v7.n12.2026

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

O USO DA INTELIGÊNCIA ARTIFICIAL NA INVESTIGAÇÃO CRIMINAL: RISCO À LEGALIDADE E À AMPLA DEFESA

THE USE OF ARTIFICIAL INTELLIGENCE IN CRIMINAL INVESTIGATION: RISK TO LEGALITY AND TO THE RIGHT TO A FULL DEFENSE

EL USO DE LA INTELIGENCIA ARTIFICIAL EN LA INVESTIGACIÓN CRIMINAL: RIESGO PARA LA LEGALIDAD Y LA AMPLIA DEFENSA

Kathleen Sousa Silva[1], Guilherme Soares Vieira[2], Pedro Henrique Oliveira[3], Marcus Vinícius Silva Coelho[4], Vitor Martins Cortizo[5]

https://doi.org/10.47820/recima21.v7i12.9956

PUBLICADO: 12/2026

RESUMO

O avanço do uso de ferramentas de inteligência artificial na investigação criminal, empregadas em atividades como reconhecimento facial, cruzamento de bases de dados, identificação de vínculos e análise automatizada de padrões, ampliou as possibilidades investigativas e levantou discussões sobre transparência, confiabilidade e controle dos resultados. O objetivo do estudo foi avaliar em que medida a utilização desses sistemas pode comprometer a legalidade dos atos investigativos e limitar a capacidade da defesa de conhecer, compreender e contestar inferências algorítmicas. Adotou-se abordagem qualitativa, de caráter exploratório e descritivo, desenvolvida pelo método dedutivo e por meio de pesquisa bibliográfica e documental, com base em doutrina, artigos científicos, legislação, atos administrativos, documentos nacionais e internacionais e jurisprudência. Os resultados indicaram que a inteligência artificial pode contribuir para a eficiência investigativa, porém sua utilização apresenta riscos quando os sistemas operam com baixa transparência, documentação insuficiente, limitações de acesso pela defesa ou ausência de supervisão humana efetiva. Verificou-se, ainda, que o ordenamento jurídico brasileiro possui fundamentos constitucionais, processuais e administrativos capazes de estabelecer controles, embora permaneçam lacunas quanto à disciplina específica da contestação de resultados algorítmicos. Concluiu-se que a inteligência artificial não é incompatível, por si só, com a investigação criminal, mas que sua utilização somente se mostra juridicamente legítima quando acompanhada de transparência suficiente, rastreabilidade, controle humano, possibilidade de verificação técnica e condições concretas para o exercício da ampla defesa.

PALAVRAS-CHAVE: Inteligência artificial. Investigação criminal. Ampla defesa. Legalidade. Prova algorítmica.

ABSTRACT

The increasing use of artificial intelligence tools in criminal investigations, including facial recognition, database cross-referencing, link identification, and automated pattern analysis, has expanded investigative possibilities and raised discussions concerning transparency, reliability, and control over the results produced. The objective of this study was to assess the extent to which the use of these systems may compromise the legality of investigative acts and limit the

[1] Graduanda em Direito pela Universidade Evangélica de Goiás (UniEVANGÉLICA), Campus Ceres (GO).
[2] Doutor em Direitos Humanos pela Universidade Federal de Goiás (PPGDH/UFG). Docente na Universidade Evangélica de Goiás – UniEVANGÉLICA, Campus Ceres (GO), na área de Direito.
[3] Especialista em Docência Universitária. Docente na Universidade Evangélica de Goiás – UniEVANGÉLICA, Campus Ceres (GO), na área de Direito.
[4] Mestre em Língua, Literatura e Interculturalidade pela Universidade Estadual de Goiás (UEG). Docente na Universidade Evangélica de Goiás – UniEVANGÉLICA, Campus Ceres (GO), na área de Direito.
[5] Especialista pela Escola da Magistratura do Estado do Paraná, Campus Umuarama, Paraná, Brasil. Docente na Universidade Evangélica de Goiás – UniEVANGÉLICA, Campus Ceres (GO), na área de Direito.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

defense's ability to know, understand, and challenge algorithmic inferences. A qualitative, exploratory, and descriptive approach was adopted, using the deductive method and bibliographic and documentary research based on legal scholarship, scientific articles, legislation, administrative regulations, national and international documents, and case law. The results indicated that artificial intelligence may contribute to investigative efficiency, although its use presents risks when systems operate with limited transparency, insufficient documentation, restricted access for the defense, or inadequate human oversight. It was also found that the Brazilian legal system provides constitutional, procedural, and administrative grounds for establishing controls, although gaps remain regarding specific rules for challenging algorithmic results. It was concluded that artificial intelligence is not inherently incompatible with criminal investigations, but its use can only be considered legally legitimate when accompanied by sufficient transparency, traceability, human oversight, technical verifiability, and concrete conditions for the effective exercise of the right to a full defense.

KEYWORDS: *Artificial intelligence. Criminal investigation. Right to a full defense. Legality. Algorithmic evidence.*

RESUMEN

El avance del uso de herramientas de inteligencia artificial en la investigación criminal, empleadas en actividades como el reconocimiento facial, el cruce de bases de datos, la identificación de vínculos y el análisis automatizado de patrones, amplió las posibilidades investigativas y suscitó discusiones sobre la transparencia, la fiabilidad y el control de los resultados. El objetivo del estudio fue evaluar en qué medida la utilización de estos sistemas puede comprometer la legalidad de los actos investigativos y limitar la capacidad de la defensa para conocer, comprender e impugnar inferencias algorítmicas. Se adoptó un enfoque cualitativo, de carácter exploratorio y descriptivo, desarrollado mediante el método deductivo y la investigación bibliográfica y documental, con base en doctrina, artículos científicos, legislación, actos administrativos, documentos nacionales e internacionales y jurisprudencia. Los resultados indicaron que la inteligencia artificial puede contribuir a la eficiencia investigativa, aunque su uso presenta riesgos cuando los sistemas operan con baja transparencia, documentación insuficiente, limitaciones de acceso por parte de la defensa o ausencia de supervisión humana efectiva. Se verificó, además, que el ordenamiento jurídico brasileño posee fundamentos constitucionales, procesales y administrativos capaces de establecer controles, aunque persisten lagunas en cuanto a la regulación específica de la impugnación de resultados algorítmicