REMUNOM
ISSN 2178-6925

Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

A APLICAÇÃO DA INTELIGÊNCIA ARTIFICIAL NA INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS: AVANÇOS TECNOLÓGICOS E IMPACTOS NO SISTEMA JURÍDICO-FORENSE

THE APPLICATION OF ARTIFICIAL INTELLIGENCE IN THE INVESTIGATION OF CYBERCRIMES: TECHNOLOGICAL ADVANCES AND IMPACTS ON THE LEGAL-FORENSIC SYSTEM

LA APLICACIÓN DE LA INTELIGENCIA ARTIFICIAL EN LA INVESTIGACIÓN DE DELITOS CIBERNÉTICOS: AVANCES TECNOLÓGICOS E IMPACTOS EN EL SISTEMA JURÍDICO-FORENSE

Antônio Ferreira do Norte Filho
Doutor em Ciências do Ambiente e Sustentabilidade na Amazônia
Universidade Federal do Amazonas (UFAM), Brasil
nortefilho@gmail.com
https://orcid.org/0000-0002-5946-3291

Andrezza de Lima Rodrigues
Graduanda em Direito, Faculdade Santa Teresa (FST), Brasil
andrezzalimajuris@gmail.com
https://orcid.org/0009-0007-6546-5270

Hajime Hattori Xaud da Cruz
Graduando em Direito, Faculdade Santa Teresa (FST), Brasil
hajimexaud2903@gmail.com
https://orcid.org/0009-0001-7319-4243

Resumo

O avanço dos crimes cibernéticos tem exigido do Estado a adoção de instrumentos investigativos mais sofisticados, dentre os quais se destaca a inteligência artificial (IA) como recurso de elevado potencial operacional. Este artigo analisa a aplicação de sistemas algorítmicos na investigação criminal em ambiente digital, com enfoque nas repercussões jurídicas decorrentes dessa incorporação tecnológica no ordenamento brasileiro. A pesquisa adota abordagem qualitativa, fundamentada em revisão bibliográfica e normativa, examinando a compatibilidade entre o uso da IA e os direitos e garantias fundamentais previstos na Constituição Federal de 1988 e na legislação infraconstitucional. São discutidas as capacidades analíticas da IA, especialmente no tratamento massivo de dados e na identificação de padrões suspeitos, bem como os desafios relacionados à sua utilização no âmbito investigativo. Destacam-se as tensões entre eficiência tecnológica e princípios como dignidade da pessoa humana, contraditório, ampla defesa e presunção de inocência. O estudo também aborda a opacidade dos sistemas algorítmicos e os riscos de reprodução de vieses discriminatórios no sistema de justiça criminal. Conclui-se que a adoção da IA demanda regulação adequada, transparência nos processos decisórios e mecanismos efetivos de controle, a fim de assegurar a conformidade com os direitos fundamentais.

Palavras-chave: Inteligência artificial; Crimes cibernéticos; Investigação criminal; Prova digital; Direitos

REMUNOM
ISSN 2178-6925

Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

fundamentais.

Abstract

The advancement of cybercrime has required the State to adopt increasingly sophisticated investigative tools, among which artificial intelligence (AI) stands out as a resource with significant operational potential. This article examines the application of algorithmic systems in criminal investigations within digital environments, focusing on the legal implications arising from this technological incorporation in the Brazilian legal framework. The study adopts a qualitative approach, based on bibliographic and normative review, analyzing the compatibility between the use of AI and the fundamental rights and guarantees established by the 1988 Federal Constitution and related legislation. The analytical capabilities of AI are discussed, particularly in the large-scale processing of data and the identification of suspicious behavioral patterns, as well as the challenges associated with its use in investigative contexts. The research highlights the tension between technological efficiency and principles such as human dignity, due process, adversarial proceedings, and the presumption of innocence. It also addresses the opacity of algorithmic systems and the risks of reproducing discriminatory biases within the criminal justice system. The study concludes that the use of AI requires appropriate regulation, transparency in decision-making processes, and effective oversight mechanisms to ensure compliance with fundamental rights.

Keywords: Artificial Intelligence; Cybercrime; Criminal Investigation; Digital Evidence; Fundamental Rights.

Resumen

El avance de los delitos cibernéticos ha exigido al Estado la adopción de instrumentos investigativos cada vez más sofisticados, entre los cuales la inteligencia artificial (IA) destaca como un recurso de alto potencial operativo. Este artículo examina la aplicación de sistemas algorítmicos en la investigación criminal en entornos digitales, con énfasis en las implicaciones jurídicas derivadas de esta incorporación tecnológica en el ordenamiento jurídico brasileño. La investigación adopta un enfoque cualitativo, basado en revisión bibliográfica y normativa, analizando la compatibilidad entre el uso de la IA y los derechos y garantías fundamentales previstos en la Constitución Federal de 1988 y en la legislación infraconstitucional. Se analizan las capacidades de la IA, especialmente en el procesamiento masivo de datos y la identificación de patrones sospechosos, así como los desafíos asociados a su uso en el ámbito investigativo. El estudio destaca las tensiones entre la eficiencia tecnológica y principios como la dignidad humana, el debido proceso, la contradicción, la amplia defensa y la presunción de inocencia. Asimismo, aborda la opacidad de los sistemas algorítmicos y los riesgos de reproducción de sesgos discriminatorios en el sistema de justicia penal. Se concluye que el uso de la IA requiere una regulación adecuada, transparencia en los procesos de toma de decisiones y mecanismos efectivos de control para garantizar el respeto de los derechos fundamentales.

Palabras clave: Inteligencia Artificial; Delitos Cibernéticos; Investigación Criminal; Prueba Digital; Derechos Fundamentales.

1 INTRODUÇÃO

A consolidação da sociedade da informação, impulsionada pela expansão acelerada das tecnologias digitais, promoveu profundas transformações nas dinâmicas sociais, comunicacionais e econômicas.

Paralelamente a esses avanços, observa-se o surgimento de novas formas de criminalidade que desafiam os modelos tradicionais de investigação e repressão

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

penal.

O ambiente digital, marcado por sua natureza transnacional, descentralizada e de rápida mutação, amplia significativamente as possibilidades de atuação criminosa, abrangendo práticas como fraudes financeiras, invasões de sistemas informáticos, disseminação de conteúdos ilícitos e ataques a infraestruturas críticas (Stevens, 2022).

Nesse contexto, a inteligência artificial (IA) assume papel de destaque como instrumento potencialmente capaz de aprimorar a atuação estatal na persecução penal. Por meio de técnicas avançadas de análise de dados, aprendizado de máquina e reconhecimento de padrões, a IA possibilita o tratamento automatizado de grandes volumes de informações, contribuindo para a identificação de comportamentos suspeitos e para a articulação de dados provenientes de múltiplas fontes digitais.

Essas capacidades conferem maior celeridade e precisão às atividades investigativas, especialmente diante da complexidade inerente aos crimes cibernéticos.

Entretanto, a incorporação de sistemas algorítmicos no âmbito da investigação criminal suscita relevantes questionamentos jurídicos e éticos. A utilização dessas tecnologias deve ser analisada à luz do ordenamento constitucional brasileiro, que estabelece limites claros à atuação do Estado, mesmo quando orientada pela busca de eficiência.

