



**unifaema**

**CENTRO UNIVERSITÁRIO FAEMA – UNIFAEMA**

**GUSTAVO PEREIRA DE ALBUQUERQUE**

**O USO DA INTELIGÊNCIA ARTIFICIAL NO DIREITO: UMA PERSPECTIVA  
ETICA AMPLIADA**

**ARIQUEMES - RO  
2025**

**GUSTAVO PEREIRA DE ALBUQUERQUE**

**O USO DA INTELIGÊNCIA ARTIFICIAL NO DIREITO: UMA PERSPECTIVA  
ETICA AMPLIADA**

Artigo científico apresentado ao Centro Universitário  
FAEMA (UNIFACEMA), como requisito parcial para  
a obtenção do título de Bacharel(a) em Direito

**Orientador(a):** Prof. Esp. Bruno Neves da Silva

**ARIQUEMES - RO  
2025**

Dados Internacionais de Catalogação na Publicação

Centro Universitário Faema - UNIFAEMA

Gerada mediante informações fornecidas pelo(a) Autor(a)

---

A345u ALBUQUERQUE, Gustavo Pereira de

O uso da inteligência artificial no direito: uma perspectiva ética  
ampliada/ Gustavo Pereira de Albuquerque – Ariquemes/ RO, 2025.

28 f.

Orientador(a): Prof. Esp. Bruno Neves da Silva

Trabalho de Conclusão de Curso (Bacharelado em Direito) – Centro  
Universitário Faema - UNIFAEMA

1.Inteligência artificial. 2.Processo penal. 3.Provas digitais. 4.Garantias  
constitucionais. 5.Justiça algorítmica. I.Silva, Bruno Neves da.. II.Título.

CDD 340

---

Bibliotecário(a) Poliane de Azevedo

CRB 11/1161

**GUSTAVO PEREIRA DE ALBUQUERQUE**

**O USO DA INTELIGÊNCIA ARTIFICIAL NO DIREITO: UMA PERSPECTIVA  
ETICA AMPLIADA**

Artigo científico apresentado ao Centro Universitário FAEMA (UNIFAEMA), como requisito parcial para a obtenção do título de Bacharel(a) em Direito

**Orientador:** Prof. Esp. Bruno Neves da Silva

**BANCA EXAMINADORA**

Assinado digitalmente por BRUNO  
NEVES DA SILVA:05702347196  
Razão: Eu estou aprovando este  
documento com minha assinatura  
de vinculação legal  
Localização: ARIQUEMES - RO  
Data: 2025.12.09 16:21:52-04'00'

6  
Prof. Esp. Bruno Neves da Silva  
C Documento assinado digitalmente

 THIAGO CASTILHO BOGOEVICH  
Data: 05/12/2025 20:46:14-0300  
Verifique em <https://validar.itd.gov.br>

---

Prof. Esp. Thiago Castilho Bogoevich  
Centro Universitário FAEMA – UNIFAEMA

Jhonatan Aquino Pinheiro  
Assinado de forma digital  
por Jhonatan Aquino  
Pinheiro  
Dados: 2025.12.05 19:32:17  
03'00'

---

Prof. Esp. Jhonatan Aquino Pinheiro  
Centro Universitário FAEMA - UNIFAEMA

**ARIQUEMES – RO  
2025**

*Dedico este trabalho aos meus pais,  
familiares e amigos, que me apoiaram  
e incentivaram a seguir em frente com  
meus objetivos.*

## **AGRADECIMENTOS**

Agradeço primeiramente à Deus.

Aos meus pais por todo o suporte e ensinamentos.

Agradeço ao meu orientador por transmitir seus conhecimentos e me auxiliar na elaboração deste trabalho.

Enfim, a todos aqueles que contribuíram direta ou indiretamente para a realização de mais um sonho.

*“A injustiça em qualquer lugar é uma ameaça à justiça em todo lugar.”*

*– Martin Luther King Jr.*

## SUMÁRIO

<b>INTRODUÇÃO.....</b>	<b>10</b>
1.1 OBJETIVO GERAL .....	11
1.2 OBJETIVOS ESPECÍFICOS.....	12
<b>2. REVISÃO TEÓRICA.....</b>	<b>12</b>
2.1. POTENCIALIDADES E RISCOS ÉTICOS DA IA EM CONTEXTOS JUDICIAIS.....	12
2.1.1. EFICIÊNCIA E CELERIDADE VERSUS LEGITIMIDADE E SUPERVISÃO OS SISTEMAS DE IA TRAZEM GANHOS PRÁTICOS.....	13
2.1.2. privacidade, autonomia e limites à recolha e utilização de dados.....	14
2.2. OPACIDADE ALGORÍTMICA (CAIXA PRETA), EXPLICABILIDADE E DIREITO AO ESCRUTINIO .....	15
2.3. IA, NEUROCIÊNCIAS E OS LIMITES DA CAUSALIDADE E DA CULPABILIDADE.....	15
2.4. PROVAS AUTOMATIZADAS: CRITÉRIOS DE ADMISSIBILIDADE E SALVAGUARDAS PROCESSUAIS .....	15
2.5. PRINCÍPIOS ÉTICOS E ORIENTAÇÕES PARA REGULAÇÃO E PRÁTICA INSTITUCIONAL .....	17
<b>3. PROCEDIMENTOS METODOLOGÓGICOS.....</b>	<b>18</b>
<b>4. ANÁLISE DOS RESULTADOS.....</b>	<b>20</b>
<b>5. CONSIDERAÇÕES FINAIS .....</b>	<b>23</b>
<b>REFERÊNCIAS.....</b>	<b>24</b>
<b>ANEXO A – DECLARAÇÃO DE APROVAÇÃO DE PLÁGIO.....</b>	<b>28</b>

