

A RESPONSABILIDADE PENAL PELO USO INDEVIDO DE INTELIGÊNCIA ARTIFICIAL: LIMITES DA IMPUTAÇÃO SUBJETIVA NOS CRIMES PRATICADOS POR MEIO DE SISTEMAS ALGORÍTMICOS

**CRIMINAL LIABILITY FOR THE MISUSE OF ARTIFICIAL INTELLIGENCE:
LIMITS OF SUBJECTIVE IMPUTATION IN CRIMES COMMITTED THROUGH
ALGORITHMIC SYSTEMS**

Ciências Sociais Aplicadas • 25/09/2026

REGISTRO DOI: [10.70773/revistatopicos/790300625](https://doi.org/10.70773/revistatopicos/790300625)

José Rúdenes Barros Nascimento¹

Maila Rocha Feitosa Herênio²

RESUMO

A difusão de sistemas de inteligência artificial generativa ampliou a capacidade de produzir conteúdos falsos e de automatizar condutas lesivas a bens jurídicos tutelados pelo direito penal. O artigo tem por objetivo analisar os limites e as possibilidades de imputação penal, no ordenamento jurídico brasileiro, pelo uso indevido desses sistemas. A pesquisa é bibliográfica e documental, de abordagem qualitativa, conduzida pelo método dedutivo, com exame da legislação penal em vigor, de proposições legislativas em tramitação e da produção doutrinária nacional e estrangeira publicada entre 2010 e 2026. Partiu-se dos pressupostos da responsabilidade penal fixados no Código Penal, em especial a exigência de conduta humana voluntária, a imputação subjetiva dos artigos 18 e 19 e a estrutura normativa da culpabilidade, para confrontá-los com os modelos de imputação sugeridos pela doutrina para entes artificiais. Os resultados indicam que o sistema penal brasileiro não comporta a punição do sistema de inteligência artificial em si, pois lhe faltam capacidade de ação, imputabilidade e potencial consciência da ilicitude, de modo que a responsabilização deve recair sobre as pessoas naturais que programam, treinam, disponibilizam ou operam a ferramenta. Verificou-se que a legislação vigente já alcança boa parte das condutas mais frequentes, por meio dos tipos de estelionato, furto mediante fraude eletrônica, crimes contra a honra e simulação de participação de criança ou adolescente em cena de sexo explícito, e que a Lei nº 15.123/2025 inaugurou a menção expressa à inteligência artificial no Código Penal. Permanecem dificuldades relevantes de prova da autoria e de delimitação do dever de cuidado dos desenvolvedores, o que recomenda cautela na criação de novos tipos penais e prioridade para respostas regulatórias, administrativas e civis.

Palavras-chave: Culpabilidade; Deepfake; Imputação penal; Inteligência artificial.

ABSTRACT

The spread of generative artificial intelligence systems has increased the capacity to produce false content and to automate conduct that harms legally protected interests. This article aims to analyse the limits and possibilities of criminal imputation, under Brazilian law, for offences committed through such systems. The research is bibliographical and documentary, qualitative in approach and deductive in method, examining criminal legislation in force, pending bills and national and foreign scholarship published between 2010 and 2026. The study starts from the requirements of criminal liability set out in the Brazilian Criminal Code, particularly voluntary human conduct, subjective imputation under articles 18 and 19 and the normative structure of culpability, and confronts them with the imputation models proposed by scholars for artificial entities. The results indicate that Brazilian criminal law does not allow punishment of the artificial intelligence system itself, since it lacks the capacity to act, criminal capacity and potential awareness of unlawfulness, so that liability must fall upon the natural persons who program, train, provide or operate the tool. Current legislation already covers most recurring conduct through the offences of fraud, theft by electronic fraud, crimes against honour and the simulation of a child in a sexually explicit scene, and Law 15,123/2025 introduced the first express mention of artificial intelligence in the Criminal Code. Significant difficulties remain regarding proof of authorship and the definition of developers' duty of care, which advises caution in creating new offences and priority for regulatory, administrative and civil responses.

Keywords: Artificial intelligence; Criminal imputation; Culpability; Deepfake.

1. INTRODUÇÃO

Ferramentas capazes de gerar texto, voz e imagem a partir de comandos escritos deixaram os laboratórios de pesquisa e chegaram ao aparelho celular de qualquer usuário. A fabricação de um vídeo falso, que até pouco tempo exigia equipamento caro, tempo e conhecimento técnico especializado, hoje se resolve em poucos minutos e a custo próximo de zero. Junto com os ganhos evidentes em produtividade, tradução e acessibilidade, essa mesma tecnologia passou a servir de meio para a prática de fraudes bancárias com clonagem de voz, para a montagem de imagens íntimas falsas e para a difusão de acusações inverídicas contra pessoas determinadas.

O direito penal brasileiro foi construído sobre uma premissa que essa realidade coloca à prova. Toda a teoria do delito parte da ação ou omissão de um ser humano, dotado de vontade, capaz de compreender o caráter ilícito do que faz e de se determinar conforme esse entendimento. Quando o resultado lesivo surge da operação de um sistema que aprende com dados, produz respostas não previstas por quem o programou e opera em uma cadeia que envolve desenvolvedores, provedores de infraestrutura e usuários finais espalhados por diferentes países, a pergunta sobre quem responde criminalmente deixa de ter resposta imediata.