A Constituição Federal (CRFB/88) consagra direitos e garantias fundamentais que orientam o devido processo legal, tais como a dignidade da pessoa humana, o contraditório, a ampla defesa, a presunção de inocência e a vedação de provas obtidas por meios ilícitos.

A tensão entre o potencial tecnológico da IA e a necessidade de preservação das garantias processuais penais configura o eixo central deste estudo. A busca por maior eficiência investigativa não pode resultar na flexibilização indevida de direitos fundamentais, sob pena de comprometer a legitimidade das práticas estatais e a própria integridade do sistema de justiça criminal. Assim, torna-se imprescindível refletir sobre os limites jurídicos e as condições de uso dessas ferramentas no

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

contexto investigativo.

Parte-se da premissa de que a adoção de tecnologias avançadas, por si só, não assegura a legitimidade das investigações nem a justiça dos resultados alcançados.

Sem a definição de marcos regulatórios adequados, sem mecanismos efetivos de transparência e controle e sem o compromisso com a proteção dos direitos individuais, a utilização da IA pode contribuir para a reprodução de desigualdades estruturais e para o aprofundamento de práticas discriminatórias no âmbito penal (O'Neil, 2021).

Diante desse cenário, o presente artigo tem como objetivo analisar a aplicação da inteligência artificial na investigação de crimes cibernéticos, examinando seus benefícios operacionais, seus riscos jurídicos e suas implicações para o sistema de justiça criminal brasileiro.

Busca-se, assim, contribuir para o debate acadêmico e institucional acerca da necessidade de compatibilização entre inovação tecnológica e proteção dos direitos fundamentais no Estado Democrático de Direito.

2 METODOLOGIA

O presente estudo adota abordagem qualitativa, orientada pela análise crítico-reflexiva acerca da utilização da inteligência artificial na investigação de crimes cibernéticos.

Trata-se de um ensaio teórico-jurídico com base em revisão bibliográfica crítica, voltado à análise interpretativa das implicações do uso da inteligência artificial na investigação criminal.

A escolha desse método justifica-se pela complexidade do objeto de pesquisa, que envolve dimensões jurídicas, tecnológicas e éticas, demandando interpretação aprofundada e contextualizada dos fenômenos analisados.

No que se refere aos procedimentos técnicos, a pesquisa caracteriza-se como bibliográfica e documental. A investigação bibliográfica foi desenvolvida a partir da seleção de obras doutrinárias, artigos científicos e produções acadêmicas nacionais e estrangeiras, com foco em autores reconhecidos nas áreas do direito penal, direito

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

processual penal, teoria do garantismo, sociologia da vigilância e ética da inteligência artificial. Como critério de seleção, priorizaram-se trabalhos com relevância acadêmica consolidada, impacto teórico e pertinência temática direta com o objeto de estudo.

Como critérios de inclusão, foram selecionados trabalhos com aderência direta ao tema, reconhecimento acadêmico e contribuição teórica relevante, sendo excluídas produções sem revisão científica ou com abordagem meramente descritiva e desvinculada do enfoque jurídico proposto.

A busca bibliográfica foi realizada em bases acadêmicas como Google Scholar, Scielo e periódicos jurídicos especializados, utilizando descritores como “inteligência artificial”, “investigação criminal”, “prova digital”, “direitos fundamentais” e “vieses algorítmicos”, em português e inglês.

Adotou-se, ainda, um recorte temporal voltado, predominantemente, à produção científica publicada a partir da última década, considerando a necessidade de acompanhar as transformações recentes no campo das tecnologias digitais e suas implicações jurídicas.

Não obstante, obras clássicas foram incorporadas sempre que indispensáveis à fundamentação teórica, especialmente no que se refere à construção dos conceitos de controle social, poder punitivo e garantismo penal.

A pesquisa documental concentrou-se na análise de diplomas normativos que regulam o uso de tecnologias e dados no contexto investigativo, incluindo a Constituição Federal de 1988, o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais e atos normativos do Conselho Nacional de Justiça. A interpretação desses instrumentos foi realizada sob uma perspectiva constitucional, com ênfase na centralidade dos direitos e garantias fundamentais.

Como método de abordagem, adotou-se o método hermenêutico-crítico, que permite não apenas a interpretação das normas jurídicas, mas também a problematização de seus limites frente às transformações tecnológicas contemporâneas.

Esse método possibilita a identificação de lacunas normativas, ambiguidades interpretativas e desafios decorrentes da incorporação de sistemas algorítmicos na

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

investigação criminal.

A técnica de análise consistiu na leitura sistemática, categorização temática e interpretação crítica do material selecionado, organizado a partir de eixos analíticos centrais, tais como, evolução do controle social e cibercriminalidade, garantias fundamentais e opacidade algorítmica, marco legal e prova digital e impactos da inteligência artificial no sistema de justiça criminal.

O estudo fundamenta-se em uma perspectiva teórica orientada pelo garantismo penal, com ênfase na proteção da dignidade da pessoa humana e na preservação das garantias processuais como limites à atuação estatal.

Por fim, a pesquisa apresenta caráter exploratório e descritivo, visando não apenas compreender o estado atual do tema, mas também contribuir para o desenvolvimento de uma abordagem crítica sobre o uso da inteligência artificial na investigação de crimes cibernéticos, à luz dos princípios que estruturam o sistema jurídico brasileiro.

Ressalta-se que a pesquisa não possui caráter de revisão sistemática, mas sim de análise teórica crítica, não se propondo à exaustividade, e sim à construção de uma interpretação juridicamente orientada sobre o tema.

3 A EVOLUÇÃO DO APARATO REPRESSIVO E A CIBERCRIMINALIDADE

A trajetória histórica do controle social e do aparato repressivo estatal revela um processo contínuo de adaptação às transformações estruturais da sociedade. Desde os mecanismos punitivos das sociedades pré-modernas, marcados pela espetacularização da punição e pela afirmação do poder soberano, até o advento das instituições disciplinares da modernidade como prisões, hospitais e escolas, observa-se a progressiva racionalização das práticas de controle, orientadas por estratégias de vigilância, normalização e sanção (Foucault, 2013).

Nesse percurso, o poder punitivo deixa de incidir exclusivamente sobre o corpo para alcançar dimensões mais sutis, voltadas à regulação das condutas e à internalização de normas sociais.

Com a emergência da sociedade da informação, esse paradigma sofre uma inflexão significativa em razão do desenvolvimento das tecnologias digitais que

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

inaugura uma nova lógica de controle, caracterizada pela descentralização, pela automação e pela capacidade ampliada de processamento de dados.

A vigilância, outrora limitada por barreiras físicas e pela atuação humana direta, passa a operar em escala global, por meio de sistemas informatizados capazes de monitorar, coletar e analisar informações em tempo real.

Trata-se de uma vigilância difusa, contínua e, muitas vezes, imperceptível aos indivíduos, o que redefine profundamente as relações entre Estado, tecnologia e liberdade individual (Stevens, 2022).