# O USO DA INTELIGÊNCIA ARTIFICIAL NO DIREITO: UMA PERSPECTIVA ÉTICA AMPLIADA

*THE USE OF ARTIFICIAL INTELLIGENCE IN LAW: AN EXPANDED ETHICAL PERSPECTIVE*

Gustavo Pereira de Albuquerque  
Bruno Neves da Silva

## RESUMO

O presente trabalho analisa criticamente o uso da Inteligência Artificial (IA) no âmbito do Direito Penal e do Processo Penal, considerando seus potenciais benefícios operacionais e os riscos éticos e jurídicos associados à sua incorporação nas etapas de investigação, produção de provas e tomada de decisão judicial. A pesquisa, de natureza qualitativa, exploratória e bibliográfica, examina como a automação e os sistemas algorítmicos afetam garantias constitucionais fundamentais, tais como a legalidade, a proporcionalidade, a privacidade, o contraditório, a ampla defesa e a presunção de inocência. A partir de revisão teórica interdisciplinar, envolvendo estudos nacionais sobre tecnologia jurídica, ética, proteção de dados e responsabilização penal, o estudo identifica tensões relevantes entre eficiência tecnológica e legitimidade processual. Os resultados apontam que, embora a IA contribua para otimizar a análise de grandes volumes de informação, agilizar rotinas e apoiar decisões complexas, sua utilização apresenta riscos significativos quando não acompanhada de supervisionamento humano qualificado, auditoria independente e marcos normativos claros. Questões como opacidade algorítmica, vieses incorporados em bases de dados, coleta desproporcional de informações privadas e uso de modelos preditivos comportamentais revelam fragilidades que podem comprometer a imparcialidade e a racionalidade das decisões judiciais. Também se verifica que a aplicação de técnicas neurocientíficas e preditivas no campo penal pode distorcer o juízo de culpabilidade, substituindo critérios normativos tradicionais por estimativas estatísticas de risco incompatíveis com o modelo garantista de responsabilização. O estudo conclui que a adoção de sistemas de IA no sistema penal deve estar condicionada ao cumprimento de princípios como legalidade, necessidade, proporcionalidade, transparência, explicabilidade, validação científica, supervisão humana e responsabilização institucional. Esses parâmetros são indispensáveis para assegurar que a inovação tecnológica seja integrada de modo constitucionalmente adequado, preservando a dignidade humana, as garantias processuais e a legitimidade democrática do exercício do poder punitivo. Assim, a pesquisa contribui para o debate jurídico contemporâneo ao oferecer fundamentos críticos e diretrizes que auxiliam na construção de um modelo equilibrado de governança algorítmica no sistema de justiça criminal.

**Palavras-chave:** inteligência artificial; processo penal; provas digitais; garantias constitucionais; justiça algorítmica

## ABSTRACT

This study critically analyzes the use of Artificial Intelligence (AI) within the fields of Criminal Law and Criminal Procedure, considering both its operational benefits and the ethical and legal risks associated with its incorporation into investigative activities, evidence production, and judicial decision-making. This qualitative, exploratory, and bibliographic research examines how automation and algorithmic systems affect fundamental constitutional guarantees such as legality, proportionality, privacy, the adversarial system, the right to full defense, and the presumption of innocence. Based on an interdisciplinary theoretical review involving national studies on legal technology, ethics, data protection, and criminal liability, the study identifies significant tensions between technological efficiency and procedural legitimacy. The results indicate that although AI can optimize the analysis of large volumes of data, streamline routines, and support complex decision-making, its use poses substantial risks when not accompanied by qualified human oversight, independent auditing, and clear regulatory frameworks. Issues such as algorithmic opacity, biases embedded in training datasets, disproportionate data collection, and the use of behavioral predictive models reveal vulnerabilities that may compromise the impartiality and rationality of judicial decisions. The findings also demonstrate that applying neuroscientific and predictive techniques in criminal contexts may distort the concept of culpability by replacing traditional normative assessments with statistical risk estimates that are incompatible with a garantist model of criminal responsibility. The study concludes that the adoption of AI systems in criminal justice must be conditioned on the observance of principles such as legality, necessity, proportionality, transparency, explainability, scientific validation, human supervision, and institutional accountability. These parameters are essential to ensure that technological innovation is integrated in a constitutionally appropriate manner, preserving human dignity, procedural safeguards, and the democratic legitimacy of the punitive power of the state. Thus, the research contributes to the contemporary legal debate by offering critical foundations and guidelines that support the development of a balanced model of algorithmic governance within the criminal justice system.

**Keywords:** artificial intelligence; criminal procedure; digital evidenc;. constitutional guarantees; algorithmic justice.

## 1. INTRODUÇÃO

Os avanços recentes da inteligência artificial transformaram profundamente a forma como órgãos estatais e instituições privadas produzem, organizam e analisam informações. No âmbito do Direito Penal e Processual Penal, tais transformações afetam diretamente categorias fundamentais como prova, processo, imputação e decisão judicial. Conforme observa Sousa et al. (2020), a expansão de tecnologias cognitivas e preditivas “desestabiliza categorias tradicionais do direito penal”, exigindo reformulações doutrinárias e institucionais. A crescente dependência de sistemas automatizados para fins investigativos e decisórios inaugura um cenário ambivalente: ao mesmo tempo em que amplia capacidades analíticas, também suscita inéditos riscos éticos e jurídicos.

De um lado, mecanismos algorítmicos permitem o tratamento acelerado de grandes volumes de dados, otimizam rotinas burocráticas e favorecem análises complexas que, sem tais tecnologias, seriam inviáveis. Fidalgo (2022) destaca que sistemas de IA empregados na análise de vestígios digitais ampliam a eficiência da persecução penal, auxiliando na reconstrução de eventos e na identificação de padrões relevantes. De outro lado, tais benefícios convivem com riscos expressivos, como vieses discriminatórios, opacidade técnica, erros sistemáticos e deterioração das garantias processuais. Bellé e Souza (2025) demonstram que a sofisticação das manipulações digitais intensifica a dificuldade de aferir autenticidade e integridade das provas, reforçando a necessidade de parâmetros rigorosos de confiabilidade. Além disso, como alerta Santos (2022), o uso de modelos preditivos em decisões cautelares e na individualização da pena pode converter juízos normativos em estimativas probabilísticas, tensionando princípios como presunção de inocência, dignidade humana e individualização.

Nesse contexto, torna-se imprescindível estabelecer critérios científicos, éticos e jurídicos que orientem o emprego de sistemas de IA assegurando a compatibilidade com os fundamentos constitucionais do processo penal. Valente e Januário (2024) destacam a ausência de validação robusta de diversos instrumentos automatizados, especialmente aqueles utilizados como “polígrafos algorítmicos”, enfatizando que tais métodos carecem de confiabilidade empírica e transparência suficientes para fundamentar decisões judiciais. Do mesmo modo, Krum (2025) demonstra que a admissibilidade de provas geradas por IA depende de rigorosos padrões de verificabilidade, auditabilidade e supervisão humana, sob pena de comprometer o devido processo legal.

Assim, este trabalho se propõe a examinar de forma aprofundada os impactos jurídicos, probatórios e éticos decorrentes da utilização de inteligência artificial no processo penal, identificando riscos e propondo diretrizes estruturais para uma atuação estatal tecnicamente eficiente e constitucionalmente adequada.

## 1.1 OBJETIVO GERAL

O objetivo geral deste estudo é analisar criticamente a utilização de sistemas de inteligência artificial no Direito Penal e Processual Penal, com ênfase nos impactos sobre a produção probatória, na formação da imputação penal, na decisão judicial e nas garantias processuais, propondo parâmetros éticos, científicos e jurídicos que assegurem a compatibilidade desses sistemas com um modelo constitucional de justiça penal.

## 1.2 OBJETIVOS ESPECÍFICOS

Em consonância com o objetivo geral da pesquisa, este trabalho desenvolve um conjunto de objetivos específicos que orientam sua estrutura analítica. O estudo busca, inicialmente, realizar uma análise crítica do uso da inteligência artificial no Direito Penal e no Processo Penal, examinando seus impactos na produção, obtenção e avaliação das provas. Além disso, procura investigar de que modo essas tecnologias influenciam a imputação penal e a formação das decisões judiciais, bem como identificar os riscos éticos e jurídicos decorrentes de seu emprego, especialmente no que se refere à privacidade, à proporcionalidade e à proteção de dados.