O estudo trata da responsabilidade penal pelo uso indevido de inteligência artificial, ou seja, de quem responde criminalmente quando esses sistemas são empregados para a prática de crimes. O

recorte alcança as figuras do usuário, do desenvolvedor e do provedor, no período compreendido entre 2019 e 2026. Ficam fora da análise a responsabilidade civil pelos danos causados por sistemas autônomos e o emprego de inteligência artificial como ferramenta de investigação ou de julgamento no processo penal, temas que possuem literatura própria e exigiriam outro desenho de pesquisa.

A investigação parte do seguinte problema: quem responde criminalmente pelo uso indevido de sistemas de inteligência artificial e de que modo as categorias da imputação penal previstas no Código Penal brasileiro, especialmente a conduta humana voluntária, o nexo causal, o dolo, a culpa e a culpabilidade, permitem alcançar cada um dos agentes envolvidos?

O objetivo geral consiste em analisar os limites e as possibilidades da imputação penal pelo uso indevido de inteligência artificial no ordenamento brasileiro. Como objetivos específicos, pretende-se identificar os pressupostos da responsabilidade penal no direito pátrio, com ênfase na exigência de conduta humana e na estrutura da culpabilidade; examinar os modelos de imputação formulados pela doutrina para condutas mediadas por entes artificiais; verificar como a legislação penal em vigor tem alcançado o emprego de inteligência artificial na prática de crimes; e discutir os critérios de repartição da responsabilidade entre os diferentes agentes da cadeia tecnológica.

Quanto à metodologia, trata-se de pesquisa qualitativa, de objetivo exploratório e descritivo, desenvolvida pelo método dedutivo. O procedimento adotado é o da pesquisa bibliográfica e documental, com exame de doutrina nacional e estrangeira, da legislação penal

vigente e de proposições legislativas em tramitação no Congresso Nacional. Não houve coleta de dados empíricos.

O texto está organizado em seis seções de desenvolvimento. A primeira delimita o conceito de inteligência artificial e os graus de autonomia relevantes para o direito penal. A segunda recompõe os pressupostos da responsabilidade penal no ordenamento brasileiro. A terceira examina os modelos de imputação propostos pela doutrina. A quarta discute a repartição da responsabilidade entre usuário, desenvolvedor e provedor. A quinta analisa o tratamento normativo brasileiro em vigor. A última trata dos limites da resposta penal e das alternativas de regulação.

2. DESENVOLVIMENTO

2.1. Inteligência Artificial: Delimitação Conceitual e Graus de Autonomia

Não existe, no direito brasileiro em vigor, definição legal de inteligência artificial. O Projeto de Lei nº 2.338, de 2023, aprovado pelo Senado Federal em dezembro de 2024 e ainda pendente de deliberação na Câmara dos Deputados, adota fórmula próxima à empregada em documentos internacionais e descreve o sistema de inteligência artificial como aquele que, a partir de um conjunto de objetivos, infere a maneira de gerar resultados capazes de influenciar ambientes virtuais ou físicos, com algum grau de autonomia (BRASIL, 2023). A definição é ampla de propósito, pois pretende abarcar tecnologias em transformação constante.

Para os fins deste trabalho, interessa menos a discussão técnica sobre arquiteturas de aprendizado e mais a distinção entre três situações de uso, que produzem consequências jurídicas diversas.

Na primeira, o sistema funciona como instrumento sob comando direto de uma pessoa, que descreve o resultado pretendido e o obtém. É o caso de quem solicita a geração de um áudio imitando a voz de terceiro para aplicar um golpe. Na segunda, o sistema opera de forma semiautônoma, executa tarefas dentro de parâmetros gerais fixados por um operador humano e produz resultados que não foram individualmente antecipados, embora fossem previsíveis em abstrato. Na terceira, discutida sobretudo em plano especulativo, o sistema atua de modo plenamente autônomo, tomando decisões desvinculadas de qualquer input humano direto (PEREIRA; TEIXEIRA, 2019).

A segunda hipótese esbarra em um obstáculo que a literatura chama de opacidade algorítmica, isto é, a impossibilidade de saber ao certo por que o sistema chegou a determinado resultado. Modelos treinados sobre grandes volumes de dados chegam a resultados por caminhos que nem sempre podem ser reconstruídos de forma inteligível, inclusive por quem os desenvolveu. Sousa (2020) descreve o fenômeno como problema da caixa negra e observa que ele dificulta o estabelecimento da relação de causalidade entre a conduta humana e o resultado desvalioso, questão que voltará a ser tratada adiante.

A mudança de escala trazida pelos modelos generativos merece registro à parte. Falsificações de imagem e de voz sempre existiram, e o direito penal conviveu com elas durante décadas por meio dos crimes de falsidade. O que se alterou foi o custo de produção, a qualidade do resultado e a velocidade de difusão. Um áudio capaz de enganar um familiar próximo pode ser gerado a partir de poucos segundos de gravação obtida em rede social, sem qualquer conhecimento técnico. A massificação desloca o problema do

campo da raridade para o da rotina, e isso repercute sobre a atividade policial, que passa a lidar com volume incompatível com a estrutura disponível de perícia.

Vale registrar um dado que a discussão teórica às vezes deixa de lado. Quase todos os casos que hoje chegam às delegacias e aos tribunais brasileiros se encaixam na primeira hipótese. Há uma pessoa que decide fraudar, humilhar ou extorquir e escolhe a inteligência artificial como meio de execução, do mesmo modo como poderia escolher um programa de edição de imagem ou um documento falsificado. O debate sobre a punição de entes artificiais autônomos, embora teoricamente estimulante, ainda não corresponde ao que se apresenta na prática forense (PAULA; CORNWALL; CABRAL, 2019).

2.2. Pressupostos da Responsabilidade Penal no Ordenamento Brasileiro

A doutrina brasileira, em sua maioria, divide o crime em três elementos: fato típico, ilicitude e culpabilidade. Cada um desses elementos supõe, direta ou indiretamente, a atuação de um ser humano. O fato típico exige conduta, entendida como comportamento voluntário dirigido a uma finalidade, do qual decorre um resultado ligado à ação por nexo de causalidade, nos termos do artigo 13 do Código Penal.

A imputação subjetiva está disciplinada no artigo 18 do Código Penal, que separa o crime doloso, quando o agente quis o resultado ou assumiu o risco de produzi-lo, do crime culposos, quando o resultado decorre de imprudência, negligência ou imperícia. O parágrafo único do mesmo artigo estabelece que ninguém pode ser

punido por fato previsto como crime senão quando o pratica dolosamente, salvo os casos expressos de punição por culpa. O artigo 19 completa o quadro ao condicionar a agravação da pena pelo resultado à sua causação ao menos culposa. O sistema, portanto, rejeita a responsabilidade penal objetiva.

A culpabilidade, na concepção normativa hoje dominante, reúne a imputabilidade, a potencial consciência da ilicitude e a exigibilidade de conduta diversa. O artigo 26 do Código Penal isenta de pena quem, por doença mental ou desenvolvimento mental incompleto ou retardado, era inteiramente incapaz de entender o caráter ilícito do fato ou de determinar-se de acordo com esse entendimento. O artigo 27 declara penalmente inimputáveis os menores de dezoito anos. O artigo 21 trata do erro sobre a ilicitude e o artigo 22 da coação irresistível e da obediência hierárquica.

Aplicados esses critérios a um sistema de computador, a resposta é direta. Falta-lhe conduta em sentido penal, porque não há vontade que se possa qualificar como própria. Falta-lhe imputabilidade, categoria que a lei construiu a partir de referências humanas, como idade e higidez mental. Falta-lhe potencial consciência da ilicitude, pois o processamento estatístico de dados não se confunde com a compreensão do valor de uma norma. A ausência de qualquer desses elementos já basta para afastar a responsabilidade penal do próprio sistema.

Um argumento adicional reforça a conclusão. A responsabilização penal da pessoa jurídica, ente que possui personalidade reconhecida pelo ordenamento, patrimônio e vontade formada por órgãos deliberativos, é admitida no Brasil apenas em caráter excepcional, com fundamento no artigo 225, § 3º, da Constituição

Federal e na Lei nº 9.605/1998, restrita aos crimes ambientais. Se mesmo a pessoa jurídica não responde criminalmente de forma ampla, seria incongruente atribuir responsabilidade penal genérica a um sistema que sequer possui personalidade jurídica (FORNASIER, 2021).

Há ainda a questão da pena. As finalidades atribuídas à sanção penal, sejam elas retributivas ou preventivas, pressupõem um destinatário capaz de sofrer a reprovação e de orientar sua conduta futura a partir dela. Moraes (2023) observa que a punição de programações esbarra na impossibilidade de conferir sentido à pena, uma vez que a desativação de um sistema ou a destruição de seu suporte físico não realiza função de prevenção especial nem satisfaz a expectativa social vinculada ao castigo. O autor adverte que a tentativa de estender o poder punitivo a entes não humanos tende a produzir efeito simbólico, sem ganho real de proteção de bens jurídicos.

Existe ainda a garantia prevista no artigo 5º, inciso XLV, da Constituição Federal, segundo a qual nenhuma pena passará da pessoa do condenado. O dispositivo pressupõe que exista uma pessoa a ser condenada e que a sanção possa ser individualizada em relação a ela. Punir um sistema significaria, na prática, atingir patrimônio de terceiros, sejam os sócios da empresa que o explora, sejam os usuários que dele dependem, o que faria a pena atingir quem não cometeu crime algum e contrariaria de forma direta a garantia constitucional.

2.3. Modelos Doutrinários de Imputação em Condutas Mediadas por Inteligência Artificial

A formulação mais citada sobre o tema é a de Hallevy (2010), que propõe três modelos de imputação penal aplicáveis a entidades de inteligência artificial. O primeiro é o modelo do agente inocente, no qual o sistema funciona como instrumento nas mãos de quem o utiliza, à semelhança do animal adestrado ou da pessoa sem capacidade de compreensão empregada por terceiro para a prática do crime. A responsabilidade recai integralmente sobre o programador ou sobre o usuário, conforme quem tenha determinado a conduta.

O segundo modelo é o da consequência natural e provável. Aplica-se quando o sistema, programado para finalidade lícita, produz resultado ilícito que era previsível para quem o desenvolveu ou operou. Nesse caso, a imputação se aproxima da estrutura da culpa, pois se funda na violação de um dever de cuidado e na previsibilidade objetiva do resultado.

O terceiro modelo, o da responsabilidade direta, sustenta que o próprio sistema poderia ser considerado autor, desde que se lhe reconheçam elementos equivalentes ao ato material e ao elemento subjetivo. Hallevy (2010) admite ainda a combinação dos três modelos, de forma que a responsabilização do ente artificial não excluiria a das pessoas envolvidas em sua criação e utilização.

Aplicados ao direito brasileiro, os dois primeiros modelos funcionam sem que seja preciso mudar a lei. O modelo do agente inocente corresponde, em substância, à autoria mediata, figura reconhecida pela doutrina nacional e pressuposta em dispositivos como o artigo 62, inciso III, do Código Penal. Quem se vale de um sistema de inteligência artificial para produzir uma imagem falsa ou para redigir uma mensagem fraudulenta é autor do crime, sendo o programa

um simples meio de execução, sem diferença estrutural em relação ao emprego de uma câmera fotográfica ou de um documento adulterado.

O modelo da consequência natural e provável também cabe na lei brasileira, com uma ressalva importante: a punição a título culposos depende de previsão legal expressa, por força do artigo 18, parágrafo único, do Código Penal. Como a maior parte dos tipos penais aplicáveis a fraudes e a ofensas praticadas por meios digitais admite apenas a modalidade dolosa, a hipótese de responsabilização culposa do desenvolvedor é mais estreita do que sugere a leitura apressada do modelo.

Uma dificuldade específica surge quando o resultado produzido pelo sistema não corresponde ao que o usuário pediu. Se alguém solicita a criação de uma imagem publicitária e a ferramenta gera material que reproduz feições de pessoa real, expondo-a a situação vexatória, não há dolo quanto ao resultado ofensivo. A hipótese se resolve pela ausência de elemento subjetivo, e não pela criação de categoria nova. O mesmo raciocínio vale quando a ferramenta vai além do que foi pedido. Quem deu o comando responde apenas pelo que quis ou aceitou como risco, do mesmo modo que ocorre quando o comparsa extrapola aquilo que havia sido combinado.

O terceiro modelo é incompatível com o direito penal brasileiro. Além de esbarrar nos requisitos da culpabilidade examinados na seção anterior, ofende o princípio da legalidade estrita, inscrito no artigo 5º, inciso XXXIX, da Constituição Federal e no artigo 1º do Código Penal, porque não há tipo penal que preveja o ente artificial como sujeito ativo. Piló e Brasil (2022), ao examinarem os reflexos do emprego de inteligência artificial na seara criminal, concluem pela

necessidade de limitar, e não de ampliar, o uso de máquinas inteligentes nesse campo, justamente porque o direito penal lida com a liberdade individual e depende de avaliações que a automação não reproduz.

A discussão europeia sobre a criação de uma personalidade eletrônica, examinada por Pereira e Teixeira (2019), não altera essa conclusão. Ainda que se admitisse, no campo civil, a atribuição de personalidade a entes artificiais como técnica de imputação patrimonial e de garantia de reparação às vítimas, a transposição para a esfera penal seria indevida, pois a responsabilidade criminal não se funda na titularidade de patrimônio, e sim na possibilidade de reprovação pessoal da conduta.

2.4. A Repartição da Responsabilidade Entre Usuário, Desenvolvedor e Provedor

Descartada a punição do sistema, resta examinar as pessoas que participam da criação e do uso da tecnologia. A posição mais simples é a do usuário. Quem formula o comando com a finalidade de produzir o resultado típico age com dolo direto e responde como autor, aplicando-se o tipo penal correspondente ao bem jurídico atingido. A circunstância de o texto, a imagem ou o áudio terem sido gerados por um programa não interfere na tipicidade, porque o verbo nuclear dos tipos aplicáveis descreve a conduta de fraudar, de ofender ou de divulgar, e não o modo técnico de produção do material.

A posição do desenvolvedor exige análise mais cuidadosa. A produção de uma ferramenta de uso geral, que serve tanto para fins lícitos quanto ilícitos, está dentro do chamado risco permitido, ou

seja, do risco que a sociedade aceita correr em troca dos benefícios da atividade. Quem fabrica um automóvel não responde pelo homicídio praticado na direção, assim como quem desenvolve um editor de imagens não responde pela falsificação feita por terceiro. A responsabilidade penal do desenvolvedor pressupõe algo mais, como a criação deliberada de sistema destinado especificamente à prática de ilícitos, o que configuraria dolo, ou a violação de dever objetivo de cuidado exigível segundo o estado da técnica, o que remeteria à culpa, sempre condicionada à existência de tipo culposos correspondente.

O provedor que hospeda ou disponibiliza o sistema pode responder por omissão, desde que se enquadre em alguma das hipóteses do artigo 13, § 2º, do Código Penal, que atribui o dever de agir a quem tenha por lei obrigação de cuidado, proteção ou vigilância, a quem de outra forma tenha assumido a responsabilidade de impedir o resultado e a quem, com seu comportamento anterior, tenha criado o risco da ocorrência do resultado. A simples disponibilização de uma ferramenta ao público não configura, por si só, posição de garantidor. A inércia deliberada diante de comunicação específica sobre uso criminoso do serviço, por outro lado, aproxima o caso da segunda e da terceira hipóteses do dispositivo.

Quando mais de uma pessoa concorre para o fato, incide o artigo 29 do Código Penal, segundo o qual quem, de qualquer modo, concorre para o crime incide nas penas a este cominadas, na medida de sua culpabilidade. O concurso de pessoas depende, contudo, de liame subjetivo entre os envolvidos. A ausência desse vínculo impede que se trate como partícipe o desenvolvedor que jamais teve conhecimento do uso indevido de sua ferramenta.

Para que exista crime por omissão nesses casos, é preciso, além do dever jurídico de agir, que a pessoa tivesse condições reais de evitar o resultado e soubesse o que estava acontecendo. Em ambientes digitais de larga escala, a demonstração desses dois elementos costuma ser problemática, pois o volume de conteúdo processado inviabiliza controle individualizado prévio. A situação muda quando existe comunicação específica e verificável sobre determinado conteúdo ou determinada conta, hipótese em que a inércia passa a ser voluntária e consciente, aproximando-se do dolo eventual.

Também é preciso separar o dolo eventual da culpa consciente na conduta de quem disponibiliza a ferramenta. Age com dolo eventual quem prevê o resultado como possível e o aceita, permanecendo indiferente à sua produção. Age com culpa consciente quem prevê o resultado, mas acredita sinceramente que ele não ocorrerá, confiando em medidas de contenção adotadas. A diferença, que na prática se apura por elementos objetivos como a existência de filtros, de canais de denúncia e de resposta a notificações anteriores, decide entre a punição por crime doloso e a atipicidade, quando não houver modalidade culposa prevista.

Sousa (2020) faz uma ressalva importante quanto ao alcance dessa dificuldade. Segundo a autora, a impossibilidade de reconstruir o mecanismo concreto que levou ao resultado não é problema inteiramente novo para o direito penal, pois já havia sido enfrentado nos casos de responsabilidade criminal pelo produto, em que os tribunais reconheceram o nexo causal mesmo sem saber qual substância exata havia provocado a lesão. O que há de novo estaria na definição da conduta proibida e do limite de risco aceitável diante de uma tecnologia em transformação, tarefa que cabe primeiro aos órgãos reguladores e só depois ao legislador penal.

O ponto mais frágil na prática não é teórico, e sim de prova. A cadeia tecnológica costuma envolver dezenas de agentes, entre quem coleta os dados de treinamento, quem ajusta o modelo, quem oferece a infraestrutura de processamento e quem opera a interface final, muitas vezes em jurisdições distintas. A dispersão dificulta identificar a contribuição individual determinante para o resultado. Soma-se a isso o uso de conexões anônimas, de contas falsas e de servidores mantidos fora do território nacional, hipótese que o próprio legislador reconheceu ao prever causas de aumento de pena no artigo 155, § 4º-C, inciso I, e no artigo 171, § 2º-B, do Código Penal, ambos incluídos pela Lei nº 14.155/2021 (BRASIL, 2021).

Existe risco real de que essa dificuldade de prova leve a soluções que, na aparência, respeitam a lei, mas que na prática criam responsabilidade penal objetiva. Presumir o dolo do desenvolvedor a partir da mera potencialidade lesiva da ferramenta, ou responsabilizar o provedor pelo simples fato de operar o serviço, significaria abandonar a exigência de imputação subjetiva que o artigo 18 do Código Penal consagra. Gomes, Silva e Domingos (2025), ao analisarem casos de manipulação de imagens, registram que a fragmentação da cadeia de agentes e o despreparo técnico das estruturas de investigação respondem por boa parte da impunidade observada, e não a inexistência de norma aplicável.

2.5. O Tratamento Normativo Brasileiro: Dos Tipos Vigentes à Lei Nº 15.123/2025

Parte da produção recente afirma que existiria um vazio na lei quanto aos crimes praticados com inteligência artificial. A afirmação merece exame cuidadoso. Boa parte das condutas hoje observadas

já encontra tipificação no ordenamento, sem necessidade de analogia.

Quem utiliza voz sintetizada ou vídeo manipulado para induzir a vítima a erro e obter vantagem ilícita praticando estelionato, na forma qualificada do artigo 171, § 2º-A, do Código Penal, que prevê reclusão de quatro a oito anos quando a fraude é cometida com informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. A subtração de valores mediante acesso fraudulento a conta bancária atrai o artigo 155, § 4º-B, com a mesma escala penal. Ambos os dispositivos foram inseridos pela Lei nº 14.155/2021 (BRASIL, 2021).

A produção e a divulgação de vídeos falsos com o objetivo de atribuir fato criminoso a alguém, de imputar fato ofensivo à reputação ou de ofender a dignidade caracterizam, respectivamente, calúnia, difamação e injúria, previstas nos artigos 138 a 140 do Código Penal. A atribuição de identidade alheia mediante material sintético pode configurar falsa identidade, nos termos do artigo 307, e a inserção de declaração falsa em documento com efeitos jurídicos pode caracterizar falsidade ideológica, na forma do artigo 299. A ameaça de divulgação de material fabricado, com exigência de vantagem, configura extorsão, tipificada no artigo 158.

Merece destaque o artigo 241-C do Estatuto da Criança e do Adolescente, que pune com reclusão de um a três anos, e multa, a conduta de simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra

forma de representação visual. O parágrafo único estende as mesmas penas a quem vende, disponibiliza, distribui, publica, divulga, adquire, possui ou armazena o material produzido. O dispositivo foi introduzido em 2008, muito antes da popularização das ferramentas atuais, e alcança de forma direta o material sexual infantil produzido por inteligência artificial, o que demonstra que a redação técnica e aberta quanto ao meio de execução tende a envelhecer melhor do que a descrição minuciosa de tecnologias específicas.

A primeira menção expressa à inteligência artificial no Código Penal brasileiro veio com a Lei nº 15.123, de 24 de abril de 2025, que acrescentou parágrafo único ao artigo 147-B para estabelecer que a pena do crime de violência psicológica contra a mulher é aumentada de metade se o delito é cometido mediante uso de inteligência artificial ou de qualquer outro recurso tecnológico que altere imagem ou som da vítima (BRASIL, 2025). A alteração responde ao uso de material sintético como instrumento de humilhação e de controle no contexto de violência doméstica e familiar.

A redação escolhida pelo legislador, porém, merece crítica. A causa de aumento equipara, para efeito de agravamento, o emprego de inteligência artificial e o de qualquer outro recurso tecnológico apto a alterar imagem ou som, fórmula que abrange desde modelos generativos sofisticados até aplicativos elementares de edição. A amplitude dessa expressão enfraquece a exigência de clareza que decorre do princípio da legalidade e transfere ao juiz a tarefa de definir qual meio tecnológico justifica o aumento da pena e qual não justifica.

No plano da regulação geral, o Projeto de Lei nº 2.338/2023 organiza o tratamento da matéria a partir da classificação dos sistemas por nível de risco, com inspiração declarada no Regulamento (UE) 2024/1689 da União Europeia, o chamado Ato de Inteligência Artificial (UNIÃO EUROPEIA, 2024). O projeto estabelece direitos das pessoas afetadas, deveres de transparência e sanções administrativas, sem criar tipos penais novos. A escolha faz sentido, porque a maior parte dos riscos ligados ao uso de inteligência artificial se resolve com regras de controle e fiscalização, e não com a criação de novos crimes (FRAZÃO; MULHOLLAND, 2019).

Fora do Código Penal, a experiência mais consolidada de disciplina do tema veio da Justiça Eleitoral. A Resolução nº 23.732/2024 do Tribunal Superior Eleitoral alterou a Resolução nº 23.610/2019 para proibir, na propaganda eleitoral, o uso de conteúdo sintético em áudio ou vídeo destinado a criar, substituir ou alterar imagem ou voz de pessoa viva, falecida ou fictícia com o objetivo de prejudicar ou favorecer candidatura, além de exigir aviso explícito quando houver emprego lícito de inteligência artificial e de restringir o uso de robôs que simulem diálogo com candidato (BRASIL, 2024). As sanções previstas são de natureza eleitoral, como a cassação do registro ou do mandato, sem prejuízo da eventual incidência do artigo 323 do Código Eleitoral, que pune a divulgação, na propaganda, de fatos que o agente sabe inverídicos e capazes de influenciar o eleitorado. Leite e Azeredo (2025), ao examinarem a aplicação da resolução pelos Tribunais Regionais Eleitorais nas eleições de 2024, concluem que a norma ofereceu fundamento jurídico suficiente para que juízes eleitorais determinassem a retirada de conteúdos manipulados, o que sugere que a via regulatória produziu resposta mais rápida do que a penal.

O conjunto normativo examinado revela um padrão. Quando o legislador ou o regulador descreve a conduta pelo resultado lesivo, e não pela tecnologia empregada, a norma permanece aplicável ao longo do tempo, como demonstra o artigo 241-C do Estatuto da Criança e do Adolescente. Quando opta por nomear a ferramenta, produz norma que envelhece com ela e que tende a exigir sucessivas atualizações.

2.6. Limites da Resposta Penal e Alternativas de Regulação

A reação legislativa a fatos de grande repercussão costuma seguir um padrão conhecido, que consiste em criar tipos penais ou majorar penas como forma de demonstrar preocupação com o problema. Morais (2023) chama atenção para o caráter expansionista desse movimento e para a distância entre o efeito simbólico da nova norma e sua eficácia protetiva concreta. No caso da inteligência artificial, o diagnóstico ganha reforço, porque a dificuldade central identificada ao longo desta pesquisa não está na ausência de tipo penal, e sim na identificação do autor e na produção da prova.

Aumentar penas não resolve investigação deficiente. A responsabilização efetiva de quem se vale de inteligência artificial para delinquir depende de estrutura de perícia digital, de capacidade de rastreamento de conteúdo sintético e de cooperação internacional para obtenção de dados armazenados no exterior. Sem esse investimento, a norma penal permanece em vigor e sem aplicação.

O caminho regulatório oferece instrumentos que o direito penal não tem condições de fornecer. A obrigação de identificar conteúdos gerados artificialmente, a exigência de registro e de documentação

dos sistemas classificados como de alto risco, os deveres de auditoria e a previsão de sanções administrativas proporcionais ao faturamento do infrator atuam antes da consumação do dano e alcançam pessoas jurídicas que o direito penal brasileiro não pode responsabilizar fora da matéria ambiental. A responsabilidade civil, por sua vez, garante reparação às vítimas independentemente da identificação do agente doloso, mediante a distribuição do risco entre os que exploram economicamente a atividade.

Isso não significa afastar por completo a intervenção penal. Há espaço legítimo para aperfeiçoamento pontual, desde que se preserve a taxatividade. Uma agravante genérica de emprego de meio tecnológico apto a dificultar a identificação do autor, por exemplo, seria mais adequada do que a multiplicação de causas de aumento vinculadas a tecnologias determinadas, que envelhecem rapidamente e produzem lacunas quando surge a próxima ferramenta.

Sousa (2020) encerra sua análise com um alerta importante. O uso das novas tecnologias pelo sistema de justiça criminal pode conduzir, em poucos passos, a um direito penal securitário, voltado ao agente tido como perigoso e não ao fato praticado, com sacrifício de direitos fundamentais em nome da prevenção. O alerta vale igualmente para a tentação de antecipar a tutela penal contra desenvolvedores e plataformas antes de qualquer resultado lesivo concreto.

Existe ainda um aspecto de política criminal que costuma passar despercebido. A criação de tipos penais amplos em matéria tecnológica produz efeito colateral sobre atividades legítimas. Pesquisadores em segurança da informação, jornalistas que

produzem material paródico devidamente identificado e profissionais que utilizam síntese de voz para acessibilidade podem ver suas condutas alcançadas por descrições típicas mal delimitadas. A exigência de que o tipo penal seja claro e bem delimitado, nesse ponto, não é apego teórico. É a condição para que a lei alcance quem pretende causar dano e não puna quem usa a mesma tecnologia para finalidade lícita.

3. CONSIDERAÇÕES FINAIS E RESULTADOS

A pesquisa investigou quem responde criminalmente pelo uso indevido de sistemas de inteligência artificial e de que modo as categorias da imputação penal previstas no Código Penal brasileiro permitem alcançar cada um dos agentes envolvidos, com o objetivo de analisar os limites e as possibilidades dessa imputação no ordenamento pátrio.

O exame dos pressupostos da responsabilidade penal mostrou que o sistema de inteligência artificial não reúne as condições exigidas para figurar como sujeito ativo de crime. Faltam-lhe conduta em sentido penal, imputabilidade e potencial consciência da ilicitude, e a pena aplicada a um programa não realizaria qualquer das funções que a sanção criminal desempenha. A comparação com o regime excepcional da responsabilidade penal da pessoa jurídica confirmou a conclusão.

A análise dos modelos doutrinários indicou que dois dos três modelos formulados por Hallevy operam no direito brasileiro sem reforma legislativa. O modelo do agente inocente corresponde à autoria mediata e resolve a grande maioria dos casos concretos, nos quais o sistema é meio de execução escolhido por quem decide

delinquir. O modelo da consequência natural e provável reproduz a estrutura da culpa, com o limite da exigência de previsão legal expressa da modalidade culposa. O modelo da responsabilidade direta é incompatível com a legalidade estrita e com a culpabilidade.

A verificação do tratamento normativo revelou que a alegada lacuna é menor do que se costuma afirmar. Estelionato na forma do artigo 171, § 2º-A, furto mediante fraude eletrônica do artigo 155, § 4º-B, crimes contra a honra, falsa identidade, falsidade ideológica, extorsão e a simulação prevista no artigo 241-C do Estatuto da Criança e do Adolescente já alcançam as condutas mais frequentes. A Lei nº 15.123/2025 introduziu a primeira referência expressa à inteligência artificial no Código Penal, com técnica legislativa que merece reparo quanto à amplitude da cláusula final.

A resposta ao problema de pesquisa é, portanto, a seguinte: respondem criminalmente pelo uso indevido de sistemas de inteligência artificial as pessoas naturais que deles se valem, tanto na condição de autores diretos e mediatos quanto, em hipóteses restritas, na condição de partícipes ou de garantidores omissos, mas não autorizam a punição do sistema em si nem a presunção de dolo ou de culpa dos desenvolvedores a partir da simples potencialidade lesiva da ferramenta.

A pesquisa tem limitações que precisam ser registradas. A análise foi feita em plano teórico e documental, sem levantamento de decisões judiciais brasileiras sobre o tema, o que impede afirmar como os tribunais vêm efetivamente resolvendo esses casos. A tramitação do Projeto de Lei nº 2.338/2023 seguia inconclusa no período de elaboração do texto, de modo que as considerações a ele relativas dependem de confirmação quanto à redação final aprovada.

Como perspectiva para investigações futuras, sugere-se o levantamento empírico de inquéritos e de decisões que envolvam o uso de inteligência artificial na prática de crimes, com o objetivo de verificar quais tipos penais têm sido efetivamente aplicados e quais obstáculos probatórios se repetem. Também se mostra promissor o estudo comparado entre a solução brasileira e a europeia quanto aos deveres de identificação de conteúdo sintético e seus reflexos sobre a apuração da autoria.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Rio de Janeiro: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 8 set. 2026.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021.** Altera o Decreto-Lei nº 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: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 8 set. 2026.

BRASIL. **Lei nº 15.123, de 24 de abril de 2025.** Altera o art. 147-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para estabelecer causa de aumento de pena no crime de violência psicológica contra a mulher quando praticado com o uso de inteligência artificial ou de qualquer outro recurso tecnológico que altere imagem ou som da vítima. Brasília: Presidência da República,

2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15123.htm. Acesso em: 8 set. 2026.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 8 set. 2026.

BRASIL. Senado Federal. **Projeto de Lei nº 2.338, de 2023.** Dispõe sobre o uso da inteligência artificial. Brasília: Senado Federal, 2023. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 8 set. 2026.

BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.732, de 27 de fevereiro de 2024.** Altera a Resolução-TSE nº 23.610, de 18 de dezembro de 2019, que dispõe sobre propaganda eleitoral, utilização e geração do horário gratuito e condutas ilícitas em campanha eleitoral. Brasília: Tribunal Superior Eleitoral, 2024.

FORNASIER, Mateus de Oliveira. **A inteligência artificial como pessoa? Responsabilidade e personalidade de entes artificiais e o direito brasileiro.** Londrina: Thoth, 2021.

FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência artificial e direito: ética, regulação e responsabilidade.** São Paulo: Thomson Reuters Brasil, 2019.

GOMES, Lucas Lima; SILVA, Rosana Reis de Melo; DOMINGOS, Leda Mourão. A responsabilidade civil e penal pelo uso de inteligência artificial na manipulação de imagens com fins ilícitos. **Cognitio**

Juris, v. 15, n. 58, 2025. Disponível em: <https://cognitiojuris.com.br/a-responsabilidade-civil-e-penal-pelo-uso-de-inteligencia-artificial-na-manipulacao-de-imagens-com-fins-ilicitos/>. Acesso em: 8 set. 2026.

HALLEVY, Gabriel. The criminal liability of artificial intelligence entities: from science fiction to legal social control. **Akron Intellectual Property Journal**, Akron, v. 4, n. 2, p. 171-201, 2010. Disponível em: <https://ideaexchange.uakron.edu/akronintellectualproperty/vol4/iss2/1/>. Acesso em: 8 set. 2026.

LEITE, Rodrigo de Almeida; AZEREDO, Sarah da Silva. A regulamentação do uso da inteligência artificial pela Resolução-TSE n. 23.732/2024 e sua aplicação pelos Tribunais Regionais Eleitorais nas Eleições 2024. **Estudos Eleitorais**, Brasília, v. 19, n. 1, e20253, 2025. DOI: https://doi.org/10.57025/14145146_v19n1_lei.rod. Acesso em: 8 set. 2026.

MORAIS, Renato Watanabe de. Programações podem ser punidas? Responsabilidade penal em decisões tomadas pela inteligência artificial. **Revista Científica do CPJM**, Rio de Janeiro, v. 2, n. 7, p. 130-148, 2023. Disponível em: <https://rcpjm.emnuvens.com.br/revista/article/view/217>. Acesso em: 8 set. 2026.

PAULA, Alice Lima de; CORNWALL, Bruno Meirelles de M.; CABRAL, Dalila M. Breves reflexões sobre a inteligência artificial e seus impactos no campo do Direito Penal. In: CHAVES, Natália Cristina (org.). **Direito, tecnologia e globalização**. Porto Alegre: Editora Fi, 2019. p. 98-117.

PEREIRA, Uiara Vendrame; TEIXEIRA, Tarcísio. Inteligência artificial: a quem atribuir responsabilidade? **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 20, n. 2, p. 119-142, maio/ago. 2019.

PILÓ, Xenofontes Curvelo; BRASIL, Deilton Ribeiro. A utilização da inteligência artificial no direito penal e seus reflexos nas garantias e direitos fundamentais. **Revista EJEJF**, Belo Horizonte, ano 1, n. 1, p. 269-299, jul./dez. 2022. Disponível em: https://ejef.tjmg.jus.br/wp-content/uploads/2023/01/artigo_10.pdf. Acesso em: 8 set. 2026.

SOUSA, Susana Aires de. Um direito penal desafiado pelo desenvolvimento tecnológico: alguns exemplos a partir das neurociências e da inteligência artificial. **Revista da Defensoria Pública da União**, Brasília, n. 14, p. 21-37, jul./dez. 2020. Disponível em:

https://bdjur.stj.jus.br/jspui/bitstream/2011/150439/direito_penal_desafiado_sousa.pdf. Acesso em: 8 set. 2026.

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

¹ Acadêmico do curso de Direito da Faculdade de Educação Santa Terezinha (FEST). E-mail: [acesse o artigo original para visualizar o e-mail](#).

² Docente orientadora e coautora. Advogada. Professora. Bacharel em direito pela Universidade Federal do Maranhão (UFMA). Licenciada em Filosofia (UniBF). Especialista em Direito Tributário (UniBF). Pós-graduanda em Direito Penal. Professora do curso de

Direito da Faculdade de Educação Santa Terezinha (FEST). E-mail:

[acesse o artigo original para visualizar o e-mail.](#)