Essa transformação não apenas altera os instrumentos de controle social, mas também impacta diretamente a configuração da criminalidade. O ambiente digital amplia as possibilidades de prática de delitos tradicionais, ao mesmo tempo em que dá origem a novas modalidades criminosas, cuja complexidade desafia os marcos normativos clássicos do direito penal.

Crimes como invasão de dispositivos informáticos, fraudes eletrônicas, disseminação de conteúdos ilícitos e ataques a sistemas críticos evidenciam a necessidade de respostas jurídicas mais específicas e tecnicamente adequadas.

No ordenamento jurídico brasileiro, a resposta legislativa a esse fenômeno materializou-se, entre outros diplomas, na Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que introduziu no Código Penal tipos penais voltados à tutela da segurança informacional, destacando-se o artigo 154-A, que tipifica a invasão de dispositivo informático mediante violação indevida de mecanismo de segurança, com o objetivo de obter, adulterar ou destruir dados, ou ainda instalar vulnerabilidades com fins ilícitos.

Essa inovação normativa representa um marco na adaptação do direito penal às demandas da sociedade digital, embora ainda enfrente desafios interpretativos e de aplicação prática.

Assim, impõe-se ao Estado o aprimoramento de suas capacidades investigativas uma vez que a complexidade da cibercriminalidade, aliada à volatilidade e ao volume massivo de dados digitais, exige ferramentas capazes de lidar com informações em escala e velocidade incompatíveis com os métodos tradicionais de investigação.

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

É nesse contexto que a inteligência artificial se apresenta como instrumento estratégico, permitindo o cruzamento automatizado de dados, a identificação de padrões comportamentais e o suporte à tomada de decisões investigativas (Santos, 2017).

Estudos recentes no campo da segurança pública apontam que o uso de inteligência artificial em investigações criminais tem se concentrado em aplicações como análise preditiva, reconhecimento de padrões e integração de bases de dados, com impactos relevantes na forma de produção de informações investigativas (Ferguson, 2017; Brayne, 2020). Essas transformações indicam uma mudança estrutural na lógica investigativa, marcada pela crescente dependência de sistemas automatizados.

Para fins analíticos, é possível distinguir diferentes categorias de uso da inteligência artificial no contexto investigativo, sistemas de apoio à mineração e organização de dados, voltados à triagem de informações e identificação de padrões, ferramentas de análise preditiva e ranqueamento de risco, que sugerem probabilidades de ocorrência de condutas ilícitas e sistemas de suporte à decisão, que influenciam diretamente a formação do juízo investigativo ou judicial. Essa distinção é fundamental para a adequada avaliação dos impactos jurídicos decorrentes do uso dessas tecnologias.

Entretanto, a incorporação dessas tecnologias ao aparato repressivo não pode ser compreendida apenas sob a ótica da eficiência, uma vez que a ampliação do poder de vigilância estatal impõe a necessidade de uma reflexão crítica acerca de seus limites e de sua compatibilidade com os direitos fundamentais.

A história do controle social demonstra que cada avanço tecnológico traz consigo novas formas de exercício do poder, o que exige constante vigilância jurídica e institucional para evitar abusos e garantir a preservação das liberdades individuais.

Essa compreensão, contudo, revela-se insuficiente para abarcar a complexidade das formas contemporâneas de controle social mediadas por tecnologias digitais, uma vez que os mecanismos de vigilância atuais operam de maneira difusa, automatizada e, muitas vezes, invisível, dificultando sua

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

identificação e controle jurídico efetivo.

Portanto, a cibercriminalidade, ao tensionar os modelos tradicionais de investigação e repressão penal, impõe ao direito o desafio de equilibrar inovação e garantias, eficiência e legitimidade, em consonância com os princípios estruturantes do Estado Democrático de Direito.

A partir das discussões apresentadas, propõe-se uma sistematização dos usos da inteligência artificial no contexto investigativo, distinguindo-se três categorias fundamentais, inteligência artificial de apoio informacional, voltada à coleta, organização e mineração de dados, inteligência artificial de apoio pericial, utilizada na análise técnica de vestígios digitais e reconstrução de eventos e inteligência artificial de apoio decisório, que influencia diretamente a formação de juízos investigativos ou judiciais.

Essa distinção não possui caráter meramente classificatório, mas busca oferecer um instrumento analítico capaz de orientar a avaliação jurídica dos diferentes níveis de impacto dessas tecnologias sobre os direitos fundamentais.

3.1 PRINCÍPIO DA DIGNIDADE DA PESSOA HUMANA E A "BLACK BOX" ALGORÍTMICA

O princípio da dignidade da pessoa humana ocupa posição nuclear no ordenamento jurídico brasileiro, constituindo-se como fundamento axiológico do Estado Democrático de Direito e eixo estruturante de todo o sistema de direitos fundamentais.

Previsto expressamente no artigo 1º, inciso III, da Constituição Federal de 1988, esse princípio consagra a ideia de que todo ser humano possui valor intrínseco e irrenunciável, impondo ao Estado e à sociedade o dever de respeito, proteção e promoção de suas dimensões física, moral e psíquica.

Essa prerrogativa não se relativiza diante da persecução penal, alcançando indistintamente investigados, acusados e condenados, uma vez que a dignidade humana não se condiciona à conduta do indivíduo, mas à sua própria condição existencial (Moraes, 2018).

No contexto da investigação criminal mediada por inteligência artificial, a

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

incidência desse princípio revela-se particularmente sensível. A crescente utilização de sistemas algorítmicos para análise de dados, identificação de suspeitos e apoio à tomada de decisões investigativas introduz uma problemática central: a opacidade estrutural desses sistemas, frequentemente descrita pela literatura como “black box” algorítmica (Pasquale, 2015).

Trata-se de modelos cujo funcionamento interno, critérios decisórios e processos de inferência não são plenamente compreensíveis nem mesmo por seus desenvolvedores, o que dificulta a explicação racional dos resultados produzidos.

Essa perspectiva ignora que a opacidade não constitui apenas uma limitação técnica, mas um elemento estrutural desses sistemas, que pode comprometer a própria legitimidade das decisões produzidas a partir de seus resultados, especialmente quando utilizados em contextos sensíveis como a investigação criminal.

Nesse sentido, a literatura sobre governança algorítmica destaca a importância de mecanismos de auditoria e avaliação independente dos sistemas de inteligência artificial, especialmente em contextos de alto impacto, como o sistema de justiça criminal (Kroll et al., 2017). Esses mecanismos visam mitigar riscos associados à opacidade e à falta de controle sobre os processos automatizados.

Essa ausência de transparência compromete diretamente garantias processuais fundamentais uma vez que a impossibilidade de acesso aos critérios que fundamentam determinada conclusão algorítmica impede o exercício efetivo do contraditório e da ampla defesa, na medida em que o investigado não dispõe de elementos suficientes para questionar, refutar ou contextualizar os resultados obtidos por tais sistemas.

Nesse sentido, a Constituição Federal (CRFB/88), assegura, em seu artigo 5º, inciso LV, que aos acusados são garantidos o contraditório e a ampla defesa, com os meios e recursos a ela inerentes, o que pressupõe, necessariamente, a inteligibilidade dos elementos que compõem a formação do juízo estatal.