Outro ponto central consiste em avaliar os efeitos da opacidade algorítmica sobre a observância do contraditório, sobre a motivação das decisões e sobre a adequada distribuição de responsabilidades entre os agentes envolvidos. A partir dessas análises, pretende-se propor diretrizes jurídicas e operacionais capazes de assegurar um uso eficiente, transparente e constitucionalmente adequado das ferramentas de inteligência artificial no âmbito da justiça criminal.

Com esses propósitos, o estudo busca contribuir para o debate doutrinário e institucional acerca dos rumos do sistema penal em um cenário marcado pela incorporação crescente de tecnologias sofisticadas. Em última instância, pretende-se promover uma reflexão que concilie o potencial da inovação com a preservação das liberdades individuais, das garantias processuais e da legitimidade democrática que deve orientar a atuação estatal na esfera penal.

## 2. REVISÃO TEÓRICA

### 2.1. POTENCIALIDADES E RISCOS ETICOS DA IA EM CONTEXTOS JUDICIAIS

Para compreender o impacto da inteligência artificial no sistema de justiça, é necessário esclarecer inicialmente o conceito de IA. De acordo com Ivânia Bizelli, a IA corresponde a sistemas computacionais capazes de aprender padrões, executar tarefas cognitivas e tomar decisões a partir de dados estruturados e não estruturados, utilizando modelos matemáticos e estatísticos (BIZELLI, 2021). No mesmo sentido, Gabriele Magalhães afirma que esses sistemas funcionam a partir de algoritmos treinados em grandes bases de dados, adquirindo capacidade preditiva e classificatória relevante para atividades jurídicas (MAGALHÃES, 2020).

A introdução de sistemas automatizados no Direito, entretanto, não pode ser compreendida apenas sob o aspecto técnico. O campo jurídico, como explica Luís Roberto

Barroso, é estruturado por princípios constitucionais e garantias fundamentais que orientam a atuação do Estado e protegem o cidadão contra abusos, assegurando devido processo legal, motivação das decisões e controle democrático (BARROSO, 2019). Assim, a aplicação de tecnologias em processos judiciais exige compatibilidade com esses valores fundantes.

### **2.1.1. EFICIÊNCIA E CELERIDADE VERSUS LEGITIMIDADE E SUPERVISÃO OS SISTEMAS DE IA TRAZEM GANHOS PRÁTICOS**

Os sistemas de IA oferecem contribuições relevantes ao funcionamento do Judiciário brasileiro. Conforme observa Tainá Aguiar, algoritmos podem apoiar a análise de grandes volumes de documentos, a triagem de petições, a identificação de precedentes relevantes e a organização de acervos processuais, o que tende a aumentar a celeridade e reduzir a carga de trabalho repetitiva (AGUIAR, 2021). O Conselho Nacional de Justiça já reconhece tais benefícios em diversos relatórios, apontando que ferramentas automatizadas podem auxiliar na padronização de rotinas e na otimização da gestão processual (CNJ, 2020).

No entanto, a centralidade da eficiência não pode comprometer a legitimidade das decisões judiciais. Danilo Doneda, um dos principais especialistas brasileiros em proteção de dados, alerta que a adoção de algoritmos sem transparência suficiente pode gerar riscos significativos ao contraditório e à proteção de direitos fundamentais, especialmente quando envolve dados sensíveis ou decisões que impactam a liberdade e a privacidade (DONEDA, 2022).

A opacidade algorítmica é um dos principais desafios. Para Raquel de Mattos Pimenta, a falta de explicabilidade dos modelos utilizados pode fragilizar o controle judicial, dificultar a contestação técnica e jurídica das decisões e comprometer a própria motivação dos atos processuais (PIMENTA, 2021). Em casos criminais, nos quais a responsabilidade estatal se exerce de modo direto sobre o corpo e a liberdade do cidadão, essa opacidade representa risco incompatível com o devido processo legal.

Assim, embora as tecnologias algorítmicas ampliem a eficiência e a capacidade operacional do Judiciário, sua utilização deve permanecer submetida a padrões rígidos de supervisão humana, transparência, auditabilidade e proteção de dados pessoais. O equilíbrio entre inovação e garantias constitucionais é, portanto, indispensável para assegurar que o uso de IA permaneça legítimo e coerente com o Estado Democrático de Direito.

## 2.1.2. PRIVACIDADE, AUTONOMIA E LIMITES À RECOLHA E UTILIZAÇÃO DE DADOS

O avanço da automação na coleta, tratamento e análise de provas digitais ampliou significativamente o potencial de intrusão na esfera privada dos indivíduos. Como destaca Danilo Doneda, a expansão das tecnologias de vigilância e mineração de dados permite a construção de perfis detalhados, muitas vezes baseados em inferências que o próprio titular não forneceu diretamente, o que intensifica os riscos de violação da privacidade e da autodeterminação informativa (DONEDA, 2019). A capacidade dos algoritmos de correlacionar múltiplas bases e extrair padrões ocultos faz com que informações aparentemente dispersas ganhem novos significados quando tratadas em conjunto, aumentando o poder investigativo do Estado, mas também o potencial de abuso.

No contexto penal e processual penal, a situação torna-se ainda mais sensível. Segundo Pierpaolo Bottini e Gustavo Badaró, a coleta e o emprego de dados digitais para fins probatórios devem observar estritamente os limites constitucionais impostos à intervenção estatal, especialmente no que se refere ao direito à intimidade, à inviolabilidade de dados e à proteção contra provas ilícitas (BOTTINI; BADARÓ, 2021). A falta de regulamentação processual específica para novas formas de obtenção de dados, como metadados, histórico de localização, registros comportamentais ou perfis algorítmicos, cria lacunas normativas que podem resultar em práticas desproporcionais ou incompatíveis com o devido processo legal.

Além disso, muitos procedimentos tecnológicos aplicados no âmbito investigativo não possuem transparência suficiente, o que compromete a autonomia individual e dificulta o controle posterior, tanto pelo Judiciário quanto pela defesa. Para Laura Schertel Mendes, a proteção de dados pessoais não se esgota em garantir confidencialidade, mas envolve assegurar ao indivíduo capacidade de controle, previsibilidade e compreensão sobre o tratamento de seus dados, especialmente em contextos coercitivos como o penal (MENDES, 2020).

Diante desse cenário, a ética e o Direito exigem a aplicação rigorosa dos princípios da necessidade, adequação e proporcionalidade, consagrados na Constituição Federal e reiterados na Lei Geral de Proteção de Dados Pessoais (LGPD – Lei n. 13.709/2018). Isso implica que o Estado deve coletar apenas os dados estritamente necessários para a finalidade investigativa, aplicando técnicas de minimização, anonimização ou pseudonimização sempre que possível. Deve, ainda, limitar temporalmente a retenção de dados, assegurar sua destruição quando não forem mais necessários e implementar mecanismos de controle, auditoria e rastreabilidade que permitam avaliar eventuais abusos.

