Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v12i6.27466

O USO DE DEEPFAKES EM ESTELIONATO E FALSA IDENTIDADE: ANÁLISE DOS DESAFIOS JURÍDICOS E DOS RISCOS À ATUAÇÃO PROFISSIONAL DE ADVOGADOS

Juliana Garcia de Souza[1]
Rosana Reis de Melo Silva[2]

RESUMO: O avanço acelerado da inteligência artificial impulsionou o surgimento dos *deepfakes*, conteúdos audiovisuais sintéticos que reproduzem rostos e vozes com notório realismo, facilitando a prática de delitos complexos no ciberespaço. Embora tais tecnologias tenham tido finalidades voltadas ao entretenimento e comunicação digital, seu uso indevido apresenta ameaças à segurança jurídica e patrimonial no ambiente virtual. O presente artigo científico teve como objetivo analisar os impactos do uso indevido das *deepfakes* em práticas de estelionato e falsificação de identidade no ambiente digital, com destaque para golpes praticados mediante o uso fraudulento da imagem e da identidade profissional dos advogados. A pesquisa buscou apreciar os desafios enfrentados pelo ordenamento jurídico-penal brasileiro diante da crescente sofisticação dos crimes digitais, especialmente no que tange à identificação da autoria, à produção de provas digitais e à prevenção de danos às vítimas. A fundamentação teórica apoiou-se em estudos sobre inteligência artificial, engenharia social e criminalidade cibernética, correlacionando-os aos tipos penais previstos nos artigos 171 e 307 do Código Penal Brasileiro, assim como à legislação relacionada à proteção de dados e aos crimes informáticos. A metodologia adotada consistiu em pesquisa bibliográfica e documental, com abordagem qualitativa, exploratória e descritiva, baseada em doutrina, artigos científicos, relatórios institucionais e materiais publicados entre 2020 e 2025. Os resultados demonstraram que os *deepfakes* potencializam práticas fraudulentas ao aumentar a credibilidade dos atos criminosos, dificultando a percepção das vítimas e impondo obstáculos técnicos à investigação e à responsabilização penal. Conclui-se que o enfrentamento eficaz dessas práticas exige atuação integrada entre atualização legislativa, fortalecimento da perícia digital, desenvolvimento de políticas públicas de educação digital e adoção de medidas preventivas por profissionais da advocacia e instituições públicas.

Palavras-chave: Deepfakes. Estelionato. Falsa identidade. Advocacia. Segurança digital.

[1]Graduanda do curso de Bacharelado em Direito, Faculdade Metropolitana de Manaus (FAMETRO).
[2]Professora Orientadora do curso de Bacharelado em Direito, Centro Universitário FAMETRO.

ABSTRACT: The accelerated advancement of artificial intelligence has driven the emergence of deepfakes, synthetic audiovisual content capable of reproducing faces and voices with remarkable realism, facilitating the commission of complex crimes in cyberspace. Although such technologies were initially developed for entertainment and digital communication purposes, their misuse poses threats to legal certainty and property security in the virtual environment. This scientific article aimed to analyze the impacts of the misuse of *deepfakes* in fraud and identity falsification practices in the digital environment, with emphasis on scams committed through the fraudulent use of lawyers' image and professional identity. The research sought to examine the challenges faced by the Brazilian criminal legal system in light of the increasing sophistication of digital crimes, especially regarding the identification of authorship, the production of digital evidence, and the prevention of harm to victims. The theoretical framework was based on studies concerning artificial intelligence, social engineering, and cybercrime, correlating them with the criminal offenses established in articles 171 and 307 of the Brazilian Penal Code, as well as legislation related to data protection and cybercrimes. The methodology consisted of bibliographic and documentary research, adopting a qualitative, exploratory, and descriptive approach, based on legal doctrine, scientific articles, institutional reports, and materials published between 2020 and 2025. The results demonstrated that *deepfakes* enhance fraudulent practices by increasing the credibility of criminal acts, hindering victims' perception and imposing technical obstacles to criminal investigation and accountability. It is concluded that the effective confrontation of such practices requires integrated action involving legislative updates, strengthening of digital forensics, development of public policies for digital education, and adoption of preventive measures by legal professionals and public institutions.

Keywords: Deepfakes. Fraud. False identity. Advocacy. Cybersecurity.

1 INTRODUÇÃO

A partir de meados do século XX, a Era da Informação, também denominada Terceira Revolução Industrial, caracteriza-se por expressivos avanços tecnológicos. O surgimento da inteligência artificial, impulsionada pelo aperfeiçoamento de técnicas que ampliaram suas aplicações, proporcionou o crescimento exponencial dos *deepfakes*[3], conteúdos audiovisuais sintéticos capazes de reproduzir rostos, vozes e ações com elevado grau de realismo.

A evolução digital da comunicação esteve voltada à ampliação da conectividade em tempo real e ao atendimento das demandas virtuais de seus usuários. Gradualmente, os meios digitais consolidaram-se como instrumentos indispensáveis às atividades cotidianas, assumindo papel central nas relações sociais, econômicas e institucionais. Embora os *deepfakes* tenham apresentado expansão inicial vinculada ao entretenimento e à exploração das potencialidades tecnológicas, posteriormente passaram a ser empregados em práticas ilícitas.

[3] Tecnologia instrumentalizada em inteligência artificial utilizada para criar vídeos, imagens ou áudios falsificados com aparência realística.

Alimentados por bases de dados fornecidas por usuários e continuamente aperfeiçoados por sistemas de inteligência artificial, tais conteúdos sintéticos favorecem a obtenção indevida de vantagem econômica, a manipulação reputacional e a usurpação de identidade.

No atual cenário virtual brasileiro, observa-se crescente incidência de golpes praticados mediante falsa identidade de profissionais da advocacia. Nessa modalidade criminosa, agentes utilizam indevidamente nomes reais, números de inscrição profissional, informações processuais autênticas ou adulteradas e recursos tecnológicos de simulação de voz e imagem para conferir aparência de legitimidade à fraude. O objetivo consiste em induzir clientes ao erro, comumente mediante solicitação de valores para suposta liberação de alvarás, pagamento de custas processuais ou levantamento de quantias judiciais. Conforme destaca Peck (2021), a transformação digital ampliou a exposição de dados pessoais e profissionais, tornando a identidade eletrônica ativo vulnerável a múltiplas formas de uso indevido.

