

RESPONSABILIDADE PENAL POR ATOS COMETIDOS POR SISTEMAS DE INTELIGÊNCIA ARTIFICIAL E SEU ENQUADRAMENTO COMO CRIME DE EMPRESA: desafios e perspectivas no direito penal brasileiro

CRIMINAL LIABILITY FOR ACTS COMMITTED BY ARTIFICIAL INTELLIGENCE SYSTEMS AND THEIR CLASSIFICATION AS CORPORATE CRIMES: Challenges and Perspectives in Brazilian Criminal Law

Ana Katia Araújo de Mesquita¹
Francisca Diva Lopes Carvalho²
Maria Rayssa da Silva Alves³
Tatiane Rego de Carvalho⁴
Alessandra Almeida Barros⁵

RESUMO

O artigo analisa a responsabilidade penal por atos cometidos por sistemas de Inteligência Artificial (IA), destacando os desafios jurídicos diante das inovações tecnológicas. Defende a responsabilidade humana e corporativa penalizando os atos produzidos pela IA no âmbito do Direito Penal, reconhecendo-a como Cegueira Deliberada. A pesquisa é qualitativa, bibliográfica e documental.

Palavras-chave: Crime de Empresa. Imputação Objetiva. Inteligência Artificial. Responsabilidade Penal.

ABSTRACT

This article analyzes criminal liability for acts committed by Artificial Intelligence (AI) systems, highlighting the legal challenges posed by technological innovations. It advocates for human and corporate liability by penalizing acts produced by AI under Criminal Law, recognizing it as Willful Blindness. The research is qualitative, bibliographical, and documentary.

Keywords: Corporate Crime. Objective Imputation. Artificial Intelligence. Criminal Liability.

¹ Aluna do curso de bacharelado em Direito da Faculdade Princesa do Oeste. Email: anakatiamesquita@hotmail.com.

² Aluna do curso de bacharelado em Direito da Faculdade Princesa do Oeste. E-mail: divalopes.lopes@hotmail.com

³ Aluna do curso de bacharelado em direito da Faculdade Princesa do Oeste. E-mail: alves.rayssafacul@gmailcom

⁴ Aluna do curso de bacharelado em direito da Faculdade Princesa do Oeste. E-mail: carvalhootatianeelive.com

⁵ Professora do curso de direito da Faculdade Princesa do Oeste. E-mail: alessandra.almeida@fpo.edu.br

1 INTRODUÇÃO

Nas últimas décadas, a tecnologia tem avançado significativamente com a popularização da Inteligência Artificial (IA), promovendo transformações profundas não só no Brasil, mas no mundo.

A crescente integração da IA em setores sensíveis como segurança pública, saúde e justiça levanta questionamentos jurídicos fundamentais, especialmente no âmbito da responsabilidade penal. Sistemas de IA, como os de reconhecimento facial e automação decisória no Judiciário, são empregados para otimizar processos, mas a imprevisibilidade de seus resultados (black box)⁶ desafia o Direito Penal clássico.

Então, como responsabilizar penalmente ações ou omissões decorrentes de sistemas que necessitam de consciência e capacidade volitiva? Quem deve ser o sujeito ativo no âmbito penal: o programador, o operador, o gestor corporativo, ou a própria empresa?

A dogmática penal brasileira, ancorada nos princípios constitucionais da legalidade (art. 5º, XXXIX da CF) e da pessoalidade da pena (art. 5º, XLV da CF), exige uma conduta humana voluntária e culpável para a imputação.

Diante desses desafios e da natureza subsidiária e fragmentária do Direito Penal, este artigo visa analisar a responsabilidade penal por atos cometidos por sistemas de IA no contexto jurídico brasileiro.

A solução dogmática para o problema reside na aplicação da Imputação Objetiva e da Teoria da Cegueira Deliberada, concentrando a responsabilidade na falha humana ou corporativa em gerir o risco tecnológico previamente à ocorrência do dano, enquadrando o dano algorítmico como um "crime de empresa".

Partindo desses apontamentos, o presente estudo tem como objetivo geral Identificar a forma de penalização de atos produzidos pela Inteligência Artificial (IA) e suas formas de penalização no âmbito do Direito Penal, propondo o enquadramento do dano algorítmico como crime de empresa.

⁶ Black box também conhecido como caixa preta é um termo usado para descrever sistemas cujo funcionamento interno não é transparente ou compreensível para os usuários, desenvolvedores ou até especialistas.

2 METODOLOGIA

A presente investigação adota uma abordagem qualitativa e jurídico-dogmática, voltada à compreensão crítica e interpretativa dos desafios que a Inteligência Artificial (IA) impõe ao Direito Penal brasileiro.

A escolha por esse tipo de abordagem justifica-se pela necessidade de analisar o fenômeno em sua complexidade normativa, dogmática e tecnológica, privilegiando a interpretação dos fundamentos constitucionais e penais diante da inovação tecnológica, em detrimento da quantificação de dados empíricos.

2.1 Coleta de Dados

A coleta de dados foi realizada por meio de pesquisa bibliográfica, normativa e jurisprudencial. A pesquisa bibliográfica consistiu no levantamento e análise de obras clássicas e contemporâneas da dogmática penal, como as de Cezar Roberto Bitencourt, Rogério Greco, Guilherme de Souza Nucci, Claus Roxin e Jesús-María Silva Sánchez, além de literatura especializada em Direito e Tecnologia, com ênfase nos riscos algorítmicos e na responsabilidade penal corporativa.

A pesquisa normativa envolveu o estudo da Constituição Federal, do Código Penal e de legislações correlatas, como a análise do Projeto de Lei nº 2338/2023, que propõe um marco regulatório para a IA no Brasil. Já a pesquisa jurisprudencial abrangeu o exame de decisões paradigmáticas do Supremo Tribunal Federal (STF) e de tribunais superiores, especialmente aquelas relacionadas à proteção de direitos fundamentais e à responsabilidade penal em contextos de risco tecnológico, como a ADPF 635.

2.2 Critérios de Seleção

Os critérios de seleção das fontes priorizaram a relevância teórica, a pertinência temática e a atualidade das discussões. Foram escolhidos autores que oferecem referenciais fundamentais para a compreensão da responsabilidade penal

e da imputação objetiva, bem como obras e decisões que dialogam diretamente com a problemática da IA e da responsabilidade penal corporativa.

2.3 Análise dos Dados

A análise dos dados foi conduzida de forma interpretativa e crítica, articulando os referenciais dogmáticos com os elementos normativos e jurisprudenciais selecionados. O procedimento consistiu em identificar categorias analíticas como imputação objetiva, cegueira deliberada, responsabilidade penal da pessoa jurídica e dano algorítmico, relacionando-as às condições concretas de aplicação do Direito Penal em face da IA.

Essa estratégia metodológica permitiu compreender a ambivalência do fenômeno: de um lado, a necessidade de responsabilização diante dos riscos tecnológicos; de outro, os limites impostos pelas garantias fundamentais e pela ausência de legislação penal específica sobre IA.

3 REFERENCIAL TEÓRICO

3.1. Responsabilidade Penal no Ordenamento Brasileiro

O Direito Penal brasileiro é estruturado sobre fundamentos constitucionais essenciais, que exigem a presença de um fato típico, ilícito e culpável, tendo como ponto de partida a conduta humana voluntária (Nucci, 2023).

Nesse sentido, a Inteligência Artificial (IA) não pode ser considerada sujeito ativo de crime, pois não possui vontade, discernimento, personalidade jurídica ou capacidade de culpabilidade. Embora seja capaz de produzir resultados autônomos, tais resultados não decorrem de intencionalidade, mas de programação e processamento algorítmico, o que afasta a noção de conduta humana.

Assim, inexistente, na dogmática penal contemporânea, previsão que permita responsabilizar penalmente as máquinas por seus erros ou efeitos indesejados (Bitencourt, 2023).

Atualmente, a responsabilização penal recai exclusivamente sobre agentes humanos ou pessoas jurídicas que desenvolvem, implementam ou utilizam sistemas de IA. No caso das pessoas físicas, a imputação pode ocorrer quando houver dolo ou culpa na concepção, implementação ou utilização da tecnologia.