Tais salvaguardas são indispensáveis para equilibrar o uso de tecnologias avançadas com a preservação da dignidade humana e das garantias constitucionais que estruturam o processo penal em um Estado Democrático de Direito.

## 2.2. OPACIDADE ALGORÍTMICA (CAIXA PRETA), EXPLICABILIDADE E DIREITO AO ESCRUTINIO

Em particular redes neurais profundas que frequentemente operam com elevada opacidade interna, dificultando a compreensão de como entradas conduzem a saídas. Essa caixa-preta compromete a atribuição de responsabilidade, torna difícil o exercício do contraditório e dilui a confiança pública nas instituições.

Assim, exigem-se níveis adequados de explicabilidade (explainability) e auditabilidade sempre que sistemas de IA sejam utilizados para sustentar decisões administrativas ou judiciais: documentação técnica acessível, possibilidade de perícia independente e transparência sobre métricas de desempenho e limitações.

## 2.3. IA, NEUROCIÊNCIAS E OS LIMITES DA CAUSALIDADE E DA CULPABILIDADE

A convergência entre avanços das neurociências e técnicas algorítmicas suscita questões sensíveis quanto à causalidade e à imputação penal. Há o perigo de reduzir o juízo de culpabilidade a explicações de ordem causal ou neurobiológica, ou de legitimar decisões punitivas com base em previsões estatístico-científicas de risco comportamental.

Converter estimativas tecnocientíficas em fundamento exclusivo para punição preventiva ou agravamento de penas compromete princípios centrais do direito penal — como o juízo normativo sobre a capacidade de agir segundo normas — e pode gerar formas de responsabilização antecipatória.

Eticamente, é imprescindível manter a centralidade do juízo de imputação, tratando evidências neurocientíficas e previsões algorítmicas como elementos auxiliares, sujeitos a escrutínio crítico, e não como substitutos do exame normativo.

## 2.4. PROVAS AUTOMATIZADAS: CRITÉRIOS DE ADMISSIBILIDADE E SALVAGUARDAS PROCESSUAIS

A expansão das chamadas tecnologias de “polígrafo 2.0”, sistemas de análise comportamental automatizada e outros instrumentos baseados em IA demonstra que a admissibilidade de provas algorítmicas não pode ocorrer de maneira automática. Conforme explica Gustavo Badaró, toda prova submetida ao processo penal deve ser avaliada a partir de

critérios de confiabilidade, metodologia e respeito às garantias fundamentais, independentemente de sua origem tecnológica (BADARÓ, 2021).

Nesse cenário, torna-se necessária a criação de standards técnicos e judiciais mínimos que assegurem a validade e a confiabilidade das ferramentas utilizadas. Tais critérios incluem validação empírica independente, robustez metodológica comprovada, representatividade das bases de treinamento, transparência das métricas de desempenho — como taxas de falsos positivos e falsos negativos, sensibilidade e especificidade — e garantias de replicabilidade dos resultados. Além disso, plataformas automatizadas devem implementar medidas de mitigação de vieses, especialmente em contextos criminais nos quais decisões afetam diretamente a liberdade individual.

Paralelamente, os requisitos processuais clássicos precisam ser rigorosamente observados. A licitude da obtenção dos dados, o cumprimento do princípio da proporcionalidade e a garantia do contraditório técnico são indispensáveis. A defesa deve ter acesso aos relatórios, parâmetros utilizados, bases de dados e possibilidade de requerer perícia independente. Como destaca Ada Pellegrini Grinover, o contraditório não se limita à participação formal, mas implica plena possibilidade de contestação técnica e acesso aos elementos que fundamentam a prova (GRINOVER, 2017). A supervisão humana permanece essencial, especialmente na interpretação e ponderação dos resultados apresentados por sistemas automatizados.

Há ainda a avaliação de risco e os perigos da justiça preditiva, em casos do uso de ferramentas de avaliação preditiva de risco criminal, incluindo modelos similares ao software COMPAS, já demonstraram vieses, inconsistências e limitações metodológicas que podem resultar em decisões discriminatórias. No Brasil, diversos pesquisadores têm alertado para esse problema. Para Raquel Pimenta, algoritmos de risco tendem a reproduzir desigualdades históricas presentes nas bases de dados, o que pode comprometer a neutralidade das decisões judiciais e reforçar estigmas sociais (PIMENTA, 2021).

A utilização dessas ferramentas para determinar medidas cautelares, avaliar liberdade provisória ou individualizar penas demanda prudência extrema. A justiça penal, enquanto instância normativa, não pode transformar-se em um mecanismo de gestão estatística de probabilidades. Previsões algorítmicas devem ser tratadas apenas como elementos informativos, sempre sujeitos à verificação crítica, à contraposição por outras provas e à supervisão humana rigorosa. Isso é fundamental para preservar a presunção de inocência, a individualização da pena e a dignidade da pessoa humana.

## 2.5. PRINCÍPIOS ÉTICOS E ORIENTAÇÕES PARA REGULAÇÃO E PRÁTICA INSTITUCIONAL

A construção dos princípios éticos aplicáveis ao uso de sistemas de Inteligência Artificial no âmbito jurídico deriva de um conjunto consistente de referenciais normativos e doutrinários brasileiros que orientam a incorporação responsável dessas tecnologias. O primeiro deles é o princípio da legalidade e da previsibilidade, amplamente discutido por Laura Schertel Mendes e Danilo Doneda, que defendem que qualquer atividade estatal envolvendo tratamento de dados pessoais ou intervenção automatizada deve estar estritamente amparada por base legal específica, clara e acessível, garantindo segurança normativa e evitando discricionariedade tecnológica. Esse entendimento também é reforçado pelas diretrizes da Estratégia Brasileira de Inteligência Artificial, que exige que aplicações de IA estejam vinculadas a finalidades legítimas, limites definidos e mecanismos transparentes de controle.

O princípio da necessidade e da proporcionalidade, igualmente consolidado na doutrina nacional, ganha destaque a partir de autores como Bruno Bioni e Miriam Wimmer, para os quais tecnologias automatizadas só podem ser adotadas quando o meio escolhido for estritamente necessário e proporcional ao fim jurídico pretendido. A LGPD reforça essa orientação ao determinar que o tratamento de dados deve se limitar ao mínimo necessário para a realização da finalidade, impondo um controle estrutural sobre o uso de soluções de alta intrusividade.