A tensão entre a opacidade algorítmica e as exigências constitucionais revela um desafio significativo para o direito contemporâneo, ou seja, a utilização de sistemas de inteligência artificial na investigação criminal não pode prescindir de

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

critérios mínimos de transparência, auditabilidade e explicabilidade, sob pena de se instaurar um modelo decisório incompatível com os fundamentos do devido processo legal.

A dignidade da pessoa humana opera como limite material à adoção acrítica dessas tecnologias, exigindo que qualquer instrumento utilizado pelo Estado seja passível de escrutínio e controle.

Todavia, a exigência de transparência, embora necessária, não se revela suficiente para assegurar a confiabilidade dos resultados produzidos, sendo preciso distinguir a transparência formal, relacionada à possibilidade de acesso aos critérios de funcionamento do sistema, da confiabilidade material, que diz respeito à consistência, robustez e validade das inferências geradas, pois, mesmo sistemas transparentes podem produzir resultados estatisticamente frágeis ou inadequados para fundamentar decisões no âmbito penal.

Ademais, a opacidade algorítmica potencializa riscos de reprodução de vieses discriminatórios, muitas vezes invisíveis e naturalizados no funcionamento dos sistemas automatizados.

A ausência de mecanismos de controle e verificação pode resultar na consolidação de práticas seletivas, comprometendo não apenas a justiça das decisões, mas também a igualdade perante a lei.

Assim, a proteção da dignidade humana demanda não apenas transparência formal, mas também responsabilidade substantiva na concepção, implementação e utilização desses sistemas.

Diante desse quadro, impõe-se a necessidade de construção de um modelo normativo que compatibilize a inovação tecnológica com os direitos fundamentais. Isso implica reconhecer que a eficiência proporcionada pela inteligência artificial não pode se sobrepor às garantias processuais, sendo indispensável a adoção de parâmetros jurídicos que assegurem a explicabilidade dos sistemas, a possibilidade de contestação de seus resultados e a supervisão humana qualificada.

Portanto, somente dessa forma será possível integrar a inteligência artificial ao sistema de justiça criminal de maneira legítima, preservando a centralidade da dignidade da pessoa humana como fundamento inafastável da atuação estatal.

REMUNOM
ISSN 2178-6925

Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

3.2 O MARCO LEGAL E O USO DE EVIDÊNCIAS DIGITAIS

O ordenamento jurídico brasileiro dispõe, atualmente, de um conjunto normativo relevante para disciplinar as relações no ambiente digital, ainda que em constante processo de adaptação diante da rápida evolução tecnológica.

Entre os diplomas centrais, destaca-se a Lei nº 12.965/2014, conhecida como Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, constituindo-se como referência estruturante para a regulação das atividades online.

Há, contudo, uma lacuna teórica e normativa relevante no que se refere à aplicação dessas disposições ao uso de inteligência artificial, uma vez que os diplomas existentes não foram concebidos para lidar com sistemas decisórios automatizados de alta complexidade.

No âmbito da investigação criminal, o Marco Civil da Internet trouxe avanços significativos ao definir parâmetros claros para o acesso a dados digitais, condicionando o fornecimento de registros e informações relacionadas às comunicações privadas à prévia autorização judicial, reforçando a proteção à intimidade e ao sigilo das comunicações.

Além disso, impõe aos provedores a obrigação de manter registros de conexão e de acesso a aplicações, criando uma base informacional que pode subsidiar a atuação das autoridades competentes.

Nesse sentido, o artigo 7º assegura a inviolabilidade do fluxo das comunicações, ressalvada a possibilidade de acesso mediante ordem judicial, o que revela a preocupação do legislador em equilibrar a atividade investigativa com a preservação dos direitos individuais.

A Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), acrescenta uma camada adicional de proteção ao disciplinar o tratamento de dados pessoais, inclusive em contextos relacionados à segurança pública e à persecução penal.

A LGPD estabelece princípios como finalidade, adequação, necessidade e transparência, que devem orientar qualquer atividade de tratamento de dados,

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

inclusive aquelas mediadas por sistemas de inteligência artificial.

Ainda que a lei preveja hipóteses de tratamento sem consentimento do titular, especialmente para fins de investigação criminal, exige-se a observância de salvaguardas que assegurem a legalidade e a proporcionalidade das medidas adotadas.

A articulação entre esses diplomas normativos e o uso de tecnologias baseadas em inteligência artificial ainda se encontra em fase de amadurecimento no contexto brasileiro.

A inexistência de regras específicas voltadas ao emprego de sistemas algorítmicos na atividade investigativa evidencia uma lacuna regulatória que demanda atenção uma vez que pode favorecer práticas que, embora tecnicamente sofisticadas, carecem de fundamentos jurídicos sólidos e de mecanismos adequados de controle.

A ausência de regulamentação específica sobre o uso de IA na segurança pública cria um vácuo normativo que pode dar margem a abusos e à utilização de evidências obtidas por meios que, embora tecnicamente eficazes, não atendem aos requisitos de legalidade e proporcionalidade exigidos pelo Estado Democrático de Direito (Nader, 2017).

Logo, a utilização de dados digitais em investigações criminais deve observar critérios rigorosos de licitude, rastreabilidade e integridade, de modo a garantir sua validade no processo penal e a preservar os direitos fundamentais dos envolvidos.

A atuação estatal precisa ser orientada por parâmetros claros, que assegurem não apenas a eficiência investigativa, mas também a legitimidade dos meios empregados.

Assim, mais do que a simples existência de normas, revela-se indispensável a construção de um modelo interpretativo e regulatório capaz de integrar o uso de tecnologias avançadas com os princípios constitucionais.

A consolidação desse modelo passa pelo fortalecimento do controle jurisdicional, pela definição de limites objetivos para a atuação estatal e pela promoção de uma cultura jurídica comprometida com a proteção da pessoa humana.

Assim, a integração de tecnologias no âmbito investigativo deve ser conduzida sob parâmetros jurídicos capazes de harmonizar inovação e garantias fundamentais,

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

assegurando o exercício do poder estatal e o respeito aos direitos fundamentais.

4 A CADEIA DE CUSTÓDIA NA ERA DOS DADOS VOLÁTEIS

A cadeia de custódia da prova representa um dos pilares do processo penal, pois garante a preservação da integridade e da autenticidade dos elementos utilizados na formação do convencimento judicial.

Trata-se de um conjunto de procedimentos que asseguram a rastreabilidade do material probatório desde sua coleta até sua apresentação em juízo. No contexto digital, essa garantia adquire contornos mais complexos, considerando que os dados eletrônicos possuem natureza imaterial, são facilmente modificáveis e frequentemente estão distribuídos em ambientes descentralizados (Lopes Jr., 2020).

No contexto digital, a cadeia de custódia exige a adoção de procedimentos técnicos específicos que assegurem a integridade, a autenticidade e a rastreabilidade dos dados coletados.

Isso inclui a utilização de técnicas como geração de hash criptográfico, que permite verificar se houve alteração no conteúdo dos dados; espelhamento forense de dispositivos, garantindo a preservação do material original; e registro detalhado de logs de acesso, responsáveis por documentar todas as interações realizadas com os dados ao longo do tempo.

