enfrentar os novos desafios trazidos pela era digital.

2.2 LEI DOS CRIMES CIBERNÉTICOS

A denominada Lei dos Crimes Cibernéticos, popularmente conhecida como Lei Carolina Dieckmann, surgiu em decorrência de um caso amplamente mediático, no qual a atriz teve seu computador pessoal invadido, resultando no furto de 36 fotografias íntimas que, posteriormente, foram divulgadas sem autorização na internet após uma tentativa de extorsão (Araújo, 2023). Promulgada em 2012, essa legislação promoveu alterações importantes no Código Penal Brasileiro, entre elas, a criação dos artigos 154-A e 154-B, que passaram a tipificar condutas específicas relacionadas à invasão de dispositivos informáticos.

O artigo 154-A do Código Penal passou a descrever o crime de invasão de dispositivo informático como a prática de acessar, sem autorização expressa ou tácita do titular, dispositivos alheios conectados ou não à internet mediante a violação de mecanismos de segurança, com o objetivo de obter, adulterar, destruir dados ou instalar vulnerabilidades para obtenção de vantagem ilícita (Brasil, 2012). Esta inovação legislativa marcou o primeiro reconhecimento formal, no Brasil, de condutas que, até então, eram apenas reprovadas socialmente, mas que careciam de previsão penal específica.

Doutrinadores apontam que a conduta descrita na Lei nº 12.737/2012 caracteriza um crime de perigo abstrato, no qual a simples prática do ato é suficiente para configurar a infração, independentemente da efetiva produção de dano. Jesus e Milagre (2016, p. 15) observam que este tipo penal reflete a preocupação do legislador com o avanço da tecnologia e o risco inerente ao seu uso indevido, justificando a antecipação da tutela penal para proteger bens jurídicos relevantes.

Além da tipificação da invasão de dispositivos, a referida lei também introduziu regras específicas para a interrupção ou perturbação de serviços informáticos, telemáticos ou de informação de utilidade pública, bem como a equiparação de cartões de crédito e débito a

documentos particulares para fins penais (Brasil, 2012). Tais mudanças proporcionaram maior segurança jurídica, ao delimitar com precisão as condutas consideradas criminosas no ambiente digital.

Com a especificação normativa trazida pela Lei 12.737/2012, tanto a acusação quanto a defesa passaram a atuar com maior segurança e previsibilidade, sem a necessidade de recorrer a analogias para fundamentar denúncias ou pedidos de absolvição. Assim, a legislação contribuiu de forma significativa para o fortalecimento do sistema de justiça penal no combate aos crimes informáticos no Brasil.

3 RESPONSABILIDADE CIVIL E PENAL NO USO INDEVIDO DA IA

A responsabilidade civil consiste nas consequências jurídicas de natureza patrimonial decorrentes do descumprimento de obrigações legais ou contratuais, especialmente no que se refere ao dever das empresas de impedir ou reparar danos causados aos utilizadores de seus produtos (Gonçalves, 2022).

No contexto da inteligência artificial (IA), essa responsabilidade apresenta desafios acrescidos, uma vez que se torna complexo identificar quem deve ser responsabilizado por eventuais erros: o operador, o programador, o fornecedor ou o próprio utilizador. Outro ponto sensível é o fato de os algoritmos de IA serem frequentemente treinados a partir de grandes volumes de dados (big data), os quais, caso contenham preconceitos ou discriminações, podem replicá-los nos resultados gerados, perpetuando injustiças sociais. Um exemplo clássico é o de algoritmos de recrutamento que, baseando-se em dados históricos enviesados, favorecem candidatos do sexo masculino em detrimento das mulheres, contribuindo assim para a manutenção da desigualdade de género no mercado de trabalho.

No que tange à responsabilidade penal relacionada à utilização da inteligência artificial na prática de crimes digitais, a doutrina brasileira apresenta duas principais correntes. A primeira sustenta que os crimes cometidos com o auxílio de IA já encontram previsão no

Código Penal Brasileiro, sendo a internet apenas o meio utilizado para a consumação da infração (Reis, 2021). Nesse sentido, Patrícia Peck Pinheiro (2021, p. 223) ressalta que "a maioria dos crimes cometidos na rede ocorre também no mundo real", sendo a internet apenas uma facilitadora, especialmente devido ao anonimato que proporciona. Assim, o conceito de crime e suas consequências jurídicas manteriam-se idênticos tanto no Direito Penal tradicional quanto no Direito Penal Digital.

Em contrapartida, uma segunda vertente doutrinária aponta que a ausência de uma tipificação penal específica para os chamados crimes virtuais tem levado o sistema jurídico a recorrer à analogia in malam partem para fundamentar a responsabilização dos agentes (Reis, 2021). Tal prática, contudo, encontra resistência à luz do princípio da legalidade estrita, fundamental no ordenamento jurídico brasileiro. Como bem destacam Damásio de Jesus e José Antônio Milagre (2016, p. 12), o Brasil adota o sistema da reserva legal, de modo que "não há crime sem lei anterior que o defina". Além disso, salientam que, no campo da tecnologia da informação, a criação legislativa deve ser especialmente cuidadosa, sob pena de se produzir normas obsoletas já no momento da sua promulgação.

No que diz respeito à classificação dos crimes envolvendo inteligência artificial, destaca-se a ideia de que tais infrações configuram crimes de forma vinculada. Diferentemente dos crimes comuns praticados na internet, aqui a rede não atua meramente como meio, mas sim como forma específica de execução do ato ilícito. Assim, a utilização da IA não apenas facilita, mas estrutura a própria prática criminosa, exigindo uma análise mais atenta e específica do legislador e dos operadores do direito quanto às novas modalidades de delinquência digital.

De acordo com Ribeiro (2017), a criação de normas técnicas e específicas é fundamental para o combate eficaz dos crimes informáticos. Embora o ordenamento jurídico brasileiro já tenha incorporado legislações destinadas a essa finalidade, tais dispositivos ainda se mostram insuficientes. As leis existentes contemplam apenas uma parcela restrita das diversas formas de criminalidade virtual, além de carecerem da precisão terminológica

necessária para acompanhar a complexidade técnica envolvida. Diante da constante e acelerada evolução tecnológica, diariamente surgem novas modalidades de delitos cibernéticos, ultrapassando a capacidade de atualização da legislação vigente.

A preparação técnica dos órgãos de investigação desempenha igualmente um papel essencial na apuração dos crimes informáticos e na correta identificação de seus autores. No Brasil, país de grande extensão territorial e elevada população, observa-se um preocupante despreparo das autoridades investigativas, sendo escassas as delegacias especializadas em crimes cibernéticos. A deficiência legislativa, aliada a práticas investigativas defasadas e à sensação de anonimato proporcionada pela internet, tem contribuído para o aumento significativo dos índices de criminalidade virtual nos últimos anos.

Para que haja uma repressão eficaz às práticas ilícitas no meio digital, torna-se imperativa a modernização constante de todos os setores envolvidos, incluindo a elaboração de normas jurídicas atualizadas e a capacitação permanente das equipes de investigação. É imprescindível que estas estejam familiarizadas com as tecnologias utilizadas pelos chamados crackers e com as técnicas mais recentes de intrusão e manipulação de dados.

Em relação ao perfil dos agentes que cometem crimes informáticos, verifica-se que, embora a prática possa ser realizada por indivíduos com conhecimentos básicos, predomina a atuação de sujeitos com razoável ou elevado domínio técnico, sobretudo em delitos que envolvem invasão de sistemas e programação especializada. Essa realidade impõe desafios adicionais às autoridades, que necessitam de provas materiais e indícios de autoria para a propositura da ação penal.