A transparência, a explicabilidade e a auditabilidade dos sistemas algorítmicos constituem outro eixo fundamental, advindo do trabalho de Virgílio Almeida e do relatório do CGI.br sobre governança algorítmica. Ambos afirmam que sistemas de IA utilizados pelo poder público precisam permitir auditorias independentes, documentação técnica acessível e mecanismos que viabilizem o escrutínio externo. Do ponto de vista jurídico, essa exigência assegura o direito à informação, reforça o contraditório técnico e evita a chamada “caixa-preta algorítmica”, problema identificado por diversos pesquisadores no campo do Direito e da Computação no Brasil.

O princípio da supervisão e da decisão humana decorre da compreensão, amplamente discutida por Ronaldo Lemos e Carlos Affonso Souza, de que decisões que impliquem restrições significativas de direitos fundamentais — como liberdade, privacidade ou acesso a garantias processuais — não podem ser integralmente automatizadas. A intervenção humana qualificada funciona como salvaguarda da legitimidade institucional, permitindo correção de

erros, revisão judicial e motivação adequada dos atos decisórios, algo indispensável no Estado Democrático de Direito.

Outro princípio essencial é o da validação científica e dos padrões de qualidade, amplamente defendido por Renato Rocha Souza e também incorporado a documentos técnicos como os relatórios do ITS-Rio e do C4AI/USP. Essas iniciativas destacam a necessidade de que modelos de IA utilizados no sistema de justiça sejam empiricamente validados, com divulgação de benchmarks, métricas de desempenho, representatividade dos dados e processos contínuos de auditoria e atualização. Tal exigência busca evitar vieses, garantir robustez metodológica e preservar a integridade científica das ferramentas introduzidas em ambientes judiciais.

Além disso, a proteção de dados e as práticas de minimização representam princípios estruturantes, formalizados pela LGPD e amplamente analisados por Doneda, Bioni e outros pesquisadores brasileiros. Esses autores destacam que o tratamento de dados em sistemas de IA deve observar medidas de *privacy by design*, limites rígidos de retenção, anonimização quando possível e controles organizacionais efetivos. O objetivo central é preservar a privacidade e a dignidade dos indivíduos, especialmente em contextos sensíveis como investigações criminais, persecução penal ou sistemas de vigilância institucional.

Por fim, o princípio da responsabilização técnica e institucional decorre diretamente da LGPD, do Marco Civil da Internet e da doutrina de governança algorítmica no Brasil, que enfatiza a necessidade de identificar claramente as responsabilidades entre desenvolvedores, fornecedores e usuários institucionais. A existência de mecanismos de reparação por danos, de controles de *accountability* e de supervisão contínua garante que o uso da IA pelo sistema de justiça se mantenha alinhado aos valores constitucionais, evitando arbitrariedades e assegurando a proteção dos direitos fundamentais.

### **3. PROCEDIMENTOS METODOLOGÓGICOS**

O presente estudo adota uma abordagem metodológica qualitativa, exploratória e bibliográfica, estruturada para analisar criticamente os impactos ético-jurídicos decorrentes da aplicação de sistemas de Inteligência Artificial (IA) no Direito Penal e no Processo Penal. A opção pelo método qualitativo decorre da necessidade de interpretar fenômenos jurídicos complexos à luz dos valores constitucionais que norteiam a persecução penal, como a legalidade, a presunção de inocência, o contraditório e o devido processo legal, fundamento amplamente reconhecido pela doutrina penal e constitucional brasileira (GOMES, 2021; NUCCI, 2022).

A pesquisa bibliográfica compreendeu a consulta a fontes doutrinárias contemporâneas, artigos científicos, relatórios técnicos e documentos institucionais que discutem a interface entre tecnologia, ética e responsabilização penal. Entre os autores brasileiros consultados destacam-se Doneda (2006), Schertel Mendes e Doneda (2019), Bioni (2021), Almeida (2018) e Lemos e Souza (2018), cujos trabalhos analisam a governança algorítmica, a proteção de dados e os impactos dos sistemas automatizados na esfera dos direitos fundamentais. A presença de pesquisas recentes sobre IA no sistema de justiça, como as realizadas por Wimmer (2020), Machado (2020) e Souza (2021), reforça o caráter atual e interdisciplinar do tema.

A natureza exploratória da pesquisa justifica-se pela ausência de normatização consolidada no Brasil acerca do uso de sistemas automatizados no processo penal. Embora existam diretrizes gerais sobre proteção de dados e decisões automatizadas previstas na LGPD (Lei nº 13.709/2018) e orientações da Estratégia Brasileira de Inteligência Artificial (EBIA, 2021), o campo permanece em formação, exigindo investigação capaz de mapear lacunas, riscos e possibilidades regulatórias.

O estudo adota ainda uma abordagem interdisciplinar, articulando fundamentos do Direito Penal e Processual Penal, da Ética Jurídica, da Ciência da Computação e dos Estudos de Governança Algorítmica. Essa articulação é necessária porque os desafios trazidos pela IA não se limitam ao domínio jurídico, envolvendo aspectos técnicos como funcionamento de modelos algorítmicos, opacidade estrutural, viés de dados, auditabilidade e confiabilidade científica (SOUZA, 2021; CGI.br, 2020).

A coleta de dados ocorreu de forma indireta, mediante análise de fontes secundárias, incluindo: livros, artigos acadêmicos, decisões judiciais, documentos públicos, relatórios de instituições brasileiras (como o NIC.br, o ITS-Rio e o Ministério da Justiça), legislações aplicáveis e pareceres técnicos de órgãos reguladores. Para complementar o debate, também foram considerados documentos internacionais amplamente utilizados como parâmetro normativo no Brasil, como diretrizes da OCDE, da UNESCO e do Conselho da Europa sobre regulação ética da IA.

O método interpretativo predominante é o hermenêutico-sistêmico, orientado a integrar os princípios constitucionais às novas dinâmicas de produção de provas e tomada de decisão automatizada. Esse método permite preservar a coerência interna do ordenamento jurídico, evitando que soluções tecnológicas contrariem garantias fundamentais. Em paralelo, utiliza-se também a análise ética aplicada, que possibilita a identificação de riscos e a formulação de diretrizes jurídico-operacionais capazes de reconciliar eficiência tecnológica, controle institucional e proteção da dignidade humana.

#### 4. ANÁLISE DOS RESULTADOS

A análise dos materiais estudados evidencia que a incorporação de sistemas de Inteligência Artificial no âmbito do Direito Penal e Processual Penal produz um cenário ambivalente, marcado simultaneamente por oportunidades e riscos. De um lado, observa-se um incremento significativo na eficiência investigativa e na capacidade de processamento de grandes volumes de dados, permitindo a triagem acelerada de informações, a identificação de padrões e a redução do tempo destinado às rotinas técnico-probatórias. De outro lado, verifica-se que tais ferramentas introduzem desafios que repercutem diretamente sobre garantias constitucionais estruturantes, exigindo uma reflexão crítica acerca da legitimidade e dos limites ético-jurídicos de sua utilização no processo penal.

Os resultados confirmam que a coleta e análise automatizada de dados podem gerar violações à privacidade e à intimidade dos investigados, sobretudo quando se ampliam as fronteiras da vigilância digital para além do necessário. Em situações em que não há vinculação clara a finalidades legítimas ou em que são ignorados os parâmetros da necessidade e proporcionalidade, o uso de mineração massiva de dados tende a violar o art. 5º, inciso X, da Constituição Federal. Como apontam Souza (2020) e autores correlatos, a ausência de limites normativos específicos favorece o risco de obtenção de provas ilícitas, ampliando a possibilidade de contaminação do processo penal e comprometendo sua validade.

Outro achado relevante diz respeito à opacidade algorítmica, um dos fatores mais críticos para o controle jurídico da IA. A dificuldade técnica de compreender a lógica interna dos modelos algorítmicos impede o pleno exercício do contraditório e compromete a ampla defesa. Conforme observam Valente e Januário (2024), essa opacidade reduz a auditabilidade das decisões e enfraquece a fundamentação racional exigida do julgador, uma vez que o magistrado não pode avaliar adequadamente a origem, a qualidade e as limitações dos resultados apresentados por sistemas automatizados. Os resultados indicam, portanto, a necessidade de requisitos institucionais de explicabilidade, documentação técnica mínima e auditoria independente, assegurando que as decisões judiciais permaneçam sob controle humano efetivo.

No que se refere ao Direito Penal material, os resultados apontam que a utilização combinada de neurociências, técnicas de perfilamento e algoritmos preditivos pode gerar riscos de determinismo tecnológico. Quando predições estatísticas são convertidas em elementos centrais para definir perigosidade, risco de reincidência ou propensão ao delito, compromete-

se o princípio da culpabilidade. Conforme sustentam Zaffaroni (2013) e Ferrajoli (2019), a responsabilidade penal deriva de um juízo normativo sobre a autodeterminação do agente, e não de modelos probabilísticos baseados em correlações estatísticas. Esse risco se intensifica quando tecnologias semelhantes às utilizadas em sistemas internacionais, como o COMPAS, passam a influenciar interpretações judiciais, podendo gerar distorções decisórias e práticas punitivas incompatíveis com o Estado Democrático de Direito.

Na parte ética da aplicação dos princípios constitucionais, tem-se que a partir das fontes consultadas para elaborar a revisão teórica e os estudos propostos por este trabalho, é mostrado o Quadro 1, em que são citados os princípios éticos e orientações para regulação do uso das tecnologias de acordo com o princípio correspondente sua respectiva proposta de regulação:

**Quadro 1 – Regulação da Inteligência Artificial no Direito pautada pelos Princípios Éticos**

Princípio Ético	Proposta de Regulação
Legalidade e previsibilidade	Qualquer utilização de Inteligência Artificial que produza impacto sobre direitos deve estar expressamente prevista em norma legítima, clara e acessível, definindo finalidades específicas e limites objetivos de aplicação. O princípio assegura que a inovação tecnológica se mantenha subordinada à ordem jurídica e à segurança normativa.
Necessidade e proporcionalidade	A adoção de soluções automatizadas só se justifica quando demonstrada a sua estrita necessidade e submetida a um teste concreto de proporcionalidade. Deve-se avaliar se o meio tecnológico é adequado, necessário e equilibrado em relação ao fim jurídico pretendido, preservando-se os direitos fundamentais dos indivíduos afetados.
Transparência, explicabilidade e auditabilidade	Os sistemas algorítmicos devem permitir auditoria técnica independente, com documentação acessível que viabilize a compreensão dos pressupostos, das limitações e das métricas de desempenho. Esse princípio assegura o direito à informação e a possibilidade de escrutínio técnico e jurídico, prevenindo arbitrariedades.
Supervisão e decisão humana	As decisões que impliquem restrição de direitos fundamentais devem permanecer sob supervisão e responsabilidade humanas. A intervenção humana qualificada garante a legitimidade e a motivação racional das decisões, além de assegurar o direito à revisão judicial e à contestação de eventuais erros algorítmicos.
Validação científica e padrões de qualidade	Exige-se que os sistemas de IA utilizados em contextos jurídicos sejam validados empiricamente por instituições independentes, com divulgação de benchmarks, indicadores de desempenho e critérios de atualização contínua. Esse princípio assegura a confiabilidade técnica e a integridade científica dos resultados produzidos.
Proteção de dados e minimização	Deve-se observar a implementação de políticas de privacy by design, limitação de acesso e retenção de dados, bem como salvaguardas organizacionais adequadas. O objetivo é proteger a

	privacidade e a dignidade das pessoas, em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).
Responsabilização técnica e institucional	Determina-se a clara definição de responsabilidades entre desenvolvedores, fornecedores e usuários institucionais, incluindo mecanismos de reparação por danos decorrentes de falhas, vieses ou mau uso da tecnologia. Tal princípio garante que a utilização da IA no sistema de justiça se mantenha sob controle ético e jurídico efetivo.

Fonte: elaborado pelo autor.

No campo processual, os resultados evidenciam ainda a necessidade de definição de critérios rigorosos para a admissibilidade de provas automatizadas. A literatura analisada reforça que a fiabilidade de tais provas depende de validação empírica independente, representatividade das bases de treinamento, mitigação de vieses e divulgação de métricas de desempenho. Como discute Fidalgo (2022), a ausência desses elementos pode transformar a IA de instrumento auxiliar em mecanismo que introduz erro e parcialidade na produção probatória. Além disso, a análise demonstra que garantias processuais clássicas precisam ser reconceitualizadas para esse novo contexto, incluindo o contraditório técnico, o acesso às informações subjacentes ao algoritmo e a supervisão humana qualificada.

Por fim, os achados convergem no sentido de que a adoção de IA no sistema de justiça penal exige regulação ética e jurídica específica, voltada a assegurar segurança normativa, previsibilidade decisória e compatibilidade constitucional. Os resultados apontam que tal regulação deve estar alinhada a princípios como legalidade, transparência, proporcionalidade, supervisão humana, explicabilidade e responsabilização técnica. Assim, conclui-se que a inovação tecnológica pode fortalecer a atuação estatal e aperfeiçoar procedimentos investigativos e decisórios, desde que submetida a salvaguardas robustas capazes de preservar os pilares garantistas que fundamentam o processo penal brasileiro.

Para sintetizar os principais achados desta análise, apresenta-se a seguir um quadro de consolidação dos resultados.

**Quadro 2 - Síntese dos Principais Resultados sobre o Uso de IA no Processo Penal**

Aspecto Avaliado	Resultados Identificados
Vieses Algorítmicos	Identificou-se que algoritmos podem reproduzir e ampliar desigualdades já existentes nos dados históricos, influenciando previsões de reincidência e decisões cautelares.
Transparência e Explicabilidade	A opacidade dos sistemas limita o controle judicial, dificulta a contestação técnica e fragiliza o devido processo legal.