Além disso, a manutenção de ambientes controlados de armazenamento e a adoção de mecanismos de versionamento são medidas essenciais para evitar contaminações ou perdas informacionais.

A particularidade dos dados digitais reside em sua volatilidade e na facilidade com que podem ser alterados, corrompidos ou mesmo eliminados sem deixar vestígios perceptíveis. Além disso, muitos desses dados estão armazenados em servidores localizados em diferentes países, o que impõe obstáculos adicionais relacionados à jurisdição e à cooperação internacional.

Essas características exigem não apenas domínio técnico, mas também rigor metodológico na coleta, preservação e análise das informações utilizadas em investigações criminais.

No campo da forense computacional, a literatura especializada destaca a necessidade de procedimentos padronizados para a preservação e análise de dados

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

digitais, incluindo técnicas de aquisição forense, verificação de integridade e documentação rigorosa das etapas de processamento (Casey, 2011; Carrier, 2005).

Essas abordagens evidenciam que a confiabilidade dos elementos digitais depende não apenas de sua obtenção, mas da observância de protocolos técnicos reconhecidos internacionalmente.

Essa abordagem, embora adequada no plano normativo, mostra-se limitada diante das especificidades dos dados digitais, cuja volatilidade e replicabilidade desafiam os modelos tradicionais de preservação probatória concebidos para evidências físicas.

No âmbito da inteligência artificial, a qualidade dos resultados obtidos está diretamente vinculada à confiabilidade dos dados inseridos nos sistemas, posto modelos algorítmicos operarem a partir de grandes volumes de informações, e qualquer irregularidade na origem ou no tratamento desses dados pode comprometer todo o processo analítico.

Um dado adulterado ou obtido de forma irregular não apenas prejudica a consistência das conclusões, mas também compromete a validade jurídica dos elementos derivados, afetando a credibilidade da investigação como um todo (Ferrajoli, 2014).

Com efeito, torna-se fundamental distinguir entre o vestígio digital bruto, correspondente ao dado originalmente coletado; o dado derivado, resultante de tratamentos técnicos como filtragem, organização ou cruzamento de informações; e a inferência algorítmica, que corresponde às conclusões produzidas por sistemas de inteligência artificial a partir desses dados.

Essa diferenciação é essencial para a adequada valoração no processo penal, uma vez que cada uma dessas camadas apresenta níveis distintos de confiabilidade e exige formas específicas de controle e verificação.

Nesse sentido, torna-se necessário diferenciar a produção de indícios a partir de análises automatizadas da efetiva constituição de prova no processo penal. Os resultados gerados por sistemas de inteligência artificial podem orientar a investigação, mas sua conversão em elementos probatórios válidos depende do

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

cumprimento rigoroso dos requisitos de legalidade, rastreabilidade e possibilidade de verificação pelas partes.

O ordenamento jurídico brasileiro passou a tratar de forma mais sistematizada a cadeia de custódia com as alterações introduzidas pela Lei nº 13.964/2019, que incorporou ao Código de Processo Penal dispositivos específicos sobre o tema.

A legislação define a cadeia de custódia como o conjunto de procedimentos destinados a manter e documentar a história cronológica do vestígio, desde o reconhecimento até o descarte.

Essa normatização reforça a necessidade de padronização e controle rigoroso na manipulação de elementos probatórios, incluindo aqueles de natureza digital.

A aplicação dessas diretrizes ao ambiente tecnológico impõe a adoção de protocolos técnicos que assegurem a integridade, a autenticidade e a rastreabilidade dos dados.

Isso inclui o registro detalhado de todas as etapas de coleta, armazenamento e processamento, bem como a utilização de mecanismos que impeçam alterações indevidas. A ausência desses cuidados pode comprometer a admissibilidade das provas no processo penal, além de fragilizar a própria legitimidade da atuação estatal (Lopes Jr., 2020).

Diante desse contexto, a utilização de inteligência artificial na investigação criminal deve ser acompanhada de uma estrutura técnica e jurídica capaz de garantir a confiabilidade dos dados utilizados, não se tratando apenas de incorporação de tecnologias avançadas, mas da garantia de que sua aplicação esteja alinhada a critérios rigorosos de validade e controle.

A ausência de observância rigorosa desses procedimentos pode gerar consequências processuais relevantes. Como exemplo, a não preservação adequada de logs de acesso pode inviabilizar a comprovação de que os dados analisados não sofreram manipulação indevida.

Da mesma forma, a inexistência de registro do processo de extração e tratamento de dados pode comprometer a confiabilidade dos resultados apresentados, levando à sua desconsideração pelo juízo. Em casos mais graves, a quebra da rastreabilidade pode resultar na invalidação de elementos utilizados na

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

investigação, afetando diretamente a admissibilidade e a valoração no processo penal.

A preservação da cadeia de custódia, especialmente no ambiente digital, é condição indispensável para que os resultados produzidos mantenham consistência técnica e aceitação jurídica, contribuindo para uma atuação investigativa responsável e fundamentada.

Nesse sentido, a cadeia de custódia no ambiente digital não se limita à preservação do dado em si, mas envolve a documentação integral de todos os processos técnicos que incidem sobre ele, incluindo sua transformação em produtos analíticos. A ausência desse controle compromete não apenas a confiabilidade técnica, mas também a legitimidade jurídica dos elementos produzidos.

4.1 VIESES ALGORÍTMICOS E A SELETIVIDADE PENAL TECNOLÓGICA

A utilização de inteligência artificial na investigação criminal traz consigo desafios que ultrapassam o campo técnico e alcançam dimensões éticas e jurídicas profundas, destacando-se dentre eles, a reprodução de vieses estruturais presentes nos dados utilizados para o treinamento dos sistemas algorítmicos.

Como esses sistemas aprendem a partir de registros históricos, acabam incorporando padrões já existentes, inclusive aqueles marcados por desigualdades sociais e práticas discriminatórias (O'Neil, 2021).

Quando bases de dados refletem abordagens policiais seletivas, direcionadas com maior intensidade a determinados grupos sociais, os algoritmos tendem a replicar esse padrão.

Isso significa que populações historicamente vulnerabilizadas, como pessoas negras, moradores de periferias e grupos economicamente marginalizados, podem continuar sendo alvos prioritários de investigações mediadas por tecnologia. Nessa perspectiva, a automação não elimina distorções, mas pode reforçá-las de forma mais ampla e silenciosa.

Pesquisas empíricas no campo da governança algorítmica demonstram que sistemas utilizados em contextos penais tendem a reproduzir padrões discriminatórios quando treinados com dados historicamente enviesados, afetando de forma

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

desproporcional grupos socialmente vulneráveis (Angwin *et al*., 2016; Eubanks, 2018). Esses achados reforçam a necessidade de análise crítica sobre os impactos sociais e jurídicos dessas tecnologias.

Com base nessa diferenciação, é possível propor uma matriz de riscos jurídicos associada ao uso da inteligência artificial na investigação criminal. Nos sistemas de apoio informacional, predominam riscos relacionados à privacidade e ao tratamento excessivo de dados.