Já no caso das pessoas jurídicas, a Constituição Federal (art. 225, §3º) e legislações específicas, como a Lei nº 9.605/1998 (crimes ambientais) e a Lei nº 12.846/2013 (Lei Anticorrupção), admitem a responsabilização penal e administrativa da empresa, ainda que de forma restrita a determinados contextos.

No campo legislativo, o Projeto de Lei nº 2338/2023, em tramitação no Senado Federal, busca instituir um marco legal para a IA no Brasil. Todavia, o texto não prevê regras específicas de responsabilidade penal, limitando-se a estabelecer princípios de governança, transparência e mitigação de riscos. Isso demonstra que, até o momento, não há previsão normativa que permita responsabilizar penalmente a IA em si, mas apenas os agentes humanos e corporativos que a controlam.

A doutrina penal contemporânea tem se dividido quanto à necessidade de expansão da responsabilidade penal diante dos riscos tecnológicos. Para Pierpaolo Bottini (2021), a responsabilização penal da pessoa jurídica em crimes de risco difuso é uma tendência global, especialmente em contextos de alta complexidade tecnológica.

Por outro lado, autores como Silva Sánchez (2013) e Zaffaroni (2018) alertam para o risco de uma expansão simbólica do Direito Penal, que, ao tentar abarcar fenômenos tecnológicos sem previsão legal clara, pode violar garantias fundamentais e gerar insegurança jurídica.

Diante desse cenário, torna-se urgente o aprofundamento do debate entre juristas, legisladores e operadores do Direito, a fim de delimitar responsabilidades em atividades de alto risco e prever mecanismos adequados de imputação. A ausência de legislação penal específica sobre IA impõe a necessidade de soluções dogmáticas que conciliem a proteção de bens jurídicos fundamentais com a preservação das garantias constitucionais, evitando tanto a impunidade quanto a hipertrofia penal.

3.2 Teorias de Imputação Penal Adaptadas

A Teoria do Domínio do Fato (TDF), desenvolvida por Claus Roxin (2000), é especialmente relevante em crimes de organização e estruturas hierárquicas, como os chamados “crimes de empresa”, tendo sido inclusive adotada pelo Supremo Tribunal Federal no julgamento da Ação Penal 470.

Contudo, para crimes de omissão de vigilância e, sobretudo, no contexto da Inteligência Artificial avançada, em especial sistemas de *machine learning* com autonomia decisória, a TDF apresenta limitações, pois exige o controle final sobre o fato criminoso.

Quando o dano decorre de um desvio algorítmico imprevisível (black box), torna-se difícil comprovar que o dirigente detinha o domínio final sobre a execução do delito. Assim, a TDF deve ser vista como uma ferramenta auxiliar, útil apenas para definir a posição de garantidor no âmbito empresarial.

Dessa forma, ainda que seja possível conceber determinadas formas de IA que possuam crenças, desejos e intenções, uma solução proposta na literatura é que a legislação limite esse nível de autonomia dos sistemas, de modo a evitar a transferência indevida de responsabilidade penal para entes não humanos (Farnosier, 2022).

Em uma pequena contextualização da TDF, relacionando-a com a AP 470 do Supremo Tribunal Federal (STF), pode-se inferir que esta teoria serviu como base para que os magistrados responsabilizassem líderes por esquema de corrupção, bem como propiciou o afastamento da alegação de inépcia da denúncia e condenou o Ministro Chefe da Casa Civil à época, por corrupção ativa, entendendo que quem controla uma organização criminosa é que detém o seu controle, mesmo que não participe materialmente do seu ato, o que gerou muitas controvérsias⁷ (Maia e Lobato, 2023).

Em contraste, a Teoria da Imputação Objetiva (TIO) mostra-se central para a responsabilidade penal em cenários de risco tecnológico. A imputação é viável quando o agente humano cria ou incrementa um risco proibido, decorrente da

⁷ A teoria do domínio do fato, que diferencia autor de partícipe, foi aplicada de forma controversa, pois o STF poderia ter condenado indivíduos como partícipes, logo, com penas menores.

violação de um dever de cuidado, e esse risco se concretiza no resultado, desde que o resultado esteja dentro do âmbito de proteção da norma penal.

A Teoria da Imputação Objetiva desloca o foco donexo causal para onexo de risco, permitindo responsabilizar programadores, operadores ou gestores que, ao não adotarem medidas de segurança ou governança adequadas, contribuíram para a ocorrência do dano algorítmico.

Como destaca Guimarães (2016), a imputação objetiva estabelece que só é atribuível a alguém o resultado de uma conduta que cria um risco juridicamente relevante e proibido, e que tal resultado seja previsível e direcionado pela vontade do agente.

Por fim, a Teoria da Cegueira Deliberada (*Willful Blindness*) permite imputar o dolo eventual a indivíduos ou gestores que, suspeitando ou tendo conhecimento da alta probabilidade de risco ilícito, como falhas de bias algorítmico ou ausência de auditoria em sistemas de IA, optam por ignorá-lo.

Essa omissão de vigilância, quando consciente, caracteriza aceitação do risco e, portanto, dolo eventual. Como observa França (2019), a cegueira deliberada consiste na conduta daquele que, consciente da possibilidade de um resultado ilícito, opta por não investigar para se eximir de responsabilidade, assumindo o risco de sua ocorrência.

Assim, embora a TDF tenha relevância dogmática e histórica, é a combinação entre a Imputação Objetiva e a Cegueira Deliberada que oferece maior potencial para enfrentar os desafios da responsabilidade penal no contexto da Inteligência Artificial, ao permitir a responsabilização de agentes humanos e corporativos sem violar os princípios constitucionais da legalidade e da pessoalidade da pena.

3.2. Inteligência Artificial no Contexto Regulatório Brasileiro (2025)

Com a crescente utilização da Inteligência Artificial (IA) em setores estratégicos do cotidiano, como segurança pública, saúde e relações de consumo, torna-se indispensável a criação de um marco regulatório sólido que assegure a proteção dos usuários e promova o uso responsável dessas tecnologias. A

regulação deve garantir não apenas os benefícios sociais e econômicos da IA, mas também mecanismos claros de responsabilização civil e penal em casos de abuso ou falha sistêmica.

O Projeto de Lei nº 2338/2023, atualmente em tramitação, propõe a classificação dos sistemas de IA de acordo com o grau de risco, estabelecendo categorias como “alto risco”, sujeitas a obrigações mais rígidas de prevenção de danos, gestão de riscos, transparência e compliance.

Esse modelo de regulação por risco, já utilizado no direito administrativo e civil, representa uma inovação importante ao ser aplicado ao campo penal. Contudo, apesar de seu potencial, o projeto ainda não foi aprovado, e a demora legislativa tem gerado um vácuo normativo preocupante.

Essa morosidade legislativa abre espaço para inúmeras brechas jurídicas. Em primeiro lugar, o PL não define de forma clara quem deve ser responsabilizado em caso de falhas graves: se o programador, o operador, o gestor corporativo ou a própria pessoa jurídica. Essa indefinição compromete a efetividade da responsabilização penal e civil, deixando em aberto a possibilidade de impunidade.

Em segundo lugar, o texto não enfrenta de maneira suficiente os problemas relacionados à opacidade algorítmica (*black box*), que dificulta a prova do nexo causal e a imputação de responsabilidade.

Além disso, a ausência de previsão específica sobre a responsabilidade penal da pessoa jurídica em casos de dano algorítmico reforça a insegurança jurídica, já que o ordenamento brasileiro ainda é restritivo quanto à responsabilização penal de empresas fora do campo ambiental.

Especialistas têm criticado o PL 2338/2023 justamente por sua falta de clareza e objetividade. Segundo análise publicada pelo Consultor Jurídico, quatro pontos permanecem polêmicos: a definição de sistema de IA, a criação de um *sandbox* regulatório, a exigência de intervenção humana e a delimitação dos papéis entre humanos e sistemas automatizados.

Da mesma forma, em audiência pública no Senado, especialistas apontaram que o projeto foca excessivamente nos riscos, mas não enfrenta de forma equilibrada as potencialidades e os impactos sociais da IA.

Portanto, embora o PL 2338/2023 represente um passo inicial, sua demora em ser aprovado e suas lacunas normativas comprometem a segurança jurídica e a proteção de direitos fundamentais. A ausência de regras claras sobre responsabilidade penal e civil em casos de falhas de IA deixa a sociedade vulnerável, exigindo não apenas celeridade legislativa, mas também um debate mais profundo e crítico sobre os limites e deveres dos agentes envolvidos na criação e utilização dessas tecnologias.

4. RESULTADOS E DISCUSSÕES

4.1. Problemas Penais e o Crime de Algoritmo como Crime de Empresa

O grande desafio dogmático é a ausência de um sujeito ativo tradicional na IA. Para superar a dificuldade em individualizar a conduta e o nexo causal em cadeias complexas de desenvolvimento, a solução mais robusta é tratar o "crime de algoritmo" como um "crime de empresa" (Prado, 2017).

Embora a responsabilidade penal da Pessoa Jurídica seja exceção no ordenamento brasileiro (aplicada primariamente em crimes ambientais, Lei nº 9.605/98), essa abordagem desloca o foco para a falha sistêmica na gestão do risco e na organização da vigilância por parte dos dirigentes da pessoa jurídica.

O instrumental penal dos crimes societários torna-se aplicável, permitindo responsabilizar os gestores que detêm a posição de garantidor em virtude do controle que exercem sobre a organização e as políticas de *compliance*, independentemente de terem praticado o ato material.

4.2. Jurisprudência, Viés Algorítmico e a Subsidiariedade Penal

Casos práticos como as prisões equivocadas decorrentes de erros nos sistemas de reconhecimento facial no Brasil, evidenciam que a IA pode levar a violações de direitos fundamentais. Esses erros são causados por vieses algorítmicos (especialmente o viés racial) que amplificam a discriminação.

A requerente alegou que a ordem judicial foi expedida de forma equivocada, com seus dados pessoais, em vez dos dados da verdadeira ré daquele processo, uma homônima parcial. Afirmou ter permanecido presa por três dias, de 16 a 18 de março de 2025, sendo liberada somente após audiência de custódia. Sustentou que a prisão indevida, agravada pelo transporte em uma viatura com dez homens, causou-lhe profunda humilhação e sofrimento psíquico, motivo pelo qual pleiteou a condenação do ente público ao pagamento de indenização por danos morais no valor de R\$ 300.000,00 (trezentos mil reais). (TJMG • PROCEDIMENTO COMUM CÍVEL • 5037242-22.2025.8.13.0024. Tribunal de Justiça de Minas Gerais) (Minas Gerais, 2020).

Em casos como esse, a omissão ou a conduta negligente na aplicação de tecnologias enviesada por agentes públicos ou privado exige uma resposta penal. O STF, na análise da ADPF 635, reconheceu a omissão estrutural dos poderes públicos na proteção dos direitos humanos de populações atingidas desproporcionalmente pela violência estatal (Brasil, 2020).

Por analogia, o uso de sistemas de IA que comprovadamente perpetuam o viés racial pode configurar uma continuidade dessa omissão estrutural, justificando a intervenção penal (além da civil) sobre o agente que viola o dever constitucional de não discriminar.

4.3. Imputação Penal por Risco Tecnológico e Dever de Cuidado

A Teoria da Imputação Objetiva permite atribuir responsabilidade a quem cria ou permite um risco tecnológico juridicamente desaprovado. A falha na gestão desse risco pode se manifestar de duas formas: Imputação Culposa e Dolosa.

A Imputação Culposa ocorre por infração do dever de cuidado objetivo. Se o desenvolvedor ou operador de um sistema de Alto Risco (conforme PL 2338/2023) falha em cumprir as obrigações de testes de bias ou auditoria (infringindo o dever de diligência qualificado), e essa falha leva a um dano, a responsabilidade penal pode ser verificada.

Enquanto que, a Imputação Dolosa (Dolo Eventual) ocorre através da Teoria da Cegueira Deliberada. Se o gestor está ciente de que um sistema de IA de Alto

Risco possui vieses ou falhas previsíveis que podem causar dano grave (discriminação), e opta por implementar o sistema, aceitando o risco da ocorrência do resultado, há dolo eventual.

A Teoria do Domínio do Fato, por exigir o controle sobre o ato de execução, deve ser vista como uma ferramenta auxiliar, sendo a Teoria da Imputação Objetiva (foco no risco prévio) e a Cegueira Deliberada (foco no elemento subjetivo/omissão de *compliance*) as ferramentas mais adequadas para lidar com a complexidade da IA (Alflen, 2014).

5. CONSIDERAÇÕES FINAIS

A pesquisa confirma que no ordenamento brasileiro atual não há imputação penal direta à Inteligência Artificial. Assim a responsabilidade deve recair sobre sujeitos humanos ou, de forma sistêmica, sobre pessoas jurídicas.

A dogmática penal clássica revela-se adequada para a análise de casos envolvendo Inteligência Artificial, desde que aplicada por meio de um novo *framework*⁸ interpretativo. Nesse sentido, o Crime de Algoritmo deve ser compreendido como uma modalidade de Crime de Empresa, direcionando a responsabilidade para a gestão do Risco Tecnológico.

Ademais, as ferramentas de imputação mais eficazes neste contexto são a Imputação Objetiva, fundamentada na infração do dever de cuidado, e a Teoria da Cegueira Deliberada, que possibilita a demonstração do dolo eventual diante da omissão no cumprimento das obrigações de *compliance*⁹ e vigilância.

Contudo, a conclusão transcende o campo teórico ao demonstrar que a eficácia plena da responsabilização exige a ação imediata do legislador, sendo cruciais tanto políticas públicas que elevem o dever de auditoria e a transparência a requisitos inegociáveis, quanto a regulação de normas incriminadoras, em especial,

⁸ Framework termo inglês que significa arcabouço ou estrutura conceitual. É a estrutura de imputação da responsabilidade penal pela falha algorítmica.

⁹ Compliance termo inglês que que significa conformidade ou adesão. Designa um conjunto de mecanismos e procedimentos internos que visa garantir que a organização atue em estrita observância às normas legais e regulamentos éticos.

a Tipificação de Omissão Qualificada para fornecer a base legal que define o "dever de cuidado" penalmente exigível.

Em última análise, este estudo demonstra que a resolução do dilema dogmático da IA é plenamente alcançável, desde que o *framework* proposto seja implementado. A efetivação desta resolução exige, por conseguinte, a reforma legislativa, que deve se concretizar na definição clara do dever de cuidado e na criação das normas incriminadoras necessárias para que o avanço tecnológico jamais comprometa o núcleo da proteção aos direitos e garantias fundamentais.

REFERÊNCIAS

ALFLEN, Pablo Rodrigo. Teoria do domínio do fato. São Paulo: Saraiva. **Cadernos Esmape – Série Teses e Dissertações**. Recife. vol. 1, n. 12, 2014.

ALENCAR, Matheus de. O crime de algoritmo como crime de empresa: uma resenha do artigo Não fui eu, foi a máquina. **Revista Científica do CPJM**. vol. 10, n.8, 2025.

BARBOSA, Wander. **A inteligência artificial no banco dos réus: quando algoritmos cometem crime**. Artigo *online*, 2025.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal: Parte Geral**. 27. ed. São Paulo: Saraiva, 2023.

BONFIM, Vinícius Alves. A. **Crimes cibernéticos: armazenamento de deepfake como crime de perigo abstrato**. Monografia. Curso de Direito. Universidade Anima: RUNA, 2025.

BRASIL. **Constituição da República Federativa do Brasil**. Senado Federal, Brasília: DF, 1988.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. **Projeto de Lei nº 2338, de 2023**. Institui o Marco Legal da Inteligência Artificial no Brasil. Senado Federal, Brasília, DF, 2023.

BRASIL. **Arguição de Descumprimento de Preceito Fundamental 635**. ADFP 635 Rel. Min. Edson Fachin. Julgamento em 5 jun. 2020, Plenário. Diário da Justiça Eletrônico, Brasília, DF, 2020.

FRANÇA, Laila Duarte Santos. **A teoria da cegueira deliberada e sua aplicação no Direito Penal brasileiro**. Monografia. Curso de Direito. Universidade de Rio Verde: UniRV, 2019.