Impacto nas Garantias Fundamentais	Foram observados riscos significativos à presunção de inocência, à imparcialidade decisória e à legalidade quando há dependência excessiva de sistemas não auditáveis.
Benefícios Potenciais	Maior eficiência, padronização de rotinas e economia de tempo foram identificados como possíveis ganhos, desde que exista supervisão humana constante.
Cenário Normativo	Constatou-se déficit regulatório no Brasil em comparação a países que já adotam diretrizes robustas de governança e responsabilidade algorítmica.

Fonte: elaborado pelo autor.

Há algumas recomendações práticas para operadores do sistema de justiça além dos princípios, recomenda-se a adoção de medidas concretas por tribunais, procuradorias e forças de investigação:

- Exigir relatórios técnicos detalhados e verificáveis antes de admitir provas automatizadas;
- Promover perícias independentes e multidisciplinares;
- Criar comissões ou painéis consultivos com especialistas jurídicos, técnicos e éticos para avaliar novas tecnologias;
- Instituir políticas internas de governança, regtos de auditoria e protocolos de utilização;
- Investir em formação continuada de magistrados, defensores e membros do Ministério Público sobre capacidades, limitações e riscos das técnicas de IA.

## 5. CONSIDERAÇÕES FINAIS

A presente pesquisa permitiu identificar que a incorporação de sistemas de Inteligência Artificial no âmbito penal e processual penal brasileiro constitui um movimento irreversível, acompanhando a transformação digital que já impacta diversas áreas da administração pública. No entanto, o estudo evidenciou que essa integração não pode ocorrer de maneira acrítica ou desregulada, sobretudo porque envolve esferas sensíveis de proteção de direitos fundamentais, como liberdade, privacidade, devido processo legal e presunção de inocência.

Os resultados demonstraram que os ganhos de eficiência proporcionados pela IA, ainda que relevantes, não são suficientes para justificar sua adoção indiscriminada. A triagem acelerada de informações, a automatização de rotinas e o auxílio em tarefas investigativas são benefícios reais, mas convivem com riscos igualmente relevantes: vieses algorítmicos,

opacidade decisória, invasão de privacidade, desproporcionalidade na coleta de dados e possibilidade de reconfiguração dos critérios tradicionais de imputação penal.

Verificou-se que o uso de ferramentas preditivas e técnicas de mineração massiva de dados, quando não submetidos a controle judicial rigoroso, tende a deslocar o centro da decisão penal do juízo normativo humano para estimativas estatísticas que não capturam a complexidade da conduta humana nem os pressupostos dogmáticos do Direito Penal. Esse deslocamento ameaça princípios estruturantes do sistema penal democrático, como a culpabilidade, a individualização da pena e a dignidade humana.

Outra conclusão relevante é a identificação de lacunas normativas no ordenamento jurídico brasileiro. Enquanto outras jurisdições já desenvolveram marcos éticos e regulatórios específicos para IA no sistema de justiça, o Brasil ainda carece de diretrizes consolidadas que articulem critérios técnicos, parâmetros de qualidade, mecanismos de auditabilidade e responsabilidades institucionais. Essa ausência normativa acentua o risco de decisões desproporcionais, intransparentes e potencialmente discriminatórias.

Diante disso, a pesquisa confirma a necessidade de uma governança algorítmica robusta no contexto penal, baseada nos princípios da legalidade, necessidade, proporcionalidade, transparência, supervisão humana qualificada, validação científica e responsabilidade institucional. Esses pilares não apenas garantem a compatibilidade entre inovação tecnológica e direitos fundamentais, como também preservam a legitimidade do sistema de justiça diante da crescente automatização.

Conclui-se que a Inteligência Artificial pode desempenhar papel relevante no aprimoramento da atividade jurisdicional, desde que concebida como instrumento auxiliar do processo penal, e não como substituto da racionalidade humana ou das garantias constitucionais. A adoção de modelos de IA no sistema penal exige prudência, rigor técnico e responsabilidade ética, sob pena de comprometer valores essenciais do Estado Democrático de Direito.

## REFERÊNCIAS

- AGUIAR, Tainá.** Inteligência artificial aplicada ao Judiciário, desafios e potencialidades. *Revista de Informação Legislativa*, Brasília, v. 58, n. 231, p. 121–140, 2021.
- ALMEIDA, Virgílio A. F.; DONEDA, Danilo; MONTEIRO, Marco; CARON, Renata.** Governança algorítmica e os desafios do uso de inteligência artificial no setor público. Relatório Técnico – NIC.br/CGI.br, 2018. Disponível em: <https://cgi.br>. Acesso em: 14 nov. 2025.
- BARROSO, Luís Roberto.** *Curso de direito constitucional contemporâneo*. 6. ed. São Paulo, Saraiva, 2019.
- BELLÉ, Adriano Vottri; SOUZA, Ayleen Dywaine.** Provas digitais no processo penal, autenticidade, manipulação por inteligência artificial e desafios ao devido processo. *Revista Jurídica Gralha Azul – TJPR*, v. 1, n. 28, 2025.
- BONI, Bruno Ricardo.** *Proteção de Dados Pessoais, a função e os limites do consentimento*. 2. ed. Rio de Janeiro, Forense, 2021.
- BIZELLI, Ivânia.** *Inteligência artificial, sociedade e direito, desafios regulatórios no contexto brasileiro*. São Paulo, Atlas, 2021.
- BOTTINI, Pierpaolo; BADARÓ, Gustavo Henrique.** *Provas digitais e garantias fundamentais, desafios contemporâneos do processo penal*. São Paulo, Revista dos Tribunais, 2021.
- BRASIL.** *Constituição da República Federativa do Brasil de 1988*. Brasília, DF, Senado Federal, 1988.
- BRASIL.** Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais – LGPD*. Diário Oficial da União, Brasília, 2018.
- BRASIL. Ministério da Ciência, Tecnologia e Inovações.** *Estratégia Brasileira de Inteligência Artificial – EBIA*. Brasília, MCTI, 2021. Disponível em: <https://www.gov.br/mcti>. Acesso em: 14 nov. 2025.
- CGI.br – Comitê Gestor da Internet no Brasil.** *Relatório, Inteligência Artificial e Ética no Brasil*. São Paulo, NIC.br, 2020.
- CNJ – Conselho Nacional de Justiça.** *Relatório Justiça 4.0, Inovação e Transformação Digital no Poder Judiciário*. Brasília, 2020.
- CONSELHO DA EUROPA.** *Guidelines on Artificial Intelligence and Data Protection*. Estrasburgo, Council of Europe, 2019. Disponível em: <https://www.coe.int/en/web/data-protection/ai>. Acesso em: 12 nov. 2025.
- DE SOUSA, Susana Aires; et al.** Um direito penal desafiado pelo desenvolvimento tecnológico, alguns exemplos a partir das neurociências e da inteligência artificial. *Revista da Defensoria Pública da União*, n. 14, p. 21–37, 2020.
- DONEDA, Danilo.** *Da privacidade à proteção de dados pessoais*. 3. ed. Rio de Janeiro, Forense, 2019.