Diante desse problema, a base central da presente pesquisa consiste em analisar em que medida o ordenamento jurídico-penal brasileiro mostra-se apto a enfrentar fraudes patrimoniais praticadas por meio de *deepfakes* e da falsa identidade profissional de advogados, em uma era de constante evolução digital.

Nesse contexto, embora a legislação vigente ofereça instrumentos relevantes de repressão, ainda subsistem fragilidades diante da crescente sofisticação das fraudes digitais praticadas por meio de *deepfakes*. Logo, Bezerra e Agnoletto (2020) observam que a criminalidade cibernética impõe obstáculos investigativos próprios, exigindo constante atualização técnica e integração institucional.

O objetivo geral do presente estudo consiste em analisar os impactos do uso indevido de *deepfakes* no ambiente digital como mecanismo de fraude patrimonial, com ênfase nos golpes praticados mediante falsa identidade de advogados. Entre os objetivos específicos, pretende-se examinar os fundamentos teóricos e as ferramentas digitais relacionadas ao tema; identificar o enquadramento jurídico-penal aplicável às condutas delituosas; apurar implicações relativas à autoria e à prova digital; e propor medidas preventivas voltadas à segurança digital.

A metodologia adotada baseou-se no método dedutivo, com abordagem qualitativa e cunho exploratório, desenvolvendo-se por meio de revisão bibliográfica referente ao período de 2020 a 2025. Para tanto, foram analisados artigos científicos, obras doutrinárias e documentos institucionais pertinentes ao tema. A estrutura do artigo foi organizada em seções que

abrangem os fundamentos técnicos dos *deepfakes*, sua utilização criminosa, os desafios jurídico-penais e os impactos relacionados à segurança digital na advocacia.

2 ASPECTOS TÉCNICOS DOS DEEPFAKES E SUA UTILIZAÇÃO CRIMINOSA

O crescimento acelerado da Internet pode ser comparado a um eixo neural social, visto que cada indivíduo atua como uma unidade essencial que transmite e recebe impulsos por toda uma rede estrutural. A cocriação em inteligência artificial moldou novas camadas de produção informacional, intensificando a geração, a circulação e o consumo de dados no meio virtual. Destaca-se, assim, o presente mecanismo global, com capacidade de gerar conteúdos sintéticos manipulados por usuários capacitados e produzidos por sistemas computacionais avançados, capazes de adulterar voz, imagem, vídeo e comportamento humano com elevado grau de verossimilhança. Atualmente, a modelagem das inteligências artificiais acrescenta uma dimensão de realidade que exige atenção minuciosa a seus detalhes. Conforme Peck discorre em sua obra:

> A dinâmica da era da informação exige uma mudança mais profunda na própria forma como o Direito é exercido e pensado em sua prática cotidiana. Toda mudança tecnológica é uma mudança social, comportamental, portanto, jurídica. Quando a sociedade muda, deve o Direito também mudar, evoluir. (PINHEIRO, 2021, p. 31-32).

Emergidas como ferramentas inicialmente utilizadas para fins lícitos, como se observa em redes sociais, suas aplicações abrangem o entretenimento, a publicidade, a propaganda, a acessibilidade e a inovação tecnológica no contexto da Era da Informação, considerando-se a tendência crescente de digitalização da sociedade. Porém, tais ferramentas passaram a ser utilizadas e modificadas para práticas indevidas, como campanhas de desinformação, violação de direitos de personalidade e, no âmbito dos crimes cibernéticos, como instrumento para fraudes associadas à falsa identidade. No cenário em questão, a constante evolução tecnológica impõe novos desafios ao campo do Direito, especialmente na esfera digital, no que se refere à proteção da identidade digital, à preservação da confiança social e à responsabilização por condutas praticadas em ambiente virtual.

Dessa forma, na atual realidade, torna-se imprescindível compreender as novas formas de fraude patrimonial e digital, bem como as dinâmicas de manipulação de imagem, correlacionadas ao estudo dos *deepfakes*, a fim de viabilizar a aplicação eficaz do Direito.

2.1 A evolução tecnológica e o surgimento dos Deepfakes

A sociedade passa por constantes transformações e, desde os primórdios, evidencia a necessidade de interação comunicativa e do uso de gestos para a compreensão humana. Ao longo dos séculos, esse processo consolidou-se como um percurso de transformação contínua: as antigas trocas comerciais foram gradualmente estruturadas em relações mais complexas, posteriormente substituídas por mecanismos bancários e outros instrumentos que acompanharam a evolução das relações econômicas.

Apesar das transformações sociais e tecnológicas, a comunicação permanece como elemento essencial. Gestos e palavras foram progressivamente acrescentados por tecnologias como aparelhos celulares e redes sociais. Em decorrência disso, observa-se constante busca por atualização tecnológica, com o objetivo de facilitar o cotidiano e proporcionar maior agilidade às atividades humanas. Nesse contexto, a inteligência artificial surge como resposta à necessidade de otimização de processos, caracterizando-se pela praticidade, acessibilidade e ampla aplicabilidade.

Em relação aos *deepfakes*, estes consistem em técnicas de *machine learning*[4] e deep learning[5], alimentadas pelo treinamento de algoritmos em extensas bases de dados compostas por imagens, gravações de voz e registros audiovisuais. Nesse processo, o reconhecimento de padrões faciais, vocais e comportamentais pode ser reproduzido artificialmente, permitindo a simulação de personagens fictícios e indivíduos reais com elevado grau de verossimilhança. Anteriormente, as montagens digitais eram limitadas a edições simples realizadas em softwares como o Photoshop, restritas à manipulação estática de imagens. Contudo, os *deepfakes* apresentam nível significativamente superior de sofisticação, ao possibilitar a criação de simulações dinâmicas e realistas, baseadas em dados reais, o que amplia sua capacidade persuasiva, especialmente em situações nas quais a vítima mantém relação de confiança com a pessoa imitada.