3.1 O CÓDIGO PENAL E A RESPONSABILIZAÇÃO PENAL NO USO DA IA

Com o avanço da inteligência artificial e sua aplicação em diversas áreas, inclusive na manipulação de imagens com fins ilícitos, o Direito Penal brasileiro enfrenta novos desafios em relação à responsabilização de condutas realizadas por ou com o auxílio dessas

tecnologias. De acordo com o artigo 1º do Código Penal e sua Lei de Introdução, a responsabilização penal é, tradicionalmente, direcionada a pessoas físicas, sem que haja previsão específica para agentes não humanos, como sistemas de inteligência artificial (Paula; Cornwall; Cabra, 2019).

O sistema penal brasileiro adota o modelo finalista de Hans Welzel, no qual o crime é compreendido como uma conduta humana voluntária e dirigida a um fim, com dolo ou culpa. Essa concepção exige a presença de vontade consciente ou, no caso da culpa, a ocorrência de negligência, imprudência ou imperícia (Morais, 2023). Esse entendimento, contudo, não abarca entidades que não possuam consciência ou discernimento moral, como os sistemas autônomos de IA, o que dificulta sua responsabilização penal direta.

A culpabilidade, um dos elementos essenciais do crime, está diretamente ligada à imputabilidade, à consciência da ilicitude do fato e à exigibilidade de conduta diversa. Segundo os autores, a imputabilidade "consiste na capacidade mental de compreender o caráter ilícito do fato", o que é inviável de ser atribuído à inteligência artificial, considerando seu funcionamento baseado em algoritmos e não em julgamento moral (Estefam; Gonçalves, 2019).

Embora a responsabilização penal de pessoas jurídicas já seja admitida em casos específicos, como nos crimes ambientais, conforme o artigo 225, §3º da Constituição Federal de 1988, ainda não há previsão legal para estender tal responsabilização à inteligência artificial ou aos próprios sistemas automatizados. Assim, quando esses sistemas são utilizados de forma ilícita, a responsabilização recai sobre seus operadores, programadores ou usuários finais (Brasil, 1988).

No campo do Direito Civil, há maior abertura doutrinária para se reconhecer a responsabilidade por danos causados por sistemas autônomos, utilizando-se, em muitos casos, da responsabilidade objetiva. No entanto, no âmbito penal, essa discussão ainda é

incipiente e cercada de limitações conceituais (Reale, 2020).

Segundo Sousa (2020), a responsabilização penal de agentes não humanos exige uma reavaliação dos fundamentos clássicos do Direito Penal. Ele argumenta que, com a crescente sofisticação dos sistemas autônomos, torna-se imprescindível refletir sobre os limites da responsabilidade jurídica e os critérios de imputação penal.

Nesse contexto, é necessário considerar a possibilidade de que o ordenamento jurídico evolua no sentido de criar dispositivos específicos para lidar com infrações praticadas por meio da inteligência artificial. Enquanto isso não ocorre, a responsabilização penal seguirá restrita a indivíduos com plena capacidade mental e às pessoas jurídicas nos casos expressamente previstos em lei.

A manipulação de imagens com uso de IA, com o intuito de causar prejuízos a terceiros, como violação de honra, imagem e privacidade, coloca em xeque a eficácia das normas penais atuais. Assim, é urgente promover o debate jurídico sobre atualizações legislativas, a fim de garantir que a evolução tecnológica não se sobreponha à proteção dos direitos fundamentais.

3.2 DESAFIOS ENFRENTADOS NA RESPONSABILIZAÇÃO DO USO DE IA DE FORMA ILÍCITA

O uso da inteligência artificial tem imposto desafios inéditos aos modelos tradicionais de responsabilização civil e penal, principalmente devido à autonomia e complexidade dos sistemas baseados em aprendizado de máquina (*machine learning*) e aprendizado profundo

(*deep learning*). Diferentemente dos softwares convencionais, as tecnologias contemporâneas não apenas executam comandos previamente determinados, mas aprendem, modificam parâmetros internos e produzem resultados novos, muitas vezes imprevisíveis até mesmo para seus desenvolvedores. Essa capacidade de adaptação gera incertezas sobre a autoria, o nexo causal e o grau de culpa humana envolvida em condutas

ilícitas praticadas com auxílio da IA.