GUIMARÃES, Phelipe Dimas Machado. **A teoria da imputação objetiva**. Disponível em <https://www.jus.com.br/artigos>. Acesso em 13 out 2025.

GRECO, Rogério. **Curso de Direito Penal: Parte Geral**. 25. ed. Rio de Janeiro: Impetus, 2023.

JUSLABORIS. **Inteligência artificial e racismo algorítmico: análise da neutralidade dos algoritmos frente aos episódios de violação de direitos nos meios digitais**. Brasília: TST, 2025.

LIMA, Fewigelson. **Quando o algoritmo comete o crime**. Adaptado do texto de Alan Sapis.

MAIA Lósso & LOBATO, Danilo Tavares. Domínio do fato à brasileira: na prática, a teoria é outra - Uma análise da relação entre a denúncia genérica em crimes societários e a aplicação da teoria do domínio do fato, na jurisprudência do Superior Tribunal de Justiça. **Revista Científica Do CPJM**, 2(06), 140–166, 2023.

MARQUES, Daniel da Silva. **Reconhecimento facial e segurança pública: Lawethics by design como novo paradigma regulatório**. Biblioteca de Teses e Dissertações. Universidade do Rio de Janeiro: UERJ, 2025.

MÜLLER, Willian; SILVEIRAS, Raphael. A evolução e a regulamentação da inteligência artificial no Brasil: uma perspectiva histórica e conceitual. **Revista Interciência – IMES Catanduva** - V.1, Nº 11, julho 2023.

NUCCI, Guilherme de Souza. **Código Penal Comentado**. 21. ed. Rio de Janeiro: Forense, 2023.

PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro: Parte Geral**. 44. ed. São Paulo: **Revista dos Tribunais**, v.2, n.1, 2019.

QUEIROGA, Alana Cassimiro. **A responsabilização civil das big techs pelo treinamento de I.A. à luz da racionalidade protetiva do direito autoral brasileiro e da teoria da cegueira deliberada da justiça**. Monografia, Curso de Direito. Universidade Federal da Paraíba. João Pessoa: UFPB, 2025.

ROQUE, Bruna Tamy Yamamoto. **A responsabilidade civil da inteligência artificial**. Repositório institucional da Universidade Federal de Santa Catarina: FSC, 2023.

ROXIN, Claus. **Autoría y dominio del hecho en Derecho Penal**. Madrid: Marcial Pons, 2000.

SANTOS, Fabio Antonio Tavares. **A responsabilidade penal horizontal no seio empresarial**. Tese (Doutorado). Universidade de São Paulo: USP, 2025.

SATO, Catherine Ruriko. **Deveres de cuidado e dimensões do risco**: da regulação de risco ao direito penal. Dissertação Mestrado. Universidade de São Paulo: USP, 2025.

SENADO FEDERAL. **Revista de Informação Legislativa**, n. 240. Brasília, DF: Senado Federal, 2025.

SILVA SÁNCHEZ, Jesús María. A expansão do Direito Penal: aspectos da política criminal nas sociedades pós-industriais. 3. ed. São Paulo: **Revista dos Tribunais**, v.12, n.11, 2013.

SUPREMO TRIBUNAL FEDERAL (STF). **Ação Penal 470**. Rel. Min. Joaquim Barbosa. Julgamento em 17 dez. 2012, Plenário. Diário da Justiça Eletrônico, Brasília, DF, 22 abr. 2013.

SUPREMO TRIBUNAL FEDERAL (STF). **Recurso Extraordinário 548.181/PR**. Rel. Min. Rosa Weber. Julgamento em 6 mar. 2013, Plenário. Diário da Justiça Eletrônico, Brasília, DF, 20 mar. 2013.

SUPREMO TRIBUNAL FEDERAL (STF). **Habeas Corpus 136.250/PE**. Rel. Min. Ricardo Lewandowski. Julgamento em 2017.

MINAS GERAIS. Tribunal de Justiça. **Procedimento Comum Cível n. 5037242-22.2025.8.13.0024**. Belo Horizonte, março de 2025.