Conforme Peck (2021), a identidade digital passou a representar uma verdadeira extensão da personalidade humana, reunindo reputação, presença social e histórico informacional. Por essa razão, sua manipulação indevida pode ocasionar danos morais,

[4] Técnica amplamente utilizada em sistemas de algoritmos capazes de identificar padrões em dados e aprimorar o desempenho, sem necessidade explícita de programar essa tarefa.

[5] Subárea do *Machine Learning* que simula a atividade do funcionamento do cérebro humano para aprimorar a capacidade de aprendizagem das máquinas.

patrimoniais e reputacionais relevantes. Sob a perspectiva técnica, os *deepfakes* não exigem elevado conhecimento técnico, pois se baseiam em plataformas automatizadas com interfaces simplificadas e modelos pré-estruturados, o que democratiza o acesso à tecnologia e amplia seu potencial de uso abusivo, demonstrando certa fragilidade. A partir de 2020, observou-se a expansão significativa dessa tecnologia, impulsionada pelo acesso público a softwares de edição baseados em inteligência artificial, especialmente no contexto da pandemia. Nesse período, seus usos ainda apresentavam caráter experimental e menor grau de realismo, permitindo a produção de manipulações convincentes em curto espaço de tempo com o intuito de entretenimento.

O impacto dessa evolução foi diretamente sentido na segurança das comunicações digitais em âmbito global. O que antes demandava estúdios especializados e altos investimentos passou a ser executado em dispositivos eletrônicos domésticos, facilitando a disseminação em larga escala de desinformação. Diretrizes do Ministério da Justiça e Segurança Pública (BRASIL, 2023) apontam que os *deepfakes* passaram a ser amplamente utilizados na prática de fraudes e crimes cibernéticos relacionados à falsa identidade.

Portanto, constata-se que a velocidade do avanço tecnológico superou a capacidade de resposta das estruturas institucionais tradicionais. O Direito Penal, historicamente voltado a falsificações documentais físicas e estáticas, passou a enfrentar mídias digitais dinâmicas que desafiam a percepção humana e os mecanismos tradicionais de prova.

2.2 Mecanismos de engenharia social com *Deepfakes*

A engenharia social consiste na indução da vítima ao erro por meio de manipulação psicológica, levando-a à prática de determinados atos em benefício do sujeito fraudador. Seu emprego associado aos *deepfakes* representa uma evolução dos métodos tradicionais de fraude, na medida em que não se limita à exploração de falhas técnicas de sistemas, mas à instrumentalização das vulnerabilidades humanas, como confiança, medo, urgência, expectativa financeira e desconhecimento informacional. Marques (2024) já enfatizava que a exploração da boa-fé e da confiança constitui a base da engenharia social no estelionato contemporâneo, premissa que alcança nível de complexidade ainda maior com o uso da inteligência artificial.

Os *deepfakes* potencializam e atualizam a engenharia social ao explorarem a fragilidade humana baseada na confiança, agregando aparência visual e sonora de autenticidade à narrativa

falsa. A criação de uma identidade convincente, somada à utilização de documentos adulterados ou simulações de voz e imagem, tende a reduzir significativamente as barreiras naturais de desconfiança. É fácil de acreditar quando se possui dados relevantes. Castells (2021) sustenta que a sociedade em rede deslocou parte substancial das relações de confiança para ambientes digitais. Assim, quando a confiança migra para plataformas tecnológicas, também migram os mecanismos de fraude.

No caso do popularmente conhecido golpe do "falso advogado", a utilização de dados pessoais da vítima e da imagem profissional do advogado é suficiente para induzir a vítima ao erro, ainda que as solicitações financeiras ultrapassem padrões usuais de verificação de legitimidade.

A eficácia desses golpes decorre da subversão da percepção sensorial da vítima. Diferentemente de e-mails fraudulentos tradicionais, que dependem de processo de convencimento e múltiplas interações, como falsas ameaças de exposição de dados pessoais ou solicitações de resgate financeiro em criptomoedas, os *deepfakes* permitem interações síncronas altamente realistas, simulando voz, imagem e comportamento em tempo real. Isso reduz significativamente o tempo de reação e compromete a capacidade de discernimento da vítima diante de situações de urgência artificialmente construídas pelos fraudadores.

As empresas de segurança digital têm buscado acompanhar esse avanço por meio da criação de filtros e mecanismos de detecção; contudo, o fator humano permanece como o elo mais vulnerável da cadeia. Sobral e Bezerra lecionam:

> A impunidade no mundo virtual muito se dá a problemas nas legislações existentes, como a falta de previsão legal para a tipificação do delito e a ausência de cooperação penal e processual entre estados soberanos. A soberania que antes era a proteção de um estado passou a ser aliada dos cibercriminosos para a garantia de sua impunidade. (SOBRAL; BEZERRA, 2015, p. 14).

A sofisticação técnica dessas fraudes desafia diretamente os métodos tradicionais de verificação de identidade, ultrapassando a esfera tecnológica, exigindo o desenvolvimento de novas camadas de proteção biométrica e comportamental. No campo jurídico, essa realidade evidencia que os *deepfakes* não apenas falsificam conteúdos, mas instrumentalizam relações sociais previamente existentes, o que potencializa sua eficácia e execução.

2.3 Vulnerabilidade digital e impacto social

A proliferação de *deepfakes* em fraudes envolvendo a identidade de advogados repercute diretamente sobre os direitos da personalidade, especificamente no que tange à honra, imagem

e reputação profissional. Tais direitos, constitucionalmente protegidos, integram o núcleo da dignidade da pessoa humana e possuem significa pertinência no exercício da advocacia, visto que é uma atividade que depende da credibilidade perante clientes e instituições. Logo, a violação da identidade profissional não se limita tão somente a um dano individual, mas atinge também a confiança depositada na função social exercida pelo advogado no sistema de justiça.

O uso indevido dessa tecnologia retoma o impacto potencializado pela capacidade de simular feições realísticas do advogado. Tal exposição não compromete apenas a sua imagem, mas também a percepção da vítima. Conforme leciona Doneda (2019), os dados pessoais e os elementos informacionais da identidade do indivíduo integram a própria esfera da personalidade, assim, sua utilização inadequada no ambiente digital pode acarretar violações diretas à dignidade e à autonomia da pessoa humana.