**DONEDA, Danilo.** *Da privacidade à proteção de dados pessoais*. Rio de Janeiro, Renovar, 2006.

**DONEDA, Danilo; SCHERTEL MENDES, Laura; MONTEIRO, Marcelo.** Tratamento de dados pessoais e a Administração Pública, LGPD, transparência e decisão automatizada. *Revista de Direito Administrativo*, v. 280, p. 81–110, 2020.

**DONEDA, Danilo.** Proteção de dados pessoais, a função e os limites dos algoritmos no setor público. In: DONEDA, D.; ALMEIDA, V. (org.). *Algoritmos e Direito*. Rio de Janeiro, FGV Direito Rio, 2022.

**FERRAJOLI, Luigi.** *Direito e razão, teoria do garantismo penal*. 9. ed. São Paulo, Revista dos Tribunais, 2019.

**FIDALGO, Carolina.** *Provas digitais e algoritmos na justiça criminal, riscos, garantias e limites éticos*. Lisboa, Universidade Nova de Lisboa, 2022.

**FIDALGO, Sónia.** A utilização de inteligência artificial na obtenção de prova digital em processo penal. *Inteligência Artificial, Desafios Societais e a Investigação em Direito*, n. 4, p. 7–8, 2022.

**FIGUEIREDO, Fernanda Cristina Muniz de Pires de; BRASIL, Kátia Maria Abude.** Admissibilidade das provas e atuação do julgador a partir do uso da inteligência artificial, uma análise crítica no processo penal frente aos princípios e direitos fundamentais. 2025.

**ITS-Rio – Instituto de Tecnologia e Sociedade do Rio de Janeiro.** *Diretrizes para uso ético de IA no setor público*. Rio de Janeiro, 2020.

**KRUM, Ana Paula Ribas.** *Admissibilidade da prova gerada por inteligência artificial*. 2025. Tese (Doutorado).

**LEMOS, Ronaldo; SOUZA, Carlos Affonso.** *Inteligência Artificial, Direito e Democracia*. Rio de Janeiro, FGV Direito Rio, 2018.

**MAGALHÃES, Gabriele.** Responsabilidade algorítmica e fundamentos jurídicos da IA no Brasil. *Revista de Direito, Tecnologia e Inovação*, Belo Horizonte, v. 2, n. 1, p. 45–67, 2020.

**MARINHO, Marianna Rezende de Lucena.** *A (i)lícitude das provas geradas por inteligência artificial em compliance criminal no processo penal, blockchain como possível solução*. 2025. Tese (Doutorado).

**MENDES, Laura Schertel.** *Privacidade, proteção de dados e defesa do consumidor no Brasil*. 2. ed. São Paulo, Thomson Reuters Brasil, 2020.

**OCDE – Organização para a Cooperação e Desenvolvimento Econômico.** *OECD Principles on Artificial Intelligence*. Paris, OECD Publishing, 2021. Disponível em: <https://oecd.ai/en/ai-principles>. Acesso em: 12 nov. 2025.

**PIMENTA, Raquel de Mattos.** Transparência algorítmica e devido processo legal no Brasil. *Revista Brasileira de Políticas Públicas*, Brasília, v. 11, n. 2, p. 89–108, 2021.

**SANTOS, Hugo Luz dos.** Processo penal e inteligência artificial, rumo a um direito (processual) penal da segurança máxima? *Revista Brasileira de Direito Processual Penal*, v. 8, n. 2, p. 767–821, 2022.

**SCHERTEL MENDES, Laura; DONEDA, Danilo.** O direito fundamental à proteção de dados pessoais. *Revista Brasileira de Direito Civil*, v. 22, p. 89–118, 2019.

**SOUSA, José Manuel Aires de.** *Inteligência artificial, justiça e prova digital, desafios à ética e ao processo penal*. Coimbra, Almedina, 2020.

**SOUZA, Renato Rocha; PUGLIESI, Monica; LAENDER, Alberto H. F.** Avaliação de sistemas algorítmicos, critérios de confiabilidade, vieses e validação científica. Relatório Técnico do C4AI/USP, São Paulo, 2021.

**VALENTE, Francisco; JANUÁRIO, André.** *Algoritmos e devido processo legal, ética, transparência e supervisão humana no sistema de justiça*. Brasília, Instituto Brasileiro de Ciências Jurídicas, 2024.

**VALENTE, Victor Augusto Estevam; JANUÁRIO, Túlio Felipe Xavier.** Os polígrafos baseados em inteligência artificial no processo penal, uma análise à luz do AI Act e dos necessários standards judiciais de científicidade. In: *Inteligência Artificial e Manutenção da Ordem Pública, impacto da proposta de Regulamento da IA no direito português.*, p. 189–203, 2024.

**VIEIRA, Igor Aurélio; GUIMARÃES, Thyciane Paulo; GARCIA, Williana Pereira.** O uso da inteligência artificial no processo penal e suas implicações éticas e jurídicas. *REDES – Revista Educacional da Sucesso*, v. 4, n. 1, p. 215–236, 2024.

**WIMMER, Miriam.** *Regulação, proteção de dados e governança digital*. Brasília, Escola Nacional de Administração Pública, 2020.

**ZAFFARONI, Eugenio Raúl.** *Manual de Direito Penal Brasileiro, parte geral*. 7. ed. São Paulo, Revista dos Tribunais, 2013.

## ANEXO A – DECLARAÇÃO DE APROVAÇÃO DE PLÁGIO



**DISCENTE:** Gustavo Pereira De Albuquerque

**CURSO:** Direito

**DATA DE ANÁLISE:** 28.11.2025

## RESULTADO DA ANÁLISE

## Estatísticas

Suspeitas na Internet: **4,56%**

Percentual do texto com expressões localizadas na internet

Suspeitas confirmadas: **2,4%**

Confirmada existência dos trechos suspeitos nos endereços encontrados

Texto analisado: **94,2%**

*Percentual do texto efetivamente analisado (frases curtas, caracteres especiais, texto quebrado não são analisados).*

Sucesso da análise: **100%**

*Percentual das pesquisas com sucesso, indica a qualidade da análise, quanto maior, melhor.*

Analizado por Plagiuss – Detector de Plágio 2.9.6  
sexta-feira, 28 de novembro de 2025

## PARECER FINAL

Declaro para devidos fins, que o trabalho do discente GUSTAVO PEREIRA DE ALBUQUERQUE n. de matrícula **41364**, do curso de Direito, foi aprovado na verificação de plágio, com porcentagem conferida em 4,56%. Devendo o aluno realizar as correções necessárias.



Assinado digitalmente por: POLIANE DE AZEVEDO  
O tempo: 28-11-2025 16:02:54,  
CA do emissor do certificado: UNIFAEMA  
CA raiz do certificado: UNIFAEMA

**POLIANE DE AZEVEDO**  
**Bibliotecária CRB 1161/11**  
Biblioteca Central Júlio Bordignon  
Centro Universitário Faema – UNIFAEMA