Nos sistemas de apoio pericial, destacam-se riscos ligados à integridade e à rastreabilidade dos dados analisados. Já nos sistemas de apoio decisório, os riscos assumem maior gravidade, envolvendo a possibilidade de comprometimento da imparcialidade, da presunção de inocência e da racionalidade decisória.

Essa matriz permite compreender que nem todos os usos da inteligência artificial apresentam o mesmo grau de impacto jurídico, sendo necessário calibrar os mecanismos de controle conforme a natureza da aplicação tecnológica.

No caso de sistemas voltados à mineração de dados, os riscos concentram-se na coleta excessiva e no tratamento indevido de informações pessoais. Já em ferramentas preditivas, destaca-se a possibilidade de reforço de padrões discriminatórios e antecipação indevida de suspeitas.

Por sua vez, sistemas de suporte à decisão apresentam riscos mais sensíveis, na medida em que podem influenciar diretamente a formação do convencimento estatal, afetando garantias como o contraditório, a ampla defesa e a presunção de inocência.

Essa interpretação, contudo, não pode ser tratada como mera hipótese teórica, uma vez que estudos empíricos já demonstram que sistemas automatizados tendem a reproduzir desigualdades estruturais quando alimentados por bases de dados historicamente enviesadas.

Esse fenômeno, denominado seletividade penal tecnológica, desafia diretamente o princípio da igualdade, posto a aparência de neutralidade dos sistemas algorítmicos contribuir para a naturalização de seus resultados, dificultando a identificação de distorções e a contestação por parte dos indivíduos afetados.

Essa opacidade não impacta apenas a compreensão dos resultados, mas

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

também compromete a própria auditabilidade da cadeia de custódia, na medida em que dificulta a reconstrução do percurso informacional que levou à produção de determinada inferência.

A impossibilidade de rastrear as etapas intermediárias do processamento algorítmico fragiliza o controle jurídico sobre a origem e a integridade dos dados utilizados.

A lógica matemática que sustenta esses sistemas tende a conferir uma aura de objetividade, o que pode enfraquecer o debate crítico e limitar o espaço para questionamentos no âmbito jurídico (Pasquale, 2015).

Nesse contexto, torna-se essencial diferenciar correlação estatística de prova juridicamente relevante. Sistemas de inteligência artificial operam, em grande medida, a partir da identificação de padrões probabilísticos, os quais não necessariamente estabelecem nexos causais ou imputações individualizadas.

A transposição direta dessas correlações para o campo jurídico pode resultar em conclusões inadequadas, incompatíveis com o padrão de certeza exigido no processo penal.

No Brasil, essa problemática assume contornos ainda mais delicados. A estrutura social desigual e o histórico de atuação seletiva das instituições de controle penal evidenciam o risco de que a tecnologia seja utilizada como mecanismo de reforço dessas assimetrias.

A Constituição Federal (CRFB/88), ao estabelecer a igualdade como direito fundamental e ao vedar qualquer forma de discriminação, impõe limites claros à atuação estatal, inclusive quando mediada por recursos tecnológicos.

Nesse sentido, a Resolução nº 332/2020 do Conselho Nacional de Justiça (CNJ) representa um avanço ao estabelecer diretrizes para o uso de inteligência artificial no âmbito do Poder Judiciário.

O normativo determina que os sistemas devem observar princípios como transparência, explicabilidade, responsabilização e não discriminação, reforçando a necessidade de controle sobre o funcionamento dessas ferramentas.

Ainda assim, a existência de diretrizes normativas não é suficiente para garantir sua efetividade, tornando-se indispensável a implementação de mecanismos concretos

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

de auditoria, capazes de identificar padrões discriminatórios e corrigir distorções ao longo do ciclo de funcionamento dos sistemas.

Além disso, é fundamental que haja responsabilização clara dos agentes envolvidos no desenvolvimento e na utilização dessas tecnologias, assegurando que eventuais impactos negativos não permaneçam sem resposta institucional, sobretudo diante de um modelo tecnológico que, ao capturar e processar dados comportamentais em larga escala, tende a reproduzir e intensificar mecanismos de controle e predição social (Zuboff, 2019).

Diante desse quadro, a incorporação da inteligência artificial na investigação criminal exige uma postura crítica e responsável, devendo o uso dessas ferramentas ser orientado por critérios que priorizem a justiça, a equidade e o respeito às garantias fundamentais.

4.2 O PAPEL DO PODER JUDICIÁRIO ENTRE A EFICIÊNCIA E O GARANTISMO

O Poder Judiciário ocupa posição estratégica na estrutura institucional brasileira, exercendo não apenas a função de resolver conflitos, mas também a de assegurar a proteção dos direitos fundamentais frente à atuação estatal.

Sua atuação ganha especial relevância no contexto da investigação criminal mediada por inteligência artificial, em que se exige uma postura crítica diante de elementos produzidos por sistemas tecnológicos complexos.

Cabe ao juiz, nesse cenário, não apenas receber tais elementos, mas avaliar sua validade, sua origem e sua compatibilidade com os parâmetros jurídicos estabelecidos (Ferrajoli, 2014).

Para além da verificação formal dos elementos apresentados, impõe-se considerar os limites epistêmicos inerentes aos sistemas de inteligência artificial, pois, ainda que devidamente regulados e auditáveis, tais sistemas podem produzir inferências baseadas em probabilidades, cujo valor cognitivo não é suficiente para sustentar imputações penais individualizadas. Isso exige do julgador não apenas a análise da legalidade do meio empregado, mas também a avaliação crítica da qualidade do conhecimento produzido.

Nesse contexto, impõe-se distinguir o uso da inteligência artificial como

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

ferramenta auxiliar, destinada à organização e análise de dados, daquele em que há efetiva influência sobre o processo decisório. Enquanto o primeiro pode ser compreendido como instrumento técnico de apoio, o segundo exige maior rigor jurídico, uma vez que pode impactar diretamente a formação do convencimento e a valoração dos elementos probatórios.

A incorporação de ferramentas tecnológicas no campo investigativo introduz um desafio significativo à função jurisdicional dada a crescente complexidade dos crimes cibernéticos e o volume expressivo de dados analisados por sistemas automatizados os quais podem induzir à aceitação acrítica dos resultados apresentados por tais ferramentas.

Essa dinâmica pode fragilizar o papel do magistrado, que corre o risco de assumir posição meramente homologatória, afastando-se de sua responsabilidade de análise autônoma e fundamentada.

Essa tendência revela uma fragilidade institucional preocupante, na medida em que transfere, ainda que de forma indireta, o núcleo da decisão judicial para sistemas tecnológicos cuja lógica interna não é plenamente acessível ou controlável.

Diante disso, torna-se essencial reafirmar os pilares do processo penal, especialmente o devido processo legal, o contraditório e a exigência de fundamentação das decisões judiciais.

O julgador deve ser capaz de compreender, ao menos em nível suficiente, os critérios que orientaram a produção das informações utilizadas no processo. A ausência dessa compreensão compromete a racionalidade da decisão e dificulta o exercício pleno da defesa, o que se revela incompatível com os parâmetros constitucionais (Lopes Jr., 2020).