No campo da advocacia, compreende-se que a confiança constitui elemento estrutural da relação advogado-cliente, bem como fator que viabiliza o acesso do cidadão ao sistema de justiça, aproximando-o da efetivação de seus direitos. Em muitos casos, a ausência de informação ou o receio em relação ao funcionamento do sistema jurídico faz com que indivíduos deixem de buscar a tutela jurisdicional. Nesse cenário, a atuação do advogado exerce papel fundamental na concretização do acesso à justiça.

Quando ocorre um ato fraudulento envolvendo a falsa identidade profissional, há comprometimento da integridade dessa relação, podendo gerar descrédito profissional, ainda que a fraude seja posteriormente desmentida. Além disso, tal situação pode impactar diretamente a atuação do próprio advogado, afetando sua imagem, a relação com o cliente e a confidencialidade de informações processuais. Trata-se, portanto, de um dano que ultrapassa a esfera patrimonial, alcançando dimensões existenciais e profissionais.

Diante disso, entende-se que a disseminação de *deepfakes* aplicados à falsa identidade de advogados evidencia um risco estrutural à confiança social no ambiente jurídico-digital, exigindo o aprimoramento dos mecanismos de proteção aos direitos da personalidade e ao exercício profissional. A preservação da validação institucional do sistema de justiça depende, nesse contexto, não apenas de respostas penais adequadas, mas também de medidas preventivas e educativas voltadas à segurança digital.

Então, a atuação coordenada entre instituições jurídicas, profissionais da advocacia e usuários do sistema de justiça mostra-se essencial, especialmente por meio da capacitação contínua de advogados, da conscientização digital de clientes e do fortalecimento de políticas

institucionais de proteção informacional. Embora não se restrinja ao Estado, é papel das instituições públicas promover políticas de educação digital e incentivo à segurança informacional, considerando que a vulnerabilidade decorre, em parte, da falta de orientação adequada dos usuários no ambiente digital.

3 DEEPFAKES NO DIREITO PENAL: TIPICIDADE, RESPONSABILIZAÇÃO E LACUNAS NORMATIVAS

Ao se analisar os crimes cibernéticos no âmbito penal, observa-se que não se trata necessariamente da criação de novos tipos penais, mas sim da intensificação e sofisticação de condutas já previstas no ordenamento jurídico. Nessa perspectiva, a inteligência artificial atua como meio executório complexo, utilizado para potencializar fraudes por meio da simulação de identidade e utilização indevida de dados pessoais.

Em muitos casos, o agente se vale de comunicações digitais aparentemente autênticas, como solicitações de pagamento vinculadas a supostos alvarás ou liberações judiciais, com o objetivo de induzir a vítima ao erro e obter vantagem ilícita. Visto isso, torna-se necessário analisar a adequação dos tipos penais vigentes às fraudes praticadas por meio de simulação audiovisual e comunicação digital aparentemente autêntica, bem como os limites da responsabilização penal nessas hipóteses. Além disso, evidencia-se a necessidade de constante atualização normativa, tendo em vista a defasagem de respostas jurídicas específicas para condutas praticadas no ambiente digital.

3.1 Aplicação do Estelionato (art. 171, CP) aos *Deepfakes*

Disposto no ordenamento jurídico, o crime de estelionato, previsto no art. 171 do Código Penal, consiste em:

> Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento. Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis. (BRASIL, 1940).

Portanto, trata-se de um delito no qual a fraude constitui elemento apto a induzir a vítima em erro para obter uma vantagem. Greco (2023) discorre que o estelionato exige a presença de um meio fraudulento idôneo a induzir a vítima em erro, sendo o engano elemento estruturante do tipo penal. Sob essa ótica, os *deepfakes* podem ser entendidos como meio contemporâneo de execução do delito, uma vez que funcionam como instrumento tecnológico de simulação de identidade, voz e imagem. Nucci (2020) também leciona sobre,

compreendendo o estelionato como um delito que admite diversas formas de execução, desde que presentes o engano e a obtenção de vantagem ilícita, sendo irrelevante o meio empregado para sua consumação.

Com isso, o art. 171 também abrange formas qualificadas de fraude. A legislação passou a prever a hipótese de fraudes cometidas pelo ambiente virtual:

> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (BRASIL, 2021).

Apesar dessa ampliação normativa, ainda subsistem desafios interpretativos diante do uso de *deepfakes* e de outras formas de inteligência artificial generativa. O dispositivo trata de fraudes em ambiente digital, contudo, não discute expressamente a simulação audiovisual hiper-realista, a dificuldade de identificação do autor em contextos automatizados, nem aspectos relacionados à autenticidade da prova digital.

3.2 Adequação típica ao crime de Falsa Identidade (ART. 307, CP)

A prática delituosa de usurpação de identidade mediante o uso de *deepfakes* encontra sustento normativo nas disposições do art. 307 do Código Penal brasileiro, que dispõe:

> Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem: Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave. (BRASIL, 1940).

A identidade pode ser compreendida como o agrupamento de características que individualizam a pessoa, sendo que o referido tipo penal tutela a fé pública, especialmente no que se refere à veracidade da identificação pessoal nas relações sociais e jurídicas. A simulação de advogados, autoridades ou terceiros por meio de inteligência artificial pode configurar a conduta típica prevista no art. 307 do Código Penal.

O Superior Tribunal de Justiça já consolidou entendimento de que o crime de falsa identidade se consuma no momento da atribuição da identidade falsa, sendo irrelevante a ocorrência de prejuízo ou a efetiva obtenção de vantagem. Conforme destacado pelo Ministro Joel llan Paciornik no julgamento do REsp 2.083.968 (BRASIL, 2025), entendeu-se que:

> A consumação delitiva ocorre assim que o agente inculca a si ou a outrem a falsa identidade, sendo irrelevantes a causação de prejuízo ou a obtenção de efetiva vantagem pelo agente, bem como a posterior verificação da Real identidade do indivíduo. (BRASIL, 2025)

Logo, a adequação do art. 307 aos casos envolvendo *deepfakes* suscita debates quanto aos limites entre a falsa identidade tradicional e a utilização de identidade sintética altamente sofisticada. Em determinadas situações, a falsa identidade pode funcionar em concurso com outros delitos, como o estelionato, o que exige análise conjunta dos tipos penais para correta subsunção da conduta.