Além disso, a criação de conteúdos manipulados especialmente imagens e vídeos falsificados, como os *deepfakes* intensifica as dificuldades de imputação de responsabilidade. Sistemas capazes de gerar representações hiper-realistas ampliam o risco de crimes contra a honra, pornografia não consensual, fraudes e danos à imagem pública de indivíduos, dificultando a identificação do agente responsável pelo material ilícito.

Como destaca Floridi (2022), o cenário tecnológico contemporâneo lida com agentes artificiais que, embora desprovidos de personalidade jurídica, intervêm diretamente no processo de produção de danos, exigindo novas formas de interpretação normativa.

De acordo com Soyer e Tettenborn (2023), é indispensável o desenvolvimento de regimes de responsabilidade diferenciados para aplicações de IA considerando o nível de risco envolvido. Em setores de alto impacto, como saúde, segurança pública e transporte, os autores defendem a adoção da responsabilidade objetiva, assegurando a reparação independentemente da comprovação de culpa. Já para áreas de menor risco, sugerem a manutenção da responsabilidade subjetiva, de modo a equilibrar inovação tecnológica e segurança jurídica.

Entretanto, os desafios não se limitam à escolha do regime de responsabilidade. Um ponto crucial diz respeito à fragmentação da cadeia de atores envolvidos. Na criação de imagens manipuladas por IA, podem existir múltiplos responsáveis: desenvolvedores da tecnologia, provedores de plataformas, usuários finais e terceiros que distribuem o conteúdo ilícito. A ausência de um responsável único dificulta a determinação do nexo causal e a imputação jurídica.

Nesse sentido, Hildebrandt (2020) afirma que “os sistemas algorítmicos contemporâneos operam dentro de ecossistemas distribuídos, nos quais a causalidade é compartilhada e diluída”, tornando insuficientes os modelos tradicionais de culpa individual.

Outro obstáculo relevante consiste nas limitações técnicas das perícias digitais. A sofisticação das imagens geradas por redes neurais generativas especialmente GANs (*Generative Adversarial Networks*) torna cada vez mais difícil distinguir material autêntico de conteúdo manipulado. Peritos judiciais enfrentam, assim, um cenário em que a prova digital pode ser facilmente contestada, comprometendo a produção de evidências essenciais à responsabilização penal.

Conforme observa Chesney e Citron (2019), a expansão dos *deepfakes* cria uma "crise

de autenticidade", na qual tanto conteúdos falsos podem parecer reais quanto conteúdos reais podem ser falsamente alegados como manipulados.

No âmbito jurídico brasileiro, o desafio é ainda maior devido à ausência de regulamentação específica, o que obriga magistrados e operadores do Direito a interpretar normas anteriores ao surgimento dessas tecnologias. As lacunas legislativas tornam a aplicação da lei menos uniforme e dificultam a responsabilização efetiva do agente.

O Marco Civil da Internet e a Lei dos Crimes Cibernéticos fornecem orientações gerais, mas não contemplam de forma direta a manipulação avançada de imagens por IA criando zonas cinzentas quanto à autoria, intenção e materialidade do delito.

Nesse contexto, a regulamentação da responsabilidade civil no uso da inteligência artificial deve adotar uma abordagem híbrida, combinando os regimes de responsabilidade objetiva e subjetiva conforme a natureza do dano e o contexto da aplicação tecnológica. Como apontam Soyer e Tettenborn (2023), essa solução permite "harmonizar decisões humanas e automatizadas sob o mesmo regime de responsabilidade", equilibrando o avanço tecnológico com a proteção dos direitos dos lesados.

Além disso, diversos autores sugerem que o Direito avance na criação de parâmetros específicos para casos envolvendo IA incluindo deveres claros de diligência para

desenvolvedores, plataformas e usuários, mecanismos de auditoria algorítmica e políticas robustas de transparência no treinamento e operação dos modelos (Floridi, 2022; Hildebrandt, 2020).

Assim, os desafios da responsabilização no uso ilícito da IA não se restringem apenas à técnica ou à legislação, mas envolvem uma transformação mais ampla sobre como o Direito compreende causalidade, culpa, autoria e prova em um cenário tecnológico em constante evolução.

3.3 PRECEDENTES JURÍDICOS EM CASOS RELACIONADOS

Um caso recente e emblemático, que serve de base para reflexão sobre os limites e desafios do ordenamento jurídico frente à inteligência artificial, envolve a Deputada Federal Tabata Amaral. A parlamentar foi vítima de manipulação digital por meio de *deepfake*, uma das mais sofisticadas ferramentas de inteligência artificial voltada à geração de imagens falsas com aparência real.

Entre os meses de agosto e setembro de 2024, passaram a circular nas redes sociais imagens sensuais atribuídas à Deputada, com evidente conotação sexual. A repercussão foi imediata e intensa, especialmente por se tratar de uma figura pública com reputação ilibada.

Como já apontado anteriormente neste trabalho, pesquisas indicam que a maioria dos brasileiros ainda encontra dificuldades em distinguir imagens geradas por IA daquelas captadas por meios tradicionais, o que contribuiu para a comoção pública e agravou os efeitos do ato criminoso.

Essas imagens falsas comprometeram diretamente a reputação da parlamentar e trouxeram prejuízos significativos à sua campanha eleitoral. De acordo com o portal G1, as imagens foram divulgadas com legendas que, embora apresentassem dados verdadeiros sobre sua trajetória política, tinham nítido caráter satírico e depreciativo. Trata-se, claramente, de uma

tentativa de abalar sua imagem pública e minar sua candidatura à prefeitura da capital paulista.

Ainda segundo reportagens, mesmo com o realismo das imagens, peritos identificaram falhas típicas de criações por IA. Em uma das fotos, por exemplo, foi constatado que o comprimento das pernas destoava da anatomia humana padrão indício comum em composições digitais. Além disso, características como a forma das mãos, os detalhes nos cabelos e a definição das bordas revelaram inconsistências técnicas comuns em imagens sintéticas. Contudo, essas falhas tendem a desaparecer à medida que as ferramentas de IA se tornam mais avançadas, tornando a detecção de falsificações cada vez mais difícil o que levanta preocupações sérias sobre o futuro da integridade da imagem pessoal na era digital.

A jurisprudência brasileira tem se manifestado sobre a matéria, especialmente no âmbito eleitoral. O Tribunal Regional Eleitoral de Minas Gerais (TRE-MG), por exemplo, concedeu mandado de segurança em um caso no qual a imagem do avô falecido de um candidato foi manipulada e utilizada em um vídeo por adversários políticos. A decisão reforçou a proibição do uso de *deepfakes* durante o período eleitoral, conforme a nova redação da Resolução TSE n° 23.610/2019, modificada pela Resolução n° 23.732/2024 (Brasil, 2024), a ementa é clara:

Mandado De Segurança. Decisão Proferida Pelo Juízo Eleitoral. Indeferimento De Pedido Liminar Em Representação Eleitoral. Preliminar De Inépcia Da Petição Inicial. Ausência De Degravação E Íntegra De Vídeo. Rejeição. Mérito. Utilização De Inteligência Artificial (Ia). Deep Fake Em Período Pré-Eleitoral. Impossibilidade. Vedação Total, Independentemente De Induzir O Eleitorado A Erro. Concessão Da Segurança.

(Tre-Mg – Mandado De Segurança Cível: Msciv Xxxxx-47.2024.6.13.0000, Uberlândia-Mg, 22/08/2024).

Essa decisão sinaliza o posicionamento do Judiciário quanto à necessidade de coibir o uso de tecnologias de manipulação digital que possam comprometer a lisura do processo eleitoral.

No entanto, mesmo com tais avanços normativos e jurisprudenciais, ainda não há um sistema de controle eficaz que permita identificar e punir, de forma célere, os responsáveis por esses atos ilícitos. No caso da Deputada Tabata Amaral, por exemplo, até o momento da conclusão desta pesquisa, os autores da montagem não foram identificados, o que evidencia a fragilidade na proteção dos direitos fundamentais diante da velocidade de disseminação dessas imagens.

O episódio também reforça a importância de se debater o direito à imagem, à privacidade e à honra no ambiente digital, bem como a necessidade de se estabelecer limites à liberdade de expressão, especialmente quando ela serve de escudo para práticas ofensivas e ilícitas. Como alerta Daniella Scott (2020), "a humilhação pública decorrente do uso de *deepfakes* pode ser devastadora, especialmente para as mulheres, que muitas vezes enfrentam uma dupla penalização: a exposição de sua imagem e a desconfiança social sobre sua veracidade".

Portanto, esse caso concreto serve como ponto de partida para reflexões profundas sobre o uso da inteligência artificial na criação de realidades simuladas, suas consequências jurídicas e sociais, e a urgência de medidas legislativas e institucionais mais eficazes no combate a essas práticas. Além disso, evidencia a necessidade de conscientização da sociedade sobre a responsabilidade na disseminação de conteúdos digitais, especialmente em um contexto de crescente desinformação. A liberdade de expressão, embora assegurada constitucionalmente, não pode ser utilizada como justificativa para ferir direitos alheios e desestabilizar o processo democrático.

4 METODOLOGIA

A metodologia utilizada no desenvolvimento do presente trabalho trata-se de pesquisa bibliográfica e documental, com o intuito de analisar os posicionamentos doutrinários sobre a responsabilidade civil e penal pelo uso de inteligência artificial na manipulação de imagens

com fins ilícitos, assim como examinar decisões jurisprudenciais que tratam do tema, complementa-se a pesquisa com opinião crítica dos entendimentos doutrinários e jurisprudenciais coletados.

Para a realização da pesquisa, foram adotados procedimentos metodológicos fundamentados em pesquisas documental e bibliográfica. Segundo Gil (2018), a pesquisa documental caracteriza-se pelo exame de documentos de primeira mão, que não receberam tratamento analítico prévio, tais como documentos oficiais, reportagens de jornais, diários, filmes e fotografias. Além disso, a pesquisa documental pode utilizar fontes secundárias, como relatórios, fichas de cadastro e demais registros administrativos que fornecem subsídios relevantes à investigação.

O presente estudo fundamenta-se no método dedutivo, caracterizando-se por uma abordagem qualitativa. Essa abordagem prioriza a descrição e a interpretação aprofundada do tema, sem se ater exclusivamente à quantificação das informações. Dessa forma, com um objetivo descritivo, o procedimento adotado foi essencialmente bibliográfico, compreendendo uma ampla sondagem de dados extraídos de doutrinas, artigos científicos, livros, teses, monografias, legislação e jurisprudências. O estudo busca, assim, estabelecer uma relação entre conceitos, ideias e características do tema proposto.

5 CONSIDERAÇÕES FINAIS

O presente estudo permitiu demonstrar que o uso de inteligência artificial para manipulação de imagens com fins ilícitos representa um dos maiores desafios contemporâneos para o Direito, especialmente no campo da responsabilidade civil e penal. A tecnologia de *deepfake*, amplamente discutida ao longo deste artigo, evidencia o potencial danoso da síntese digital e sua capacidade de afetar diretamente a honra, a imagem e a vida privada dos indivíduos, produzindo efeitos que extrapolam o ambiente virtual e alcançam dimensões sociais, psicológicas e políticas.

A análise da legislação brasileira demonstra que, embora não exista um diploma legal específico voltado exclusivamente aos delitos praticados por IA, há dispositivos capazes de fundamentar a responsabilização dos agentes, tanto na esfera civil quanto na penal. O Código Civil, ao proteger a honra e a imagem, e o Código Penal, ao prever crimes contra a honra, já fornecem mecanismos iniciais de tutela. Além disso, o Marco Civil da Internet regula a responsabilidade dos provedores e assegura direitos fundamentais no ambiente digital. Contudo, tais instrumentos não dão conta, por si só, da complexidade técnica dos delitos envolvendo novas tecnologias. Falta, portanto, precisão normativa, definição técnica adequada e, sobretudo, meios eficientes de investigação.

O caso analisado, envolvendo a deputada federal Tabata Amaral, reforça a tese de que os danos provocados pelas montagens digitais podem ser devastadores, impactando não apenas a esfera privada, mas também o processo democrático e a vida pública. Ainda que o Tribunal Regional Eleitoral de Minas Gerais tenha confirmado a vedação total do uso de *deepfakes* no período eleitoral, a dificuldade de rastrear os responsáveis permanece como um obstáculo relevante. A ausência de mecanismos robustos de identificação digital e a rapidez com que conteúdos falsos se disseminam nas redes sociais contribuem para um cenário de insegurança, no qual os danos se concretizam antes mesmo de qualquer medida judicial.

Diante disso, torna-se evidente a necessidade de modernização legislativa. É imprescindível que o Direito acompanhe a evolução tecnológica, criando normas específicas para lidar com a síntese digital e com seus potenciais abusos, sem, contudo, comprometer a liberdade de expressão e a inovação tecnológica. Paralelamente, o Estado deve investir na capacitação contínua de peritos e autoridades investigativas, ampliando o número de delegacias especializadas e fortalecendo parcerias com instituições de tecnologia e pesquisa.

Além dos aspectos jurídicos, este estudo também chama atenção para o papel fundamental da educação digital. A sociedade precisa estar mais bem preparada para reconhecer

conteúdos manipulados e para compreender os riscos de compartilhá-los sem verificação prévia. A responsabilização social, portanto, deve caminhar ao lado da responsabilização jurídica.

Por fim, o enfrentamento do uso indevido da inteligência artificial não depende apenas de reformas legislativas, mas de uma atuação coordenada entre Estado, sociedade, provedores de tecnologia e órgãos de investigação. A construção de um ambiente digital seguro exige a combinação de normas eficientes, técnicas avançadas de detecção, políticas públicas de conscientização e uma cultura social de verificação da informação. Somente assim será possível reduzir a impunidade, proteger a dignidade humana e garantir que as ferramentas tecnológicas sejam utilizadas para o progresso, e não para a violação de direitos fundamentais.

REFERÊNCIAS

ARAÚJO, Janaína. **Dez anos de vigência da Lei Carolina Dieckmann:** a primeira a punir crimes cibernéticos. Rádio Senado, 2023. Disponível em:

https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-leicarolinadieckmann-a-primeira-a-punircrimesciberneticos#:~:text=Dos%20seis%20meses%20a%20dois,Da%20R%C3%A1dio%20S enado %2C%20Jana%C3%ADna%20Ara%C3%BAjo, Acesso em: 24 abril 2025.

BRASIL. **Lei 12.737, de 30 de novembro de 2012.** Lei dos crimes cibernéticos, Brasília, DF: Diário Oficial da União, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 24 abril 2025.

BRASIL. **Lei 12.965, de 23 de abril de 2014.** Marco Civil da Internet, Brasília, DF: Diário Oficial da União, 2014. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato20112014/2014/lei/l12965.htm. Acesso em: 24 abril 2025.

BRASIL. **Constituição (1988).** Constituição da República Federativa do Brasil.Brasília: Senado. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 12 jun 2025.

BRASIL. **Senado Federal. Projeto de Lei 2.338/2023.** Dispõe sobre o uso da Inteligência

Artificial. 2023, Disponível em: https://www25.senado.leg.br/web/atividade/materias//materia/157233. Acesso em:24 abril 2025.

BRASIL. Tribunal Regional Eleitoral de Minas Gerais. **Mandado de Segurança Cível: MSCiv XXXXX-47.2024.6.13.0000**, Uberlândia-MG, 22 ago. 2024.

CÂMARA DOS DEPUTADOS, **Projeto de Lei 21 de 2020**, disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236340. Acesso em: 24 abril 2025.

CASTILHO, Bianca Gabrielli Borges. **Responsabilidade civil na violação dos direitos da personalidade através da inteligência artificial no Brasil.** Trabalho de Conclusão de Curso. 2024.

ESTEFAM, André; GONCALVES, Victor Eduardo Rios. Direito penal esquematizado: parte geral. 8. ed. São Paulo: Saraiva, 2019

JESUS, Damásio de; MILAGRE, Jose Antônio. **Manual de crimes informáticos.** São Paulo Saraiva, 2026.

GIL, Antônio Carlos. **Metodologia do Ensino Superior.** São Paulo: Atlas. 2018.

GONCALVES, Carlos R. Direito Civil Brasileiro: **Responsabilidade Civil.** v.4. São Paulo/SP: Editora Saraiva, 2023. E-book. ISBN 9786553628410. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553628410/. Acesso em: 25 abril 2025.

KORSHUNOV, P; MARCEL, S. Vulnerability assessment and detection of deepfake videos. In 2019 International Conference on Biometrics (ICB)(pp. 1-6). IEEE. 2019. https://doi.org/10.1109/ICB45273.2019.8987375 > Acesso em: 25 abril 2025.

MORAIS, Renato Watanabe de. **Programações podem ser punidas?**Responsabilidade penal em decisões tomadas pela inteligência artificial. Rio de Janeiro: Revista Científica do CPJM, 2023. Disponível em: https://rcpjm.emnuvens.com.br/revista/article/download/217/187. Acesso em: 15 jun 2025.

PAULA, Alice Lima; CORNWALL, Bruno Meirelles de M.; CABRAL, Dalila M. **Breves reflexões sobre a inteligência artificial e seus impactos no campo do Direito Penal.**In: CHAVES, Natália Cristina (org.). Direito, tecnologia e globalização. [online]. Porto Alegre, 2019. p. 98-117. Disponível em: https://www.direito.ufmg.br/wpcontent/uploads/2019/12/direito_tecnologia_globalizacao.pdf. Acesso em 17 jun 2025.

PINHEIRO, Patrícia Peck. **Direito digital.** 7. ed. São Paulo: Saraiva Educação, 2021. e-book.

QUEIROZ, João Quinelato de. **A responsabilidade civil dos provedores de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros:** análise na perspectiva civil- constitucional. Universidade Estadual do Rio de Janeiro. Dissertação de Mestrado. 2018. Disponível em: http://www.bdtd.uerj.br/handle/1/9862. Acesso em: 27 abril 2024.

REALE JUNIOR, M. **Fundamentos de Direito Penal,** 5ª ed. São Paulo: Grupo GEN, 2020. p. 42.

RUSSELL, Stuart; NORVIG, Peter. *Artificial intelligence: a modern approach*. 2. ed. Upper Saddle River: Prentice Hall, 2003.

SCOTT, Daniella. **The terrifying rise of deepfake porn.** Cosmopolitan UK, 2020.

SOUSA, Susana Aires de. "**Não fui eu, foi a máquina":** Teoria do crime, responsabilidade e inteligência artificial. Inteligência artificial no Direito Penal. Coimbra: Almedina, 2020, p. 68111.

---

[1]Graduando do curso de Bacharelado em Direito no Centro Universitário Fametro, Manaus, Brasil. E-mail:lucasgombr92@gmail.com

[2]Orientadora, Profª. Especialista do Departamento de Direito da Fametro do Centro Universitário Fametro, Manaus, Amazonas, Brasil, E-mail: rosanareismello@gmail.com.

[3] Coorientadora. Professora do Centro Universitário Fametro. Mestra em Direito Ambiental pela Universidade do Estado do Amazonas. Advogada. Manaus, Amazonas, Brasil. E-mail: leda.domingos@fametro.edu.br.