

O TIPO PENAL DE ESTELIONATO DIANTE DAS FRAUDES MEDIADAS POR INTELIGÊNCIA ARTIFICIAL

THE CRIMINAL OFFENSE OF FRAUD IN THE FACE OF ARTIFICIAL
INTELLIGENCE-MEDIATED FRAUDS

Ciências Sociais Aplicadas • 11/10/2026

REGISTRO DOI: [10.70773/revistatopicos/791606381](https://doi.org/10.70773/revistatopicos/791606381)

Danilo Aguiar Quadros Gramosa¹

Eliel Gustavo de Araújo Silva²

Gustavo Luís Mendes Tupinambá Rodrigues³

RESUMO

Este artigo tem como objetivo analisar se o tipo penal de estelionato, previsto no art. 171 do Código Penal Brasileiro, é dogmaticamente suficiente para abarcar as fraudes patrimoniais mediadas por Inteligência Artificial (IA), especialmente aquelas praticadas por meio de *deepfakes*, clonagem de voz e outras técnicas de manipulação digital. Parte-se da premissa de que a estrutura típica do estelionato, concebida para fraudes analógicas, pode apresentar dificuldades para abranger, sem complementação legislativa, o maior grau de sofisticação e potencial lesivo dessas novas modalidades de engano. Para tanto, examinam-se os elementos estruturais do art. 171, caput, e da qualificadora de fraude eletrônica prevista no §2º-A, confrontando-os com as características das fraudes mediadas por IA, além de se analisarem criticamente as tendências legislativas nacionais e internacionais voltadas à tipificação específica de fraudes tecnológicas. A pesquisa é de natureza qualitativa, bibliográfica e documental, valendo-se do método dedutivo. Os resultados indicam que, embora o tipo penal de estelionato seja estruturalmente apto a alcançar, em regra, as fraudes praticadas com uso de IA, sua maior sofisticação e capacidade de indução a erro justificam a inserção de uma causa de aumento de pena específica, seja como acréscimo ao §2º-A, seja como qualificadora autônoma, de modo a assegurar maior segurança jurídica e proporcionalidade na resposta penal.

Palavras-chave: Estelionato; Inteligência Artificial; Fraude eletrônica; Direito Penal Digital; Código Penal.

ABSTRACT

This article aims to analyze whether the criminal offense of fraud (estelionato), provided for in Article 171 of the Brazilian Penal Code, is dogmatically sufficient to encompass patrimonial frauds mediated

by Artificial Intelligence (AI), particularly those carried out through deepfakes, voice cloning, and other digital manipulation techniques. It is assumed that the typical structure of estelionato, originally conceived for analogous frauds, may face difficulties in covering, without legislative complementation, the greater sophistication and harmful potential of these new forms of deception. To this end, the structural elements of Article 171, caput, and the electronic fraud aggravating circumstance set out in §2-A are examined and confronted with the characteristics of AI-mediated frauds, together with a critical analysis of national and international legislative trends aimed at the specific criminalization of technological frauds. The research is qualitative, bibliographic, and documentary in nature, employing the deductive method. The results indicate that, although the criminal offense of estelionato is, as a rule, structurally capable of encompassing frauds committed through the use of AI, their greater sophistication and capacity to induce error justify the inclusion of a specific penalty-increasing clause, either as an addition to §2-A or as an autonomous qualifying circumstance, so as to ensure greater legal certainty and proportionality in the criminal response.

Keywords: Fraud; Artificial Intelligence; Electronic fraud; Digital Criminal Law; Penal Code.

1. INTRODUÇÃO

Com a evolução da sociedade e da ciência, houve o surgimento da figura da Inteligência Artificial (IA), desta vez como algo utilizável e não como algo futurístico como já vinha sendo.

A Inteligência Artificial entrou na rotina das pessoas e aparenta ser uma coisa nova, porém este termo foi inventado em 1956 e

idealizado pelo cientista da computação norte-americano John McCarthy. Nesse sentido, atualmente já teve uma enorme evolução, sendo capaz de produzir rostos, vozes, vídeos com apenas alguns comandos dos usuários.

Ademais, foi se observando que tais evoluções estavam sendo utilizadas para a prática de ilícitas, algo que era para ser utilizado apenas para beneficiar e ajudar as pessoas em suas rotinas, atualmente é frequentemente utilizada na prática de crimes, principalmente no crime de estelionato presente no art. 171 do Código Penal.

Isso ocorre muito pela facilidade e propagação da IA, assim criminosos se utilizam desse meio para induzir as vítimas a algum tipo de erro e assim manter uma vantagem ilícita sobre seu prejuízo.

Logo, por ser algo tão disseminado e em constante evolução surge a dúvida que é objeto de investigação deste artigo, que gira em torno da capacidade do atual art. 171 do CP em abranger os possíveis novos cenários que estão surgindo.

Diante desse cenário, o problema que orienta esta investigação consiste em saber se o tipo penal de estelionato, previsto no art. 171 do CP Brasileiro, é dogmaticamente suficiente para abarcar as fraudes mediadas por Inteligência Artificial. Nesse sentido, a pesquisa busca responder às seguintes questões norteadoras: quais são os elementos estruturais do art. 171, caput, do CP, incluindo a fraude eletrônica prevista no §2º-A? De que forma as fraudes mediadas por inteligência artificial se relacionam com os elementos típicos do estelionato? As tendências legislativas atuais são

suficientes para lidar com essas novas formas de fraude ou demandam aprimoramento para garantir maior segurança jurídica?

O objetivo geral deste artigo é analisar se o tipo penal de estelionato previsto no art. 171 do CP necessita de reformulação legislativa para enfrentar adequadamente as fraudes praticadas com o uso de inteligência artificial. De forma mais específica, pretende-se analisar estruturalmente o art. 171, caput, e seu §2º-A, referente à fraude eletrônica; examinar a utilização da Inteligência Artificial e as fraudes por ela mediadas frente aos elementos estruturais do estelionato; avaliar criticamente as tendências legislativas de tipificação específica de fraudes tecnológicas, à luz da coerência sistemática do Direito Penal; e sugerir possíveis soluções que ofereçam mais segurança jurídica e uma resposta judicial e legislativa adequada para as fraudes patrimoniais praticadas com o uso de Inteligência Artificial.

O estudo desse tema mostra-se relevante ao se observar o crescimento da prática do crime de estelionato por meio da utilização da Inteligência Artificial, impulsionado, sobretudo, pela facilidade de acesso a esses recursos. Esse crescimento evidencia uma lacuna normativa, na medida em que o tipo penal em comento ainda é interpretado de maneira superficial diante de uma prática que confere maior credibilidade ao engano, já que possibilita a criminosos produzirem vídeos e áudios que simulam a identidade de terceiros. Além disso, a pesquisa possui relevância acadêmica e prática, podendo contribuir tanto para o refinamento técnico da estrutura do delito de estelionato quanto para a obtenção de uma resposta penal mais coerente, proporcional e fundamentada.

2. CRIME DE ESTELIONATO

2.1. Estrutura do Delito de Estelionato

Tendo a fraude como seu ponto central, o delito de estelionato já faz parte do rol de crimes desde muito tempo, chegando a ter pena de morte caso o prejuízo fosse superior a vinte mil-réis, conforme a Ordenações Filipinas (1603-1830), sendo na época denominado 'burla', ou 'inliço'.

Embora historicamente voltado à repressão de fraudes em contextos interpessoais e menos complexos, o estelionato manteve, ao longo do tempo, uma estrutura típica praticamente inalterada, mesmo diante das profundas transformações tecnológicas. Assim, um tipo penal concebido para realidades analógicas mostra-se, em certa medida, defasado frente às novas formas de fraude digital, especialmente aquelas mediadas por inteligência artificial, que ampliam significativamente o alcance, a sofisticação e o potencial lesivo das condutas enganosas.

No ordenamento jurídico atualmente o conceito do estelionato não se alterou tanto "Art. 171 - 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"(Brasil, 1940).

Depreende-se, portanto, que o estelionato constitui um tipo penal de longa tradição histórica cuja estrutura normativa permaneceu essencialmente a mesma ao longo dos séculos, refletindo a inalterada essência da fraude como conduta humana. Essa estabilidade tipológica, embora demonstre a solidez dogmática do art. 171 do CP, suscita questionamentos relevantes quanto à sua capacidade de alcançar, sem complementação legislativa, as novas

e mais sofisticadas modalidades de engano viabilizadas pela inteligência artificial.

2.1.1. Elementos do Delito

Ocupando a fraude o seu ponto central, é possível identificar os seguintes elementos que integram sua figura típica: a) conduta do agente com a finalidade de obter vantagem ilícita de natureza econômica; b) essa vantagem poder ser para si ou para outrem; c) a vítima é induzida ou mantida em erro; d) o agente faz uso de um artifício, ardil ou qualquer outro meio fraudulento (Greco, 2026).

Nesse sentido, a conduta do agente deve ter o objetivo de obter uma vantagem ilícita que será conseguida às custas do prejuízo alheio. Segundo Greco (2026), a vantagem é ilícita quando ela não tem respaldo no ordenamento jurídico, sendo na verdade contrária a ele, pois se ela fosse lícita poderia ser caracterizada como outra infração penal.

Além do mais, ainda sobre a vantagem ilícita, Luiz Regis Prado afirma que a tal vantagem não necessariamente teria que ser econômica, visto que o legislador não restringiu como fez no delito de extorsão ao empregar a expressão indevida vantagem econômica. Entretanto, Greco contrapõe ao afirmar que não se pode abandonar a interpretação sistêmica e, já que o delito encontra-se no Título II que corresponde aos crimes contra o patrimônio, a interpretação não poderia ser diferente. Tal interpretação também é feita no que se refere ao prejuízo alheio, sendo de natureza econômica e podendo ser algo que o sujeito possuía e perdeu, ou então algo que tinha o direito de receber e não pôde. Diferentemente afirma Cezar Roberto Bitencourt, ao dizer que a

vantagem deve ser injusta mas não precisa ser econômica, não importando a sua natureza (Greco, 2026; Bitencourt, 2019).

Conforme o caput, a vantagem ilícita pode ser em favor próprio ou de terceiro, não sendo necessário que esse terceiro saiba que o que recebeu foi obtido ilicitamente. A fraude que o agente utiliza objetiva induzir a vítima a erro ou mantê-la num erro preexistente, e isso se dá com o emprego de artifício, ardil ou qualquer outro meio fraudulento.

O artifício é uma simulação ou dissimulação da realidade que induz uma pessoa a erro; ardil corresponde à astúcia, à sutileza. É necessário que o meio fraudulento seja suficientemente apto para que possa induzir ou manter a vítima no erro, sendo este uma representação ou avaliação equivocada da realidade (Bitencourt, 2019).

Nesse sentido, os elementos estruturais do delito de estelionato, especialmente o artifício, o ardil e o erro da vítima, possuem contornos dogmaticamente bem definidos pela doutrina, os quais servirão de parâmetro fundamental para a análise, desenvolvida nos tópicos seguintes, acerca da adequação típica das fraudes mediadas por inteligência artificial ao tipo previsto no art. 171 do CP.

2.1.2. Classificação Doutrinária e o Bem Jurídico

Partindo para sua classificação doutrinária, é um crime comum tanto em relação ao sujeito ativo quanto ao sujeito passivo; doloso, afirmando Hungria que um crime em que se provoca ou mantém erro com astúcia não tem como não ter vontade consciente; material; comissivo e omissivo, levando em conta que é possível comissivamente induzir ao erro ou omissivamente mantê-la no erro;

de forma livre; instantâneo; de dano; monossubjetivo; plurissubsistente; transeunte ou não transeunte, podendo deixar vestígios materiais ou não, dependendo da forma como é praticado (Greco, 2026; Bitencourt, 2019).

O bem jurídico tutelado é a inviolabilidade do patrimônio, protegendo-se tanto o interesse social, presente na confiança recíproca que deve existir nos relacionamentos patrimoniais individuais e comerciais, e o interesse público ao punir a fraude causadora de dano alheio. O sujeito ativo pode ser qualquer pessoa, podendo haver o concurso eventual de pessoas por coautoria ou participação, podendo o terceiro a quem seja destinada a vantagem ilícita ser um coautor ou partícipe; entretanto, nada impede que o terceiro não tenha ciência do crime (Bitencourt, 2019).

Constata-se que a estrutura subjetiva e objetiva do crime de estelionato, com seu bem jurídico voltado à tutela do patrimônio e à manutenção da confiança nas relações patrimoniais, oferece base dogmática suficiente para a análise das fraudes mediadas por inteligência artificial, embora a amplitude das condutas possíveis com o uso dessas tecnologias possa demandar respostas normativas complementares para garantir a proporcionalidade da resposta penal.

2.1.3. Consumação, Tentativa e o Elemento Subjetivo

Em relação à consumação e tentativa:

Tem-se por consumado o estelionato, em sua modalidade básica, quando o agente consegue obter a vantagem ilícita, em prejuízo da vítima. Há necessidade, para efeitos de reconhecimento de consumação do estelionato, da afirmação do binômio vantagem ilícita/prejuízo alheio. Assim, quando o agente consegue auferir a vantagem ilícita em prejuízo da vítima, o delito chega à sua consumação. Se, no entanto, depois de iniciados os atos de execução configurados na fraude empregada na prática do delito, o agente não conseguir obter a vantagem ilícita em virtude de circunstâncias alheias à sua vontade, o crime restará tentado (Greco, 2026).

Em continuidade, a prática do delito de estelionato demonstra uma vontade livre e consciente de enganar alguém, por qualquer meio fraudulento, para em prejuízo de outrem obter vantagem indevida, representando como elemento subjetivo geral, o dolo, que deve abranger não apenas a ação como também seu meio, vantagem ilícita e prejuízo alheio. O dolo está presente em momentos diferentes dos cenários de induzimento e manutenção: na primeira figura, 'induzir a erro', ele se faz antes mesmo do emprego do meio ou da produção dos resultados. Já na segunda figura, 'manter em erro', o dolo é simultâneo ao erro, visto que percebe a existência do erro, consistindo o dolo exatamente na sua manutenção (Bitencourt, 2019).

Também destaca Bitencourt (2019) a existência do *elemento subjetivo especial* do tipo que se constitui pelo *especial fim* de obter qualquer vantagem ilícita para si ou para outrem, sendo necessário que o agente tenha consciência de que está obtendo uma

vantagem indevida, pois se ele acredita que é legítima desaparecerá o dolo, constituindo erro de tipo o erro sobre a justiça ou legalidade, já que incide sobre uma elementar típica. Dessa forma, somente o fim de produzir dano patrimonial ou prejuízo a alguém, sem objetivar um proveito injusto não caracteriza o estelionato. Em consonância com Hungria, afirma a inexistência da modalidade culposa, mesmo diante da possibilidade de alguém ser induzido ou mantido em erro por imprudência ou negligência.

Conclui-se, portanto, que o elemento subjetivo do estelionato, o dolo genérico acrescido do especial fim de obter vantagem ilícita, mantém plena aplicabilidade nas fraudes mediadas por inteligência artificial, posto que o agente que se utiliza dessas tecnologias age com plena consciência e vontade de enganar, conservando intacto o juízo de reprovabilidade penal sobre sua conduta.

2.1.4. Estelionato e Falsidade

Quando o agente se utiliza de *falsum* como meio para a prática de estelionato Nucci (2025) afirma que se deve aplicar a Súmula 17 do STJ que diz "Quando o falso se exaure no estelionato, sem mais potencialidade lesiva, é por este absorvido", no qual se refere da regra de que o crime-fim absorve o crime-meio. Entretanto, se o documento falsificado não está destinado para a prática de um delito de estelionato, servindo para outros objetivos do falsificador, estaremos diante de um concurso material de crimes.

Segundo Bitencourt (2019), ainda há mais dois cenários possíveis, um diante da existência de um concurso formal entre o estelionato e o crime de *falsum*, sendo indiferente se a falsidade é ideológica, material, de documento público ou particular, o outro seria de o

crime de falso versar sobre documento público, em que a pena seria superior ao estelionato.

Entende-se, nessa perspectiva, que a relação entre falsidade e estelionato já possui tratamento doutrinário e jurisprudencial consolidado, o qual deverá ser observado igualmente nas hipóteses em que a falsidade se opera por meio de tecnologias de inteligência artificial, como os *deepfakes*, sendo o princípio da absorção aplicável sempre que a conduta falsária esgotar sua lesividade no próprio delito patrimonial.

2.1.5. A Qualificadora Referente à Fraude Eletrônica (§2º-a)

Segundo o Código Penal Brasileiro assim dizem os parágrafos §§ 2º-A e 2º-B, que tratam respectivamente sobre fraude eletrônica e sua causa de aumento de pena:

§ 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.

§ 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.

Segundo Greco (2026), essa modalidade qualificada do estelionato apresenta que a vítima ou o terceiro são induzidos a erro pelo

agente que se utiliza: a) das redes sociais; b) contatos telefônicos; c) envio de correio eletrônico fraudulento; d) ou por qualquer outro meio fraudulento análogo.

Cunha (2013 *apud* Greco, 2026), traz situações que esclarecem esse meio apresentados no tipo:

- a. **por meio de redes sociais:** atualmente as redes sociais como Facebook e Instagram contêm muitos anúncios veiculados, não raramente, dentre esses há anúncios fraudulentos;
- b. **por contatos telefônicos:** as fraudes por meio telefônicas são muito comuns, um exemplo recorrente envolve cartão de crédito no qual o fraudador finge ser funcionário de uma instituição financeira e que detectou compras que possam ser fraudes com o cartão da vítima e pede que ela confirme os dados e digite a senha do cartão. Assim ele obtém a senha para fazer compras, efetuar etc.;
- c. **pelo envio de correio eletrônico fraudulento:** Nesta situação a vítima recebe um e-mail fraudulento, que se assemelha aos caracteres utilizados por organizações ou empresas conhecidas e através do acesso pelo link que é disponibilizado ele obtém acesso aos dados pessoais e bancários;
- d. **por qualquer outro meio fraudulento análogo:** esta expressão analógica inclui outras práticas fraudulentas cometidas por meios eletrônicos ou informáticos, a exemplo daqueles em que a vítima não é abordada diretamente pelo agente, mas é induzida a erro por outros fatores, como simulação de estabelecimento comercial, cópia de outra página bem conhecida, etc.

Diferencia também, Cunha (2013 apud Greco, 2026), o furto com fraude do estelionato praticado através de fraude eletrônica ao exemplificar duas situações:

1. Um hacker que invade uma rede pública de internet e obtém dados de acesso a contas bancárias, efetuando saques;
2. Um indivíduo que acessa um anúncio de uma rede varejista oferecendo uma TV com preço muito abaixo das concorrentes, insere seus dados bancários sem saber que é uma página clonada, efetua o pagamento que é recebido pelo autor da fraude.

No primeiro exemplo temos um caso típico de furto mediante fraude, já neste exemplo a vítima participa diretamente ao ser induzida por um anúncio enganoso, fornecendo os dados que dão a vantagem ilícita ao agente.

Em relação ao §2º-B, a pena prevista no §2º-A do art. 171 do CP, em razão da prática do crime utilizando-se de um servidor mantido fora do território nacional, aumenta-se de $\frac{1}{3}$ (um terço) a $\frac{2}{3}$ (dois terços), aplicando o julgador esta causa especial de aumento de pena por conta da relevância do resultado gravoso (Greco, 2026).

Dessa forma, embora o §2º-A e o §2º-B do art. 171 do CP representem avanços na tipificação das fraudes eletrônicas, suas redações apresentam limitações estruturais diante das especificidades das fraudes mediadas por inteligência artificial, especialmente quanto à ausência de referência expressa a essa tecnologia e à insuficiência das causas de aumento vigentes para refletir o grau de reprovabilidade destas condutas, questão que será aprofundada nos tópicos subsequentes.

3. A INTELIGÊNCIA ARTIFICIAL COMO INSTRUMENTO DE FRAUDE NO DELITO DE ESTELIONATO

A sociedade encontra-se em constante evolução, e atualmente a tecnologia está diariamente presente na vida de todos, seja para obter informações, para se promover através de redes sociais ou até mesmo para transferir valores econômicos. Dessa maneira a Inteligência Artificial se tornou uma ferramenta muito importante utilizada para inúmeras atividades em áreas distintas.

A inteligência artificial pode ser compreendida como um campo que envolve a criação de sistemas capazes de reproduzir ou superar desempenhos humanos em determinadas tarefas, estando seu conceito relacionado a processos de pensamento e resultados observáveis (Russel; Norvig, 2009, apud Hayward; Maas, 2026, p. 47).

a. ***Deepfakes***

O *deepfake* consiste em uma técnica avançada de manipulação de mídias que utiliza inteligência artificial para criar vídeos, áudios e imagens falsas com aparência autêntica, tendo sua denominação originada da fusão entre os termos *deep learning*, subárea do aprendizado de máquina baseada em redes neurais, e *fake*, que significa falso (Distrito, 2025). Em termos técnicos, os *deepfakes* geralmente se baseiam nas chamadas Redes Generativas Adversariais (GANs), segmento da inteligência artificial com capacidade para gerar novos conteúdos a partir de dados de treinamento (Tecnoblog, 2024). No campo das fraudes patrimoniais, criminosos se valem dessa tecnologia para imitar autoridades, colegas de

trabalho ou familiares, solicitando transferências bancárias ou informações sigilosas (Distrito, 2025).

Infere-se que os *deepfakes* representam uma das modalidades mais graves de instrumentalização da inteligência artificial para fins fraudulentos, na medida em que potencializam o artifício enganoso do estelionato a ponto de tornar o erro da vítima praticamente irresistível, o que impõe reflexão crítica sobre a suficiência do tipo penal vigente para capturar a superior reprovabilidade dessas condutas.

b. Clonagem de voz

A clonagem de voz é uma das vertentes mais preocupantes dos *deepfakes*, consistindo na replicação sintética das características vocais de uma pessoa por meio de algoritmos de IA generativa, sendo necessária apenas uma pequena amostra de áudio para que o sistema reproduza com alta fidelidade o timbre, a entonação e o ritmo da fala do indivíduo (Revista Tecnológica da Fatec Americana, 2025). Observando pelo viés criminal, essa tecnologia serve como artifício que induz a vítima ao erro, fazendo-a acreditar que está interagindo com familiar, amigo ou superior hierárquico, o que leva à realização de transferências financeiras ou ao fornecimento de dados sensíveis.

Dessa maneira a clonagem de voz por inteligência artificial representa uma modalidade de fraude de alta lesividade, cujo potencial de indução ao erro supera em muito os meios tradicionais de engano, impondo ao operador do direito o desafio de enquadrá-la adequadamente nos elementos do

tipo penal de estelionato, especialmente no que diz respeito ao artifício e ao erro da vítima.

c. ***Phishing* automatizado por grandes modelos de linguagem**

O *phishing* é uma modalidade de ataque cibernético em que o agente utiliza mensagens fraudulentas para convencer a vítima a fornecer informações confidenciais ou realizar ações em benefício do criminoso (Rafael, 2025). Com o uso de grandes modelos de linguagem, essa prática tornou-se ainda mais sofisticada, uma vez que passou a permitir a geração automatizada de mensagens altamente personalizadas, multilíngues e persuasivas em larga escala, eliminando os erros gramaticais e as inconsistências que antes facilitavam a identificação do conteúdo fraudulento (Bertacchini, 2025).

Conclui-se que o *phishing* automatizado por grandes modelos de linguagem constitui uma evolução qualitativa das práticas fraudulentas tradicionais, cuja principal característica, a capacidade de produzir engano em larga escala com alto grau de personalização potencializa os elementos do estelionato sem criar, necessariamente, uma conduta ontologicamente nova, embora exija respostas normativas que contemplem sua superior ofensividade.

d. **Engenharia social assistida por inteligência artificial**

A engenharia social é uma técnica de manipulação psicológica usada para enganar usuários e obter informações confidenciais ou induzir a realização de ações que beneficiem o atacante, explorando vulnerabilidades humanas em vez de técnicas, com ênfase no fator da confiança (Gomes, 2024).

Com a incorporação da inteligência artificial, essa prática adquiriu escala e sofisticação inéditas, na medida em que ferramentas automatizadas passaram a coordenar ataques simultâneos contra múltiplas vítimas, ajustar estratégias em tempo real e responder de forma autônoma às interações das vítimas, tornando o processo de manipulação praticamente indistinguível de uma comunicação humana legítima (Souza, 2025).

Diante do exposto, verifica-se que a inteligência artificial não apenas amplia o alcance das fraudes patrimoniais, mas confere a cada uma de suas modalidades um grau de sofisticação que desafia os parâmetros tradicionais de análise do tipo penal de estelionato. Ao possibilitar a simulação de identidades, a automação da manipulação psicológica e a personalização em massa do engano, a IA potencializa os elementos estruturais do delito sem, necessariamente, criar condutas ontologicamente novas. Essa constatação impõe o exame crítico de cada elemento típico do art. 171 do CP à luz dessas novas realidades tecnológicas, que será desenvolvido a seguir.

3.1. Limites Estruturais do Tipo Penal de Estelionato Frente à Inteligência Artificial

O CP, promulgado em 1940 em contexto analógico e alheio à inteligência artificial, apresenta evidente descompasso com a realidade tecnológica contemporânea. A inserção da figura qualificada da fraude eletrônica no art. 171, §2º-A, por meio da Lei n. 14.155/2021, representa um esforço de atualização, mas revela-se insuficiente diante das modalidades de fraude mediadas por

sistemas de inteligência artificial. O presente tópico examina, a partir dos elementos estruturais do estelionato, se o uso de IA representa mero aperfeiçoamento do meio executivo ou alteração qualitativa que reclama resposta legislativa específica.

3.1.1. Análise dos Elementos do Estelionato à Luz das Modalidades de Fraude Mediada por Inteligência Artificial

A estrutura típica do estelionato organiza-se em torno de quatro elementos: o emprego de artifício, ardil ou qualquer outro meio fraudulento; o induzimento ou a manutenção da vítima em erro; a obtenção de vantagem ilícita; e o prejuízo alheio.

Quanto ao elemento 'artifício, ardil ou qualquer outro meio fraudulento', a IA potencializa, mas não cria uma estrutura ontologicamente nova. Conforme Bitencourt (2019), o artifício corresponde à simulação ou dissimulação da realidade destinada a induzir alguém ao erro. Tecnologias como o *deepfake* e a clonagem de voz operam sobre esse mesmo substrato jurídico, sendo enquadráveis na cláusula aberta 'qualquer outro meio fraudulento'.

O phishing automatizado por grandes modelos de linguagem e a engenharia social assistida por IA apresentam uma nuance relevante: a IA permite que a elaboração de mensagens enganosas ocorra de forma automatizada, personalizada e em larga escala, eliminando os erros que antes serviam como sinais de alerta para vítimas mais atentas (Bertacchini, 2025). Essa automação não altera a natureza jurídica do meio fraudulento, mas impõe reflexão sobre a imputabilidade do resultado quando a conduta típica é parcialmente delegada a um sistema computacional.

O elemento de maior relevância dogmática é o 'erro da vítima'. No estelionato tradicional, o erro consiste em uma representação equivocada da realidade produzida pelo engodo do agente (Bitencourt, 2019). A IA, especialmente por meio de *deepfakes* e clonagem de voz, torna esse erro praticamente irresistível, inclusive para pessoas dotadas de discernimento acima da média.

Esse fenômeno foi demonstrado de forma eloquente no caso ocorrido em Hong Kong, em janeiro de 2024, em que um funcionário financeiro da empresa de engenharia britânica Arup foi induzido a transferir aproximadamente US\$ 25 milhões após participar de uma videoconferência em que todos os participantes, incluindo o suposto diretor financeiro, eram recriações geradas por *deepfake*. O funcionário, inicialmente desconfiado, cedeu ao ver rostos e vozes conhecidos na tela, o que ilustra como a IA pode eliminar a capacidade de discernimento da vítima mesmo diante de suspeita prévia (CNN, 2024). Tal fenômeno é ainda mais visível na engenharia social assistida por IA, em que sistemas automatizados conduzem interações em tempo real com múltiplas vítimas, ajustando a estratégia de persuasão de forma autônoma (Souza, 2025).

Quanto aos elementos 'vantagem ilícita' e 'prejuízo alheio', não se verificam alterações estruturais relevantes. A finalidade do agente permanece a obtenção de proveito patrimonial indevido em detrimento do patrimônio alheio, mantendo esses elementos inalterados em sua essência jurídica. Conclui-se que a IA impacta primordialmente os elementos instrumentais do tipo, especialmente o meio fraudulento e o induzimento ao erro, sem modificar, em regra, sua configuração jurídica básica.

3.1.2. Critérios para Distinção Entre Meio Executivo e Alteração Estrutural do Tipo Penal: Contribuições da Teoria da Imputação Objetiva

Para distinguir a mera evolução do meio executivo de uma eventual modificação qualitativa do tipo penal, a teoria da imputação objetiva de Claus Roxin oferece ferramenta interpretativa valiosa. Para Roxin (2002), a responsabilidade penal depende da demonstração de que o agente criou um risco juridicamente proibido e de que esse risco se realizou concretamente no resultado. A IA incrementa significativamente esse risco, tornando-o mais eficaz e difícil de ser identificado pela vítima, sem necessariamente criar um risco de natureza jurídica diversa.

Segundo Mello e Lazari (2022), há quatro critérios que permitem aferir se o uso de IA representa mero aperfeiçoamento do meio executivo ou transformação estrutural do tipo. O primeiro é o grau de autonomia do sistema: quando a IA opera como ferramenta controlada pelo agente, a imputação segue o modelo tradicional; quanto maior a autonomia do sistema, mais complexa se torna a cadeia de imputação, pois o sistema finalista exige conduta humana voluntária como pressuposto da responsabilidade penal.

O segundo é a intensidade da indução em erro: se a tecnologia torna o erro praticamente inevitável, há impacto qualitativo relevante que, embora não afaste a tipicidade, pode influenciar a dosimetria. O terceiro é a capacidade de controle humano sobre a IA: o agente que programa e aciona um sistema de *phishing* automatizado continua sendo o autor do crime por deter o domínio do fato.

O quarto é a previsibilidade do resultado típico: quando o uso da IA conduz com elevada probabilidade à indução da vítima em erro, reforça-se a manutenção da estrutura típica clássica. Na maioria dos casos, a IA atua como instrumento sofisticado nas mãos do agente humano, sem alterar a essência do tipo penal, embora cenários de elevada autonomia tecnológica tensionem os limites da imputação vigente.

3.1.3. O §2º-A e Sua Dificuldade Frente às Fraudes Mediadas por Inteligência Artificial

A expressão 'qualquer outro meio fraudulento análogo', constante do §2º-A, é cláusula aberta que autoriza a interpretação analógica, permitindo incluir condutas que guardam semelhança com os meios exemplificados no dispositivo. Sob esse aspecto formal, as fraudes mediadas por IA tendem a ser subsumíveis ao tipo, pois constituem instrumentos digitais empregados para induzir a vítima ao erro.

Entretanto, a subsunção formal não esgota o problema. Há ao menos duas insuficiências estruturais relevantes. A primeira é a ausência de agravante específica para o uso de IA no estelionato: o §2º-A trata de forma idêntica um golpe enviado por e-mail e uma fraude executada por *deepfake* de alta resolução, sem capturar a distinção no grau de sofisticação e no potencial de produzir erro irresistível, o que fragiliza a proporcionalidade da resposta penal (Correio Braziliense, 2025). Nesse sentido, merece atenção o fato de que o próprio legislador brasileiro, ao editar a Lei n. 15.123/2025, reconheceu expressamente a necessidade de majorar em metade a pena quando determinado crime é praticado mediante uso de inteligência artificial ou recurso tecnológico que altere imagem ou

som da vítima, ainda que o tenha feito apenas para o crime de violência psicológica contra a mulher, previsto no art. 147-B do CP. A ausência de previsão equivalente para as fraudes patrimoniais revela uma lacuna normativa que o §2º-A não supre.

A segunda insuficiência diz respeito aos cenários de elevada autonomia da IA: quando o processo de indução ao erro é delegado integralmente a um sistema automatizado que interage com centenas de vítimas sem supervisão direta, a cadeia de imputação se torna turva, gerando o que a doutrina denomina vazio de imputação criminal (Mello; Lazari, 2022).

Sob essa perspectiva, o uso da IA para a prática de fraudes como no caso de estelionatos cometidos por meio de simulações de voz, imagem ou identidade digital configura hipótese típica de criação de risco proibido, na medida em que potencializa a capacidade de indução em erro da vítima, ampliando significativamente a eficácia do meio fraudulento. A sofisticação desses mecanismos tecnológicos, inclusive, reduz a possibilidade de detecção da fraude pela vítima média, o que reforça o desvalor da conduta.

4. METODOLOGIA

A pesquisa adota o método dedutivo, que parte de teorias e princípios gerais para examinar situações particulares (Lakatos; Marconi, 2003). Partindo de premissas consolidadas, como a estrutura dogmática do estelionato, presente no art. 171 do CP, os elementos do tipo e a teoria da imputação objetiva de Claus Roxin, busca-se verificar se as fraudes mediadas por Inteligência Artificial se incluem ao tipo vigente ou se há lacunas que demandem resposta legislativa específica. A abordagem é qualitativa, voltada à

interpretação sistemática e à análise crítica de normas, decisões e doutrina, sem mensuração numérica, o que se adequa à natureza jurídico-dogmática do objeto.

Quanto às técnicas, utiliza-se a documentação indireta, que reúne as pesquisas bibliográfica e documental por operarem com fontes já existentes, sem contato com sujeitos de pesquisa (Lakatos; Marconi, 2003). A pesquisa bibliográfica abrange livros, artigos, teses e dissertações sobre a dogmática do estelionato, a imputação objetiva e o direito penal digital, além de publicações de tecnologia e criminologia sobre o uso de IA em fraudes patrimoniais, permitindo examinar o tema sob novo enfoque. A pesquisa documental analisa o Código Penal, especialmente o art. 171 e seus parágrafos, a Lei n. 14.155/2021, que inseriu a qualificadora da fraude eletrônica, a Lei n. 15.123/2025, que estabeleceu causa de aumento de pena para crimes praticados com uso de IA no campo da violência psicológica, os Projetos de Lei n. 6.119/2023 e n. 2.338/2023 e decisões dos tribunais superiores. A combinação dessas técnicas confere rigor metodológico à avaliação da suficiência do tipo penal de estelionato e de eventuais lacunas diante dessas fraudes.

5. TENDÊNCIAS LEGISLATIVAS NACIONAIS E INTERNACIONAIS

A análise das tendências legislativas sobre fraudes tecnológicas mediadas por IA revela dois modelos regulatórios predominantes no direito comparado: o modelo de tipificação autônoma e o modelo de agravação qualificada dentro de tipos preexistentes. Compreender suas virtudes e defeitos é essencial para avaliar qual deles melhor se ajusta à coerência sistemática do Direito Penal brasileiro.

O modelo de tipificação autônoma consiste na criação de novos crimes específicos para condutas mediadas por IA. Nos Estados Unidos, esse caminho foi percorrido pelo TAKE IT DOWN Act (2025), que criminalizou a publicação não consensual de conteúdo íntimo gerado por IA, e por legislações estaduais como a de Pennsylvania (2025) e Washington (2025), que estabeleceram sanções penais para a criação de *deepfakes* com intenção fraudulenta ou lesiva. No Reino Unido, o Online Safety Act passou a tratar o *deepfake* pornográfico como ofensa criminal prioritária (Crowell & Moring, 2025). A vantagem desse modelo é a precisão comunicativa: ao nominar o crime e descrever especificamente a conduta, o legislador oferece sinalização clara sobre o que é proibido e quais são as consequências. A desvantagem é que tipos muito específicos tendem a se tornar obsoletos rapidamente diante da aceleração tecnológica, além de criarem o risco de lacunas entre o que o tipo prevê e o que a tecnologia efetivamente permite.

O modelo de agravação qualificada, por sua vez, mantém tipos penais preexistentes e insere causas de aumento de pena ou qualificadoras específicas para condutas praticadas com uso de IA. Esse é o caminho que o Brasil já trilhou parcialmente com a Lei n. 15.123/2025, que majorou penas em crimes praticados mediante uso de inteligência artificial ou recurso tecnológico que altere imagem ou som da vítima, embora restrita ao campo dos crimes de violência psicológica e não ao patrimonial. A Convenção de Budapeste sobre crimes cibernéticos, da qual o Brasil é signatário desde 2021, também adota essa lógica ao agravar condutas já tipificadas quando praticadas por meios informáticos, sem criar tipos autônomos para cada nova modalidade tecnológica de crime.

No direito brasileiro, essa movimentação legislativa ainda se encontra em fase de consolidação, mas já apresenta sinais claros de expansão. Um exemplo relevante é o Projeto de Lei nº 6.119/2023, que propõe a alteração do CP para tratar especificamente do uso fraudulento da inteligência artificial, especialmente em contextos de publicidade enganosa. O referido projeto busca criminalizar a criação, utilização e disseminação de conteúdos manipulados por IA, como imagens, áudios e vídeos, com o objetivo de induzir consumidores a erro (Brasil, 2023).

Além disso, o projeto prevê a criação de um tipo penal específico no âmbito do Código de Defesa do Consumidor, com pena de reclusão de 4 a 8 anos para condutas que envolvam o uso de inteligência artificial para manipulação e engano do consumidor. Tal proposta evidencia uma clara opção pelo modelo de tipificação autônoma, ao reconhecer que determinadas condutas mediadas por IA possuem grau de reprovabilidade e especificidade suficiente para justificar um tratamento penal próprio (Brasil, 2023).

Outro ponto relevante do substitutivo apresentado no parecer legislativo é a previsão de aumento de pena para crimes já existentes quando praticados com o uso de inteligência artificial, como no caso de crimes contra a honra. Essa técnica legislativa demonstra a tentativa de combinar os dois modelos regulatórios, promovendo tanto a criação de novos tipos quanto o agravamento de condutas já tipificadas (Brasil, 2023).

A justificativa do projeto também reforça um elemento central para a presente pesquisa: a dificuldade crescente de identificação de fraudes por parte das vítimas. Estudos citados no parecer indicam que a maioria dos consumidores não consegue distinguir conteúdos

autênticos de *deepfakes*, o que potencializa significativamente o erro da vítima, elemento essencial do estelionato e amplia o risco social dessas condutas (Brasil, 2023).

No âmbito do marco regulatório da IA no Brasil, o Projeto de Lei n. 2.338/2023, aprovado pelo Senado em dezembro de 2024 e em tramitação na Câmara dos Deputados em 2025 não cria novos tipos penais, mas estabelece um regime de responsabilização baseado em risco, com obrigações de governança, transparência e gestão para desenvolvedores e operadores de sistemas de IA, inspirado no AI Act da União Europeia. Embora a proposta reconheça que as fraudes patrimoniais cometidas com IA encontram tipificação parcial no ordenamento vigente, ela reconhece, implicitamente, que o Código Penal precisará ser atualizado para abarcar as especificidades dessas condutas (Lexprime, 2026). Essa constatação confirma que a resposta legislativa adequada não consiste em abandonar o tipo penal de estelionato, mas em complementá-lo com instrumentos que capturem o grau superior de reprovabilidade das fraudes mediadas por IA.

Observa-se, portanto, que as tendências legislativas nacionais e internacionais convergem para o reconhecimento de que as fraudes mediadas por inteligência artificial demandam resposta normativa específica, seja por meio do aprimoramento dos tipos penais existentes, seja pela criação de novos instrumentos de agravamento da pena, revelando que a simples aplicação interpretativa do art. 171 do CP, embora possível em grande parte dos casos, mostra-se insuficiente para garantir a proporcionalidade e a segurança jurídica exigidas pelo princípio da legalidade.

5.1. Sugestão Legislativa para uma Maior Segurança Jurídica

A criação de um tipo penal autônomo de 'fraude por inteligência artificial' ou 'estelionato por *deepfake*', sem que se avalie com rigor se a conduta é estruturalmente distinta do estelionato tradicional, não supera o teste da coerência sistemática. Como analisado nos tópicos anteriores deste artigo, a IA não cria uma conduta qualitativamente nova, ela potencializa o meio executivo da fraude sem alterar os elementos típicos do art. 171. Nesse contexto, um tipo autônomo seria ineficiente e potencialmente inconstitucional, por violar a lei certa ao duplicar a incriminação de uma conduta já tipificada em termos que não se distinguem com clareza dos existentes.

Por outro lado, a inércia legislativa também não se sustenta. A ausência de circunstâncias específica para fraudes patrimoniais com uso de IA representa uma lacuna de proporcionalidade que o simples recurso à interpretação evolutiva não pode suprir, pois a pena aplicável, limitada pelos parâmetros do art. 171 e de seu §2º-A, não reflete adequadamente a superior ofensividade de condutas que podem vitimar centenas de pessoas simultaneamente, produzir erros praticamente irresistíveis mesmo para pessoas atentas e operar com alto grau de anonimato tecnológico.

A proposta que melhor equaciona essas tensões, e que mais se aproxima dos princípios de intervenção mínima, legalidade e proporcionalidade, é a inserção de causa de aumento de pena específica para as fraudes patrimoniais praticadas com uso de IA generativa, seja como parágrafo adicional ao §2º-A do art. 171, seja como qualificadora autônoma dentro do tipo de estelionato. Esse modelo preserva a coerência da estrutura típica existente, evita a inflação legislativa, respeita os limites da lei certa ao nominar com precisão o elemento intensificador (uso de IA) e responde

proporcionalmente ao superior dano potencial dessas condutas. É também o caminho apontado pela Lei n. 15.123/2025, que já adotou essa lógica em outros tipos penais, indicando que o ordenamento brasileiro já reconhece a IA como fator de agravação da reprovabilidade, faltando apenas estender essa lógica ao campo das fraudes patrimoniais.

Conclui-se, assim, que a avaliação crítica das tendências legislativas de tipificação específica de fraudes tecnológicas aponta não para a criação indiscriminada de tipos penais novos, mas para o aprimoramento técnico e sistemático do tipo penal de estelionato, mediante a inserção de causa de aumento que capture adequadamente o grau de reprovabilidade das fraudes mediadas por IA, em respeito à tradição dogmática do Direito Penal brasileiro e aos princípios constitucionais que a fundamentam.

6. CONCLUSÃO/CONSIDERAÇÕES FINAIS

A presente pesquisa teve como problema central verificar se o tipo penal de estelionato, previsto no art. 171 do CP, é dogmaticamente suficiente para abarcar as fraudes patrimoniais mediadas por Inteligência Artificial. A análise dos elementos estruturais do delito, confrontados com as modalidades de fraude viabilizadas por *deepfakes*, clonagem de voz, *phishing* automatizado por grandes modelos de linguagem e engenharia social assistida por IA, permitiu confirmar, ainda que parcialmente, a hipótese inicial: a estrutura típica do estelionato, concebida para fraudes analógicas, revela-se apta, em regra, a alcançar essas novas modalidades de engano, mas apresenta insuficiências pontuais que comprometem a proporcionalidade da resposta penal.

Constatou-se que os elementos do artifício, do ardil e do erro da vítima possuem contornos dogmáticos sólidos, capazes de recepcionar, por meio da cláusula aberta “qualquer outro meio fraudulento análogo”, as condutas mediadas por tecnologias digitais. A Inteligência Artificial não cria uma conduta essencialmente nova, mas potencializa o meio executivo da fraude e a intensidade da indução ao erro, tornando este último, em determinados cenários, praticamente irresistível. Na maioria dos casos, a IA atua como instrumento sofisticado nas mãos do agente, preservando a estrutura clássica de imputação, embora sendo bem mais eficaz e com um maior poder de ludibriar as vítimas.

O exame das tendências legislativas nacionais e internacionais evidenciou a convergência entre os modelos de tipificação autônoma e de agravação qualificada, tendo o legislador brasileiro optado por esta última via na Lei n. 15.123/2025, ainda que restrita ao crime de violência psicológica contra a mulher. Essa opção revela uma lacuna de proporcionalidade no âmbito patrimonial, na medida em que o §2º-A trata de modo equivalente um golpe eletrônico convencional e uma fraude executada por *deepfake* de alta sofisticação, sem capturar a distinção no grau de reprovabilidade entre essas condutas.

Diante disso, rejeita-se tanto a criação de um tipo penal autônomo, por importar em duplicidade de incriminação e violação à lex certa, quanto a inércia legislativa, incapaz de suprir por interpretação evolutiva o descompasso entre a pena vigente e a superior ofensividade das fraudes mediadas por IA. Propõe-se, como síntese conclusiva da pesquisa, a inserção de uma causa de aumento de pena específica para as fraudes patrimoniais praticadas com uso de inteligência artificial generativa, seja como acréscimo ao §2º-A do art.

171, seja como qualificadora autônoma dentro do próprio tipo de estelionato. Essa solução preserva a estrutura dogmática consolidada do delito, respeita os princípios da intervenção mínima, da legalidade e da proporcionalidade, e estende ao campo patrimonial a lógica já adotada pelo legislador na Lei n. 15.123/2025. Conclui-se, assim, que o tipo penal de estelionato não carece de reformulação estrutural para enfrentar as fraudes mediadas por IA, mas sim de aprimoramento técnico pontual, capaz de traduzir, em termos de dosimetria, o maior potencial lesivo dessas condutas.

REFERÊNCIAS BIBLIOGRÁFICAS

AGÊNCIA BRASIL. **Conteúdos falsos criados com IA mais que triplicam entre 2024 e 2025.** Brasília: EBC, 6 fev. 2026. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2026-02/conteudos-falsos-criados-com-ia-mais-que-triplicam-entre-2024-e-2025>. Acesso em: 20 abr. 2026.

BERTACCHINI, Thiago. **Como prevenir fraudes que usam ferramentas LLM.** IPNEWS, 2025. Disponível em: <https://ipnews.com.br/como-prevenir-fraudes-que-usam-ferramentas-llm/>. Acesso em: 22 abr. 2026.

BITENCOURT, Cezar R. Código penal comentado. 10. ed. Rio de Janeiro: Saraiva Jur, 2019. E-book. p.841. ISBN 9788553615704. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553615704/>. Acesso em: 15 abr. 2026.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 6.119/2023.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para dispor sobre o uso fraudulento de inteligência artificial. Brasília,

DF: Câmara dos Deputados, 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2415560>. Acesso em: 23 abr. 2026.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 abr. 2026.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Brasília, DF: Presidência da República, [1940]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 15 abr. 2026.

BRASIL. Lei n. 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Brasília, DF: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 22 abr. 2026.

BRASIL. Lei n. 14.155, de 27 de maio de 2021. Altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 22 abr. 2026.

BRASIL. Lei n. 15.123, de 24 de abril de 2025. Altera o art. 147-B do Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), para acrescentar causa de aumento de pena nos crimes cometidos mediante uso de inteligência artificial. Brasília, DF: Presidência da

República, 2025. Disponível em:
https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15123.htm. Acesso em: 22 abr. 2026.

BRASIL. Senado Federal. Projeto de Lei n. 2.338, de 2023. Estabelece normas gerais de caráter nacional para o desenvolvimento, implementação e uso responsável da inteligência artificial no Brasil. Brasília: Senado Federal, 2023. Disponível em:
<https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 22 abr. 2026.

BRASIL. Superior Tribunal de Justiça. Súmula n. 17 do STJ. Disponível em: <https://www.jusbrasil.com.br/busca?q=s%C3%BAmula+17+do+stj>. Acesso em: 19 abr. 2026.

BUSINESS-IT. **IA no Cibercrime: modelos de linguagem amplificam golpes de phishing.** 2024. Disponível em:
<https://business-it.pt/2024/11/12/ia-no-cibercrime-modelos-de-linguagem-amplificam-golpes-de-phishing/>. Acesso em: 20 abr. 2026.

CNN. **Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'.** Atlanta: CNN, 4 fev. 2024. Disponível em: <https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html>. Acesso em: 22 abr. 2026.

CORREIO BRAZILIENSE. **Deepfake e crimes digitais: quando a realidade se torna uma arma.** Brasília: Correio Braziliense, 8 maio 2025. Disponível em: <https://www.correiobraziliense.com.br/direito-e-justica/2025/05/7136758-deepfake-e-crimes-digitais-quando-a-realidade-se-torna-uma-arma.html>. Acesso em: 22 abr. 2026.

CROWELL & MORING LLP. Forged faces, real liability: deepfake laws take effect in Washington State and Pennsylvania. Washington: Crowell & Moring, 19 ago. 2025. Disponível em: <https://www.crowell.com/en/insights/client-alerts/forged-faces-real-liability-deepfake-laws-take-effect-in-washington-state-and-pennsylvania>. Acesso em: 22 abr. 2026.

CUNHA, Rogério Sanches. **Manual de direito penal: parte especial**, volume único. 5. ed. Salvador: Editora JusPodivm, 2013.

DISTRITO. **Deepfake: o que é, riscos e como se proteger de falsificações**. São Paulo: Distrito, 23 dez. 2025. Disponível em: <https://www.distrito.me/blog/deepfake-o-que-e-riscos-e-como-se-proteger-de-falsificacoes>. Acesso em: 20 abr. 2026.

FERRAJOLI, Luigi. Direito e razão: teoria do garantismo penal. 4. ed. São Paulo: Revista dos Tribunais, 2014.

GOMES, Bruna. **O uso de IA em golpes de Engenharia Social. Contacta, 3 set. 2024. Disponível em: <https://www.contacta.com.br/blog/inteligencia-artificial-e-o-uso-em-golpes-de-engenharia-social>**. Acesso em: 2 out. 2026.

GRECO, Luís. **Introdução à dogmática funcionalista do delito**. In: ROXIN, Claus. Funcionalismo e imputação objetiva em direito penal. Tradução de Luís Greco. Rio de Janeiro: Renovar, 2002.

GRECO, Rogério. Código Penal Comentado - 18ª Edição 2025. 18. ed. Rio de Janeiro: Atlas, 2025. E-book. p.542. ISBN 9786559776887. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786559776887/>. Acesso em: 15 abr. 2026.

GRECO, Rogério. Código Penal Comentado. 18. ed. Rio de Janeiro: Atlas, 2026.

HAYWARD, Keith J.; MAAS, Matthijs M. Inteligência artificial e crime: um guia para criminólogos. **Revista Científica do CPJM**, Rio de Janeiro, v. 5, n. 16, p. 42-91, 2026. Disponível em: <https://doi.org/10.55689/rcpjm.2026.16.003>. Acesso em: 22 abr. 2026.

IBCCRIM — INSTITUTO BRASILEIRO DE CIÊNCIAS CRIMINAIS. Direito Penal Simbólico e punitivismo. São Paulo: IBCCRIM, 2023. Disponível em: <https://ibccrim.org.br/noticias/exibir/4338>. Acesso em: 22 abr. 2026.

JESUS, Damásio de; MILAGRE, José Antonio. Manual de crimes informáticos. São Paulo: Saraiva, 2016.

JURIDIGITAL. **Deepfakes no contencioso: riscos da IA em processos.** 2026. Disponível em: <https://www.juridigital.com.br/deepfakes-no-contencioso/>. Acesso em: 20 abr. 2026.

LEAL, Giovana Gomes. **Análise forense de phishing automatizado com IA.** São Paulo: Universidade Presbiteriana Mackenzie, [2024]. Disponível em: <https://adelpha-api.mackenzie.br/server/api/core/bitstreams/f473f353-b8c0-4584-ad72-ca8b0ea0c737/content>. Acesso em: 20 abr. 2026.

LEX PRIME. A regulação da IA no Brasil e a necessidade de análise de impacto legal. São Paulo: Lex Prime, mar. 2026. Disponível em: <https://lexprime.com.br/a-regulacao-da-ia-no-brasil-e-a-necessidade-de-analise-de-impacto-legal/>. Acesso em: 22 abr. 2026.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

MASSON, Cleber. Direito penal: parte geral. 4. ed. São Paulo: Método, 2010.

MELLO, Rogério Luís Marques de; LAZARI, Rafael José Nadim de. Quem é o culpado? Uma análise criminal das interações humanas com a inteligência artificial. **Revista Brasileira de Direitos Fundamentais & Justiça**, [S. l.], v. 16, n. 46, p. 123–153, 2022. DOI: 10.30899/dfj.v16i46.1116. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/1116>. Acesso em: 22 abr. 2026.

NUCCI, Guilherme de Souza. Manual de direito penal. 21. ed. Rio de Janeiro: Forense, 2025.

OKAI. **Clonagem de Voz por Inteligência Artificial: o novo golpe da ligação silenciosa**. 2025. Disponível em: <https://okai.com.br/blog/clonagem-de-voz-por-inteligencia-artificial-o-novo-golpe-da-ligacao-silenciosa>. Acesso em: 20 abr. 2026.

PRADO, Luiz Regis. Curso de direito penal brasileiro – parte especial. 8. ed. São Paulo: Revista dos Tribunais, 2010, v. 2.

RAFAEL, Gustavo de Castro. **Guia Prático de IA e Cibersegurança: como proteger sua empresa na era digital**. PDCA TI, 2025. Disponível em: <https://www.pdcati.com.br/ebook-ia-ciberseguranca/>. Acesso em: 20 abr. 2026.

REVISTA TECNOLÓGICA DA FATEC AMERICANA. **Clonagem de voz por IA: avaliando a eficácia em ataques de phishing por voz**.

Americana: FATEC, v. 13, n. 01, 2025. Disponível em: <https://www.fatec.edu.br/revista/index.php/RTecFatecAM/article/view/412>. Acesso em: 20 abr. 2026.

ROXIN, Claus. **Funcionalismo e imputação objetiva no direito penal**. Tradução de Luís Greco. Rio de Janeiro: Renovar, 2002.

SOUZA, Ramon de. **Spear phishing e IA: a automatização de ataques de engenharia social**. Eskive, 10 abr. 2025. Disponível em: <https://conteudo.eskive.com/pt-br/spear-phishing-e-ia-a-automatizacao-de-ataques-de-engenharia-social>. Acesso em: 22 abr. 2026.

TECNOBLOG. **O que é deepfake? Conheça exemplos e entenda os riscos dessa tecnologia**. São Paulo: Tecnoblog, 24 set. 2024. Disponível em: <https://tecnoblog.net/responde/o-que-e-deep-fake-e-porque-voce-deveria-se-preocupar-com-isso/>. Acesso em: 20 abr. 2026.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS (TJDFT). O novo crime de fraude eletrônica e o princípio da legalidade. Brasília: TJDFT, 3 jun. 2022. Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2022/o-novo-crime-de-fraude-eletronica-e-o-principio-da-legalidade>. Acesso em: 22 abr. 2026.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024 (AI Act). Jornal Oficial da União Europeia, Bruxelas, 12 jul. 2024. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32024R1689>.

Acesso em: 22 abr. 2026.

¹ Discente do Curso Superior de Direito do Centro Universitário Santo Agostinho - UNIFSA. E-mail: [acesse o artigo original para visualizar o e-mail](#)

² Discente do Curso Superior de Direito do Centro Universitário Santo Agostinho - UNIFSA. E-mail: [acesse o artigo original para visualizar o e-mail](#)

³ Docente do Curso Superior de Direito do Centro Universitário Santo Agostinho. E-mail: [acesse o artigo original para visualizar o e-mail](#)