3.3 Lacunas normativas e a necessidade de regulamentação específica

Diante do exposto, é importante destacar que o ordenamento jurídico atual ainda não oferece resposta normativa específica para fraudes com o uso de *deepfakes*, principalmente quando essas condutas envolvem simulação de identidade profissional no meio digital. Diante disso, o Projeto de Lei n.º 2.338/2023 representa um avanço relevante ao buscar tipificar a criação e a divulgação dolosa e prejudicial de conteúdos sintéticos no país. A proposta legislativa procura aproximar a legislação brasileira dos marcos regulatórios já observados em países como Estados Unidos e União Europeia. Contudo, constata-se que ainda se encontra em tramitação, sem consolidar parâmetros normativos aplicáveis de forma imediata à repressão dessas condutas. Assim, embora seja possível o enquadramento em tipos penais já existentes, trata-se de construção interpretativa, sem previsão legal específica para a inteligência artificial generativa.

No que tange à advocacia, esse cenário revela uma vulnerabilidade diante da utilização indevida da identidade profissional de advogados, assim como de dados pessoais e informações processuais de clientes, como meio de indução ao pagamento de valores indevidos. Tal prática ultrapassa a esfera patrimonial, alcançando impactos psicológicos e reputacionais, além de comprometer a confiança que sustenta a relação advogado-cliente e, por consequência, a credibilidade do sistema de justiça. A ausência de normas específicas adequadas à realidade tecnológica contemporânea dificulta a atuação uniforme dos órgãos de persecução penal e contribui para a insegurança jurídica, especialmente na prevenção e repressão desses golpes. Nesse contexto, destaca-se a necessidade de mecanismos normativos mais claros de proteção à identidade profissional, aliados ao fortalecimento institucional das estruturas de investigação e resposta aos crimes cibernéticos.

Conforme leciona Nucci (2020), a interpretação dos tipos penais deve acompanhar a evolução social, sob pena de comprometimento da efetividade da tutela penal, o que se torna ainda mais evidente diante da rápida sofisticação da criminalidade digital. De forma

semelhante, Greco (2023) destaca que o avanço tecnológico exige constante atualização interpretativa do Direito Penal, especialmente quando novas ferramentas ampliam a capacidade de engano e lesão aos bens jurídicos tutelados.

Paralelamente, a atuação dos órgãos institucionais ainda carece de fortalecimento estrutural e capacitação técnica voltada aos crimes cibernéticos, considerando a natureza dinâmica e transnacional dessas condutas. A identificação da autoria, a rastreabilidade de conteúdos sintéticos e a preservação da cadeia de custódia digital permanecem como desafios relevantes, impactando diretamente a efetividade da persecução penal.

Dessa forma, a principal lacuna não se limita à ausência de tipos penais específicos, mas envolve a insuficiência de um regime jurídico integrado que contemple prevenção, responsabilização, produção de prova digital e proteção da confiança nas relações profissionais.

4 DESAFIOS PROBATÓRIOS E SEGURANÇA DIGITAL NA ADVOCACIA

Na contemporaneidade, marcada pelo desenvolvimento sofisticado das interações digitais e pelo avanço de sistemas baseados em inteligência artificial, observa-se não apenas a ampliação das facilidades tecnológicas, mas também o surgimento de novas formas de prática delituosa. Ferramentas desenvolvidas para otimizar a comunicação e automatizar respostas passaram a ser instrumentalizadas para a aplicação de golpes cada vez mais realistas. Nesse contexto, fragilidades relacionadas ao armazenamento de dados e aos meios de autenticação contribuem para a expansão de fraudes, especialmente em ambientes digitais altamente dinâmicos. Dessa forma, nascem barreiras importantes relacionados à atribuição de autoria, à preservação da prova digital e à segurança informacional da advocacia, exigindo respostas jurídicas e preventivas compatíveis com a complexidade dos crimes cibernéticos contemporâneos.

4.1 Dificuldades de atribuição de autoria nos crimes com *deepfakes*

No contexto dos crimes cibernéticos contemporâneos, um dos principais entraves à persecução penal reside na dificuldade de atribuição de autoria. Para além das fragilidades relacionadas à autenticação de segurança, a identificação do agente responsável torna-se particularmente complexa em delitos como o estelionato praticado em ambiente digital, muitas vezes intermediado por dispositivos informáticos e variados canais de comunicação.

A dinâmica desses crimes evidencia o uso de ferramentas que complicam o rastreamento. Linhas telefônicas podem ser habilitadas com cadastros mínimos ou mediante uso indevido de dados de terceiros, permitindo que números sejam ativados em localidades distintas daquela em que reside a vítima. De forma semelhante, contas bancárias são frequentemente utilizadas de maneira fragmentada, com a participação de terceiros que atuam como intermediários na recepção e transferência de valores.

Soma-se a isso o uso de recursos tecnológicos voltados à ocultação de identidade, como redes privadas virtuais (VPNs) e a utilização de diferentes provedores de conexão, que dificultam a localização precisa dos agentes. Nesse sentido, a Academia Nacional de Polícia, citada por Sobral e Bezerra (2015), destaca:

> A internet é um local de crime real e, portanto, deixa vestígios como registros de conexão à internet, registros de utilização de serviços na internet, envio e recebimento de e-mails, registros de trocas de mensagens, download de arquivos, além dos próprios computadores utilizados para a prática criminosa. (SOBRAL; BEZERRA, 2015, p. 20).

No âmbito dos meios de pagamento, observa-se ainda a utilização de chaves PIX descartáveis ou a identificadores de difícil rastreabilidade, como endereços de e-mail criados exclusivamente para a prática delituosa. Em determinados casos, os criminosos induzem as vítimas à instalação de aplicativos de acesso remoto, como o AnyDesk, o que lhes permite operar diretamente no dispositivo da vítima, ampliando o controle sobre transações e dados sensíveis, em muitos casos, danificando as provas.

Esse conjunto de estratégias demonstra a participação organizada dos criminosos, que ativamente partilham funções, coletam dados prévios sobre as vítimas e constroem abordagens planejadas, utilizando a linguagem jurídica que, em alguns casos, torna o fato com aparência legítima. A investigação dessas operações exige a adoção de medidas judiciais para acesso amplo aos dados bancários e telemáticos, o que, aliado ao elevado volume de demandas no sistema judiciário, pode impactar o tempo de resposta das diligências e prolongar.

No que diz respeito à divergência de informações locacionais, Peck (2021) discorre que, a circulação intensiva de dados no ambiente digital, ainda que para fins lícitos, traz impactos visíveis nas noções tradicionais de territorialidade e identificação, exigindo o desenvolvimento de métodos investigativos compatíveis com a Era da Informação, bem como o fortalecimento de mecanismos de cooperação institucional.

Tal problemática pode ser evidenciada na chamada “Operação Attornatus Falsus”, deflagrada pela Polícia Civil do Amazonas em conjunto com a Polícia Civil do Ceará, que

desarticulou organização criminosa responsável por fraudes eletrônicas envolvendo falsos alvarás judiciais. As diligências apontam que o grupo atuava de forma interestadual, utilizando dados reais de processos judiciais para aplicar golpes, com vítimas localizadas em uma unidade federativa e agentes operando em outras diferentes, além da utilização de contas bancárias diversas para recebimento e posterior lavagem de valores.

4.2 Limitações da prova digital no processo judicial

A prova digital assume um papel central na elucidação de fatos em investigações que se desenvolvem especificamente no campo digital. Em alternância dos crimes tradicionais, cuja materialidade pode estar associada a elementos físicos, como o corpo e o instrumento do delito, os crimes cibernéticos produzem vestígios intangíveis, dependentes de registros eletrônicos e dados armazenados por terceiros.

Após a ocorrência do fato, a vítima apresenta elementos como capturas de tela de conversas, comprovantes de transferências bancárias, chaves PIX, números telefônicos utilizados, áudios e registros de chamadas. E mesmo que tais elementos sejam relevantes para reconstruir a ordem cronológica do fato, especialmente quanto ao dia e horário do início da interação, eles nem sempre são suficientes, de forma isolada, para comprovar a autoria ou garantir a integridade da prova.

Isso se deve, em parte, à própria natureza dos documentos digitais, que são passíveis de alteração, edição ou manipulação, outro ponto que deve destacar. Existem ferramentas acessíveis que permitem modificar imagens, vídeos e áudios com facilidade, o que compromete a confiabilidade de provas apresentadas sem respaldo técnico. Logo, uma simples captura de tela, desacompanhada de elementos que assegurem sua autenticidade e integridade, pode não atender aos requisitos necessários para sua validação judicial, além de prejudicar a preservação da cadeia de custódia.

Sob essa ótica, cumpre-se essencial importância quanto à forma de coleta, preservação e apresentação da prova digital. A cadeia de custódia, compreendida como o conjunto de evidências que buscam evitar que as provas sejam anuladas e que visa garantir a integridade desde sua obtenção até sua apresentação no tribunal, é frequentemente comprometida pela falta de conhecimento técnico, especialmente por parte das vítimas.

Além disso, o tempo de preservação exerce papel significativo. Crimes digitais caracterizam-se pela rápida execução e pela célere dissipação de vestígios. Medidas como o

bloqueio de valores, rastreamento de contas e obtenção de registros de conexão dependem de atuação imediata. Nos termos do Marco Civil da Internet, os provedores de conexão são obrigados a manter os registros por, no mínimo, um ano, enquanto provedores de aplicações podem ser obrigados a armazenar registros de acesso por seis meses. Após esses prazos, a recuperação de dados pode se tornar dificultosa, demonstrando a necessidade de agir rapidamente após a consciência de que se consumou um golpe.

Outro ponto relevante diz respeito à percepção ainda limitada, em parte dos operadores do Direito, quanto a relevância da prova digital. Em alguns casos, esses elementos são tratados como acessórios ou de menor importância em relação às provas tradicionais, o que não corresponde à realidade dos crimes na Era da Informação. Essa compreensão minimizada pode comprometer a análise adequada do caso, gerar insegurança jurídica e, eventualmente, resultar em nulidades processuais.

Ainda no contexto, podemos destacar também a proposta do Projeto de Lei nº 4.939/2020, que busca aprimorar dinâmicas voltadas à investigação e responsabilização em crimes praticados no âmbito digital, incluindo o uso de tecnologias como *deepfakes*. A iniciativa demonstra a preocupação do legislador em adaptar o ordenamento jurídico aos novos acontecimentos tecnológicos, ressaltando a necessidade de instrumentos mais eficazes para a coleta, preservação e validação da prova digital.

4.3 Segurança digital do advogado e proteção do sigilo profissional

A segurança digital do advogado é uma atuação marcante e substancial, especialmente nesta margem da crescente incidência de fraudes que exploram dados sensíveis e a própria imagem profissional da advocacia. O sigilo profissional, alicerce no relacionamento do advogado com seu cliente, enfrenta riscos decorrentes dessa manipulação de informações. Ao falarmos de proteção de dados, não se trata somente de uma obrigação ética exposta no Estatuto dos Advogados, mas sim um dever estratégico de prevenção contra essas condutas delituosas.

O uso indevido de informações extraídas de processos judiciais exalta uma delicadeza estrutural relevante e que está em constante debate quanto aos meios de proteção. Os dados contidos que, em tese, deveriam servir à transparência e ao acesso à justiça, se tornam instrumentos de criminosos para aplicações de golpes, gerando o conhecido “golpe dos advogados”, que trazem debates sobre confidencialidade e a fragilidade do jurídico.

Ao se analisar a posição do advogado nesse contexto, verifica-se que ele pode figurar como vítima indireta e, simultaneamente, como instrumento involuntário na execução do golpe. Isso ocorre porque sua imagem profissional, associada à credibilidade, à confiança e ao manejo de informações sensíveis, é explorada por agentes criminosos para conferir legitimidade às fraudes

Como preleciona Marques (2025), agora, as redes sociais são métodos substanciais para a visibilidade e ampliação de conexões profissionais para advogados. Todavia, essa mesma visibilidade pode gerar vulnerabilidades. A exposição de rotinas profissionais, ainda que de forma não intencional, cria oportunidades para que agentes mal-intencionados construam narrativas fraudulentas mais convincentes, utilizando tais informações como ponto de partida para a aplicação de golpes.

Nessa conjuntura, destaca-se o Projeto de Lei (PL) 4.709/2025, aprovada pela Câmara dos Deputados em 17 de março de 2026 e que dispõe significantemente sobre meios de repressão e prevenção ao "golpe do falso advogado" e derivantes de fraudes processuais, representando um avanço na tutela da segurança jurídica no campo digital. O texto aprovado ressalta que as condutas de criminosos que venham a utilizar da imagem do advogado para a obtenção de vantagem ilícita, mediante ao uso indevido de dados processuais, venha a ser tratada de forma específica, com tipificação penal própria. Essa aprovação também engloba a proteção do sigilo profissional, preservando a integridade dos dados compartilhados no exercício da advocacia, reforçando a necessidade de mecanismos de controle de acesso do uso de informações processuais e suas plataformas.

Simultaneamente, cabe ao advogado a adoção de práticas preventivas e protetivas voltadas à tríade informacional: segurança digital, segurança da informação e segurança processual. É preciso continuidade no gerenciamento seguro de dados, a verificação rigorosa de comunicações recebidas e enviadas, e a conscientização dos riscos do uso de equipamento digital.

4.4 Medidas preventivas para escritórios e profissionais da advocacia

A recorrência progressiva de crimes cibernéticos envolvendo a imagem e a atuação de advogados suscita um questionamento central: como prevenir tais delitos em um ambiente marcado pela constante evolução tecnológica? Embora não seja possível erradicar integralmente tais condutas, é possível adotar medidas capazes de mitigá-las.

Diante desse panorama, é importante ressaltar a diferença de consciência digital e educação digital. A primeira refere-se ao discernimento crítico do sujeito em relação dos impactos de suas ações no ambiente digital, envolvendo aspectos éticos e comportamentais; a segunda diz respeito ao domínio de habilidades técnicas necessárias para a utilização segura das ferramentas digitais, essas que aprendemos quando possuímos um dispositivo informático em mãos, mesmo que aos poucos. Ambas, quando combinadas, contribuem significativamente para a redução de riscos.

Cumpre salientar que a prevenção aos crimes cibernéticos não pode ser atribuída exclusivamente à sociedade. Trata-se de uma responsabilidade compartilhada, que envolve instituições privadas, órgãos de segurança pública, entidades de classe e o próprio Estado. Nesse atual cenário, conforme leciona Patrícia Peck Pinheiro (2021), para a atuação da segurança da informação, são necessárias transformações socioculturais, assim como a adoção de hábitos seguros pelos usuários, não havendo dependência exclusiva de soluções tecnológicas. Sobral e Bezerra complementam:

> Necessitamos interpretar e ajustar nossas legislações para aplicarmos a essa realidade, pois os conflitos neste novo cenário já se fazem presentes e possuem características não pensadas em nossa realidade pretérita. Tipos penais, locais de crime, assim como jurisdição e competência de juízos precisam ser interpretados sob novos princípios de Direito. (SOBRAL; BEZERRA, 2015, p. 20).

No que tange o campo da advocacia, isso exalta mudanças em rotinas internas em protocolos estruturados de proteção de dados. Sob uma perspectiva sociológica, Castells (2021) sustenta que a velocidade de circulação da informação na sociedade em rede supera a capacidade humana de verificação imediata, o que amplia a fragilidade a fraudes. Tal observação enfatiza a necessidade de fortalecimento da segurança informacional e da construção de uma cultura de verificação contínua.

No plano prático, a adoção de medidas preventivas por escritórios e profissionais da advocacia revela-se essencial para mitigar golpes. Entre os principais métodos de segurança, destacam-se a implementação de autenticação em dois fatores em sistemas e canais de comunicação, a separação entre perfis pessoais e profissionais de atendimento e a verificação da autenticidade de perfis, principalmente em contas comerciais recentes ou com baixa rastreabilidade, assim como a atenção a insistências e solicitações financeiras incomuns. Ademais, mostra-se imprescindível a confirmação de solicitações financeiras por múltiplos meios de contato, bem como a restrição de acesso interno a documentos sensíveis, mediante controle de permissões, além da atenção a dados bancários suspeitos. Também se revela

indispensável a atualização constante de sistemas e softwares utilizados, a realização periódica de backups seguros e a divulgação contínua, por canais oficiais do escritório, de alertas sobre golpes. Outrossim, é recomendável que o advogado atue de forma ativa e constante na orientação de seus clientes, informando-os sobre práticas seguras de comunicação e procedimentos legais para solicitações financeiras, reduzindo, então, a margem de sucesso de abordagens fraudulentas e fornecendo conhecimento digital.

No âmbito institucional, a Ordem dos Advogados do Brasil desempenha uma atuação importante na proteção de sua classe. É imprescindível que a entidade invista em ambientes digitais seguros, promova campanhas educativas e disponibilize canais eficazes de atendimento para denúncias, com suporte técnico qualificado e articulação institucional voltada ao enfrentamento desses delitos.

Paralelamente, o Estado deve fortalecer sua atuação por meio da ampliação e capacitação de unidades especializadas em crimes cibernéticos, garantindo infraestrutura adequada, formação constante de seus servidores e integração entre órgãos. Iniciativas de conscientização pública também são indispensáveis para a prevenção.