A Resolução nº 332/2020 do CNJ representa um esforço institucional relevante ao estabelecer diretrizes para o uso da inteligência artificial no âmbito do Judiciário, reforçando princípios como transparência, explicabilidade e responsabilidade, indicando que a utilização dessas ferramentas deve estar submetida a critérios que permitam controle e verificação. Essa orientação busca evitar que a tecnologia seja incorporada de forma automática, sem a devida reflexão sobre seus impactos.

Além disso, a reflexão proposta por Guedes (2018) reforça a centralidade da

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

dignidade da pessoa humana como limite inafastável da atuação estatal. Mesmo diante da complexidade das investigações contemporâneas, o respeito aos direitos fundamentais não pode ser relativizado. A legitimidade das decisões judiciais depende da fidelidade a esses princípios, que funcionam como parâmetro de validade para toda atuação no âmbito penal.

Diante disso, a capacitação técnica dos magistrados revela-se medida indispensável uma vez que a compreensão dos fundamentos básicos dos sistemas de inteligência artificial permite uma atuação mais consciente e crítica, evitando a transferência indevida da função decisória para mecanismos automatizados. O juiz deve permanecer como protagonista na formação do convencimento, exercendo seu papel de forma ativa e responsável.

Assim, o uso da inteligência artificial no processo penal exige um Judiciário atento, preparado e compromissado com a análise rigorosa dos elementos submetidos à sua apreciação, não podendo a atuação jurisdicional ser substituída por respostas automatizadas, devendo preservar sua natureza fundamentada e reflexiva.

Dessa forma, a legitimidade das decisões judiciais dependerá da adoção de parâmetros que garantam clareza, possibilidade de verificação e respeito efetivo às garantias fundamentais, evitando que a atuação jurisdicional se distancie de sua base racional e jurídica.

5 SÍNTESE ANALÍTICA E IMPLICAÇÕES

A partir do percurso analítico desenvolvido, é possível sistematizar os principais achados deste estudo em eixos interpretativos que evidenciam as implicações jurídicas do uso da inteligência artificial na investigação criminal. Essa abordagem permite ultrapassar a mera descrição dos fenômenos, destacando os elementos centrais que estruturam o debate contemporâneo sobre a interface entre tecnologia e processo penal.

O primeiro eixo analítico refere-se à distinção entre eficiência operacional e legitimidade jurídica. Verificou-se que, embora a inteligência artificial amplie significativamente a capacidade investigativa do Estado, sobretudo no tratamento de grandes volumes de dados e na identificação de padrões, tal incremento não se traduz

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

automaticamente em conformidade com os parâmetros jurídicos exigidos. A eficiência tecnológica, quando desvinculada de critérios de controle, transparência e verificabilidade, revela-se insuficiente para sustentar práticas investigativas compatíveis com as garantias fundamentais.

O segundo eixo diz respeito à centralidade da cadeia de custódia no ambiente digital. Constatou-se que a confiabilidade dos resultados produzidos por sistemas algorítmicos depende diretamente da integridade, rastreabilidade e documentação dos dados utilizados. Nesse contexto, a cadeia de custódia não se limita à preservação do vestígio digital bruto, mas abrange também os processos de transformação dos dados em produtos analíticos, exigindo mecanismos técnicos capazes de assegurar a integridade informacional ao longo de todo o ciclo investigativo.

O terceiro eixo analítico concentra-se nos limites epistêmicos da inteligência artificial. Observou-se que sistemas baseados em inferências probabilísticas operam predominantemente por meio de correlações estatísticas, as quais não necessariamente produzem conhecimento apto a sustentar imputações penais individualizadas. Ainda que tais sistemas apresentem elevado desempenho técnico, sua utilização no processo penal exige cautela, uma vez que a conversão de padrões probabilísticos em elementos de convicção pode comprometer o grau de certeza exigido para a responsabilização jurídica.

Esse diagnóstico encontra respaldo em estudos interdisciplinares que apontam limitações estruturais na utilização de sistemas algorítmicos em contextos decisórios sensíveis, nos quais a precisão estatística não se traduz automaticamente em adequação jurídica (Ferguson, 2017; Kroll et al., 2017).

O quarto eixo refere-se aos riscos de reprodução de seletividade penal por meio de sistemas automatizados. A análise demonstrou que, quando alimentados por bases de dados historicamente marcadas por desigualdades sociais, os sistemas de inteligência artificial tendem a reproduzir e, em alguns casos, intensificar padrões discriminatórios. Essa dinâmica revela que a tecnologia, longe de ser neutra, pode atuar como vetor de reforço de assimetrias estruturais, exigindo mecanismos rigorosos de controle e supervisão.

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

A partir desses eixos, torna-se possível delinear implicações relevantes para o campo jurídico. Em primeiro lugar, revela-se a necessidade de diferenciação entre os usos da inteligência artificial, distinguindo-se aplicações de natureza informacional, pericial e decisória. Essa distinção permite calibrar o grau de exigência jurídica conforme o impacto potencial da tecnologia sobre o processo penal, reconhecendo que sistemas com influência decisória direta demandam níveis mais elevados de controle e justificativa.

Em segundo lugar, verifica-se que a legitimidade do uso da inteligência artificial não pode ser aferida exclusivamente pela observância formal de requisitos legais, sendo indispensável considerar a qualidade epistemológica dos resultados produzidos. A mera transparência dos sistemas não garante sua adequação ao processo penal, tornando-se necessário avaliar a consistência e a relevância das inferências geradas para fins de imputação jurídica.

Por fim, destaca-se que a incorporação da inteligência artificial na investigação criminal impõe ao sistema de justiça o desafio de desenvolver critérios normativos e metodológicos capazes de compatibilizar inovação tecnológica e garantias fundamentais. A ausência desses parâmetros pode comprometer não apenas a validade dos elementos produzidos, mas também a própria racionalidade do processo penal.

Diante disso, a análise desenvolvida permite afirmar que o principal desafio não reside na incorporação da inteligência artificial em si, mas na definição de critérios que delimitem sua utilização de forma juridicamente adequada.

A construção de um modelo que articule tipologia de usos, identificação de riscos e parâmetros de legitimidade revela-se essencial para assegurar que a tecnologia atue como instrumento de aprimoramento investigativo, e não como fator de fragilização das garantias que estruturam o sistema de justiça criminal.

6 CONSIDERAÇÕES FINAIS

O presente estudo analisou a aplicação da inteligência artificial na investigação de crimes cibernéticos, com foco em suas implicações jurídicas e nos desafios decorrentes de sua incorporação ao sistema de justiça criminal brasileiro.

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

A partir da análise desenvolvida, foi possível constatar que as tecnologias baseadas em sistemas algorítmicos oferecem contribuições relevantes para a atividade investigativa, sobretudo no tratamento de grandes volumes de dados e na identificação de padrões complexos, ampliando a capacidade operacional do Estado diante das novas dinâmicas da criminalidade digital.

Entretanto, também se verificou que tais avanços não podem ser compreendidos de forma isolada, desvinculados dos limites impostos pelos direitos e garantias fundamentais.

A utilização de inteligência artificial no contexto penal traz consigo riscos que envolvem a opacidade dos sistemas, a fragilidade da cadeia de custódia de dados digitais, a reprodução de vieses discriminatórios e a possibilidade de enfraquecimento do controle jurisdicional.

Esses fatores demonstram que a eficiência tecnológica, por si só, não é suficiente para assegurar a legitimidade da atuação estatal. A incorporação de ferramentas baseadas em inteligência artificial exige a observância de critérios jurídicos rigorosos, capazes de garantir transparência, controle e conformidade com os direitos fundamentais.

Assim, a legitimidade da atuação estatal passa a depender não apenas dos resultados alcançados, mas também da adequação dos meios empregados e da possibilidade de sua verificação e contestação no âmbito do processo.

A análise evidenciou, ainda, que o ordenamento jurídico brasileiro dispõe de instrumentos relevantes para disciplinar o uso de dados e tecnologias no âmbito investigativo, como o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais e as diretrizes estabelecidas pelo Conselho Nacional de Justiça.

Contudo, a ausência de regulamentação específica voltada à utilização da inteligência artificial na persecução penal revela a necessidade de aprimoramento normativo, capaz de acompanhar as transformações tecnológicas sem comprometer a proteção dos direitos individuais.

Nesse sentido, destaca-se o papel do Poder Judiciário como instância essencial de controle, responsável por assegurar que os elementos produzidos com apoio tecnológico sejam submetidos a critérios rigorosos de análise, compreensão e

REMUNOM
ISSN 2178-6925
Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

fundamentação.

A atuação judicial deve permanecer pautada pela autonomia decisória e pela exigência de racionalidade, evitando a delegação indevida de decisões a sistemas automatizados.

Diante disso, conclui-se que a incorporação da inteligência artificial na investigação criminal deve ser orientada por um modelo que privilegie a transparência, a possibilidade de verificação dos processos utilizados e o respeito integral às garantias fundamentais.

A tecnologia deve atuar como instrumento de apoio à atividade estatal, e não como substituto da análise humana ou como elemento de obscurecimento dos critérios decisórios.

Assim, destaca-se que o avanço tecnológico impõe ao direito o desafio permanente de adaptação, exigindo uma postura crítica e reflexiva por parte dos operadores jurídicos.

A construção de um ambiente investigativo que concilie inovação e proteção de direitos depende da adoção de parâmetros claros, do fortalecimento dos mecanismos de controle e do compromisso institucional com a justiça e a equidade.

Nesse sentido, verifica-se que parte significativa do debate ainda permanece centrada na eficiência tecnológica, negligenciando a necessidade de construção de critérios jurídicos robustos capazes de limitar e orientar o uso dessas ferramentas.

Nesse contexto, a principal contribuição deste estudo consiste na proposição de uma estrutura analítica que articula tipologia de usos, matriz de riscos e parâmetros de legitimidade, permitindo uma abordagem mais precisa e diferenciada do impacto da inteligência artificial na investigação criminal.

Portanto, nessa perspectiva, a integração da inteligência artificial ao sistema de justiça exige a consolidação de parâmetros normativos e operacionais que assegurem controle, auditabilidade e conformidade com os direitos fundamentais, de modo que a inovação tecnológica seja incorporada de forma responsável, sem comprometer a racionalidade decisória, a segurança jurídica e a legitimidade das práticas institucionais.

REMUNOM
ISSN 2178-6925

Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

REFERÊNCIAS

ANGWIN, Julia; LARSON, Jeff; MATTU, Surya; KIRCHNER, Lauren. **Machine bias**. ProPublica, 2016. Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Acesso em: 02 mar. 2026.

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

BRASIL. **Lei nº 7.210**, de 11 de julho de 1984. Institui a Lei de Execução Penal. Diário Oficial [da] República Federativa do Brasil, Brasília, 13 jul. 1984.

BRASIL. **Lei nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, 3 dez. 2012.

BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial [da] República Federativa do Brasil, Brasília, 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] República Federativa do Brasil, Brasília, 15 ago. 2018.

BRASIL. CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Resolução nº 332**, de 21 de agosto de 2020. Dispõe sobre a ética, transparência e governança na produção e no uso de Inteligência Artificial no Poder Judiciário. Brasília: CNJ, 25 ago. 2020.

BRAYNE, Sarah. **Predict and surveil: data, discretion, and the future of policing**. New York: Oxford University Press, 2020.

CARRIER, Brian. **File system forensic analysis**. Boston: Addison-Wesley, 2005.

CASEY, Eoghan. **Digital evidence and computer crime: forensic science, computers and the internet**. 3. ed. Amsterdam: Academic Press, 2011.

EUBANKS, Virginia. **Automating inequality: how high-tech tools profile, police, and punish the poor**. New York: St. Martin's Press, 2018.

FERGUSON, Andrew Guthrie. **The rise of big data policing: surveillance, race, and the future of law enforcement**. New York: New York University Press, 2017.

FERRAJOLI, Luigi. **Direito e razão: teoria do garantismo penal.** Tradução de Ana Paula Zomer *et al*. 4. ed. São Paulo: Revista dos Tribunais, 2014.

REMUNOM
ISSN 2178-6925

Received: 20/03/2026 - **Accepted:** 07/04/2026
Vol: 13.05
DOI: 10.66104/4xnfbh10
Pages: 1-28

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**. Tradução de Raquel Ramalhete. 41. ed. Petrópolis: Vozes, 2013.

GUEDES, Néviton. **Por que a sociedade deve respeitar a dignidade da pessoa humana do criminoso?** Consultor Jurídico, São Paulo, 02 jul. 2018. Disponível em: https://www.conjur.com.br/2018-jul-02/constituicao-poder-respeitar-dignidade-pessoa-humana-criminoso/. Acesso em: 02 mar. 2026.

KROLL, Joshua A.; HUEY, Joanna; BAROCAS, Solon; FELTEN, Edward W.; REIDENBERG, Joel R.; ROBINSON, David G.; YU, Harlan. **Accountable algorithms**. University of Pennsylvania Law Review, Philadelphia, v. 165, n. 3, p. 633–705, 2017.

LOPES JR., Aury. **Direito processual penal**. 17. ed. São Paulo: Saraiva, 2020.

MORAES, Maria Celina Bodin de. **O conceito de dignidade humana: substrato axiológico e conteúdo normativo**. Porto Alegre: Livraria do Advogado, 2018.

NADER, Paulo. **Introdução ao estudo do direito**. 40. ed. Rio de Janeiro: Forense, 2017.

O'NEIL, Cathy. **Algoritmos de destruição em massa: como o Big Data aumenta a desigualdade e ameaça a democracia**. Tradução de Rafael Abraham. 1. ed. Santo André: Editora Rua do Sabão, 2021.

PASQUALE, Frank. **The black box society: the secret algorithms that control money and information**. Cambridge: Harvard University Press, 2015.

SANTOS, Bruno Morais di. **A evolução histórica do sistema prisional e a tecnologia**. Brasília: Universidade de Brasília, 2017.

STEVENS, Hallam. **A vigilância digital**. São Paulo: Contexto, 2022.

ZUBOFF, Shoshana. **The age of surveillance capitalism: the fight for a human future at the new frontier of power**. New York: PublicAffairs, 2019.