Por fim, destaca-se que o enfrentamento dessas fraudes não se limita à repressão penal posterior, condiciona-se, sobretudo, na inibição dos fatores para sua ocorrência. Quanto maior o nível de conhecimento e mais extenso os meios de informações para com os clientes acerca do funcionamento dos serviços jurídicos e dos canais legítimos de comunicação, menor tende a ser a eficácia dos golpes. Assim, a combinação entre conhecimento, prevenção e cooperação institucional constitui elemento essencial para a mitigação dos riscos no ambiente digital.

5. CONSIDERAÇÕES FINAIS

A pesquisa demonstrou que os *deepfakes* ampliaram significativamente o potencial lesivo das fraudes digitais, especialmente nos casos envolvendo falsa identidade profissional de advogados. A utilização de recursos tecnológicos de manipulação sintética, somada a práticas de engenharia social, potencializa a percepção das vítimas e aumenta a incidência de fraudes patrimoniais praticadas no ambiente digital.

Constatou-se que, embora o ordenamento jurídico brasileiro possua instrumentos pertinentes para a repressão dessas condutas, especialmente por meio dos crimes de estelionato e falsa identidade previstos no Código Penal, ainda persistem limitações relacionadas à investigação, à atribuição de autoria e à preservação da prova digital.

Além disso, verificou-se que a ausência de regulamentação específica voltada à inteligência artificial e aos *deepfakes* contribui para a insegurança jurídica e para dificuldades na responsabilização penal dos agentes envolvidos. A insuficiência estrutural de órgãos especializados em crimes cibernéticos e a limitada educação digital da população também favorecem a expansão dessas práticas ilícitas.

O enfrentamento eficaz dos crimes intermediados por *deepfakes* exige abordagem integrada entre atualização legislativa, fortalecimento da perícia digital, investimento em capacitação técnica de autoridades públicas e implementação de políticas preventivas de conscientização social nos meios telemáticos.

No campo da advocacia, revela-se indispensável a adoção de medidas de segurança digital, autenticação de comunicações e proteção de dados profissionais, a fim de reduzir riscos de usurpação de identidade e utilização indevida de informações processuais.

Por fim, a pesquisa reafirma que a proteção da dignidade humana, da confiança nas relações digitais e da segurança jurídica depende da capacidade do Direito de acompanhar as constantes transformações tecnológicas. O debate sobre *deepfakes* e inteligência artificial não se limita à esfera tecnológica, mas representa tema essencial para a preservação da integridade informacional, da atividade profissional e da efetividade da tutela penal no ambiente virtual.

REFERÊNCIAS

AMAZONAS. Secretaria de Segurança Pública. *Operação Attornatus Falsus: PC-AM e PCCE desarticulam organização criminosa envolvida com falsos alvarás. Manaus*: SSP, 26 nov. 2024. Disponível em: https://www.ssp.am.gov.br/operacao-attornatus-falsus-pc-am-e-pcce-desarticulam-organizacao-criminosa-envolvida-com-falsos-alvaras/. Acesso em: 2 maio 2026.

BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso. *Combate ao Crime Cibernético: doutrina e prática*. 1. ed. Rio de Janeiro: Mallet Editora, 2020.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 4.939/2020. Dispõe sobre medidas de combate a fraudes eletrônicas e utilização indevida da identidade de advogados*. Brasília, DF: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2264367. Acesso em: 24 abr. 2026.

BRASIL. Congresso Nacional. *Decreto-Lei n.º 2.848, de 7 de dezembro de 1940*. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 03 mar. 2026.

BRASIL. Congresso Nacional. *Lei nº 14.155, de 27 de maio de 2021. Altera o Código Penal para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet*. Diário Oficial da União: seção 1, Brasília, DF, p. 3, 28 maio 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 24 abr. 2026.

BRASIL. Senado Federal. *Projeto de Lei n.º 2.338, de 2023. Dispõe sobre o uso de inteligência artificial e cria tipos penais relacionados à manipulação digital*. Brasília, DF: Senado Federal, 2023. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9915448&disposition=inline. Acesso em: 24 abr. 2026.

BRASIL. Superior Tribunal de Justiça. *Crime de falsa identidade não exige obtenção de vantagem e se consuma no ato de fornecer dado incorreto*. Brasília, DF: STJ, 17 jun. 2025. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2025/17062025-Crime-de-falsa-identidade-nao-exige-obtencao-de-vantagem-e-se-consuma-no-ato-de-fornecer-dado-incorreto.aspx. Acesso em: 17 abr. 2026.

CASTELLS, Manuel. *A sociedade em rede*. 25. Ed. São Paulo: Paz e Terra, 2021.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. Ed. São Paulo: Revista dos Tribunais, 2019.

FIDELIS, Vanderson Cadete; SOARES, Douglas Verbicaro. *Os desafios do ordenamento jurídico brasileiro frente às deepfakes*. Revista Pensamento Jurídico, São Paulo, v. 17, n. 1, 2023. Disponível em: https://ojs.unialfa.com.br/index.php/pensamentojuridico/article/view/711. Acesso em: 24 abr. 2026.

GRECO, Rogério. *Código Penal comentado*. 22. Ed. Rio de Janeiro: Impetus, 2023.

MARQUES NETO, Paulo. *Desmascarando o falso advogado: como proteger seu escritório de golpes: as lições cruciais que aprendi após passar por quatro experiências*. 1. Ed. São Paulo: Autor, 2025.

NUCCI, Guilherme de Souza. *Manual de direito penal: volume único*. 16. Ed. Rio de Janeiro: Forense, 2020.

OLIVEIRA, Giovanna Aleixo Gonçalves; ÁVILA, Gustavo Noronha de. *Deepfake, direitos da personalidade e o direito penal: uma análise dos impactos tecnológicos na era digital*. Revista Eletrônica do Curso de Direito da UFSM, Santa Maria, v. 19, e85239, 2024. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/85239. Acesso em: 01 abr. 2026.

PINHEIRO, Patrícia Peck. *Direito digital*. 7. Ed. São Paulo: Saraiva Educação, 2021.

POLÍCIA CIVIL DO AMAZONAS. *Cartilha DERCC 2024*. Manaus, AM, 2024. Disponível em: https://www.policiacivil.am.gov.br/wp-content/uploads/2024/09/Cartilha-Dercc-2024-1.pdf. Acesso em: 02 fev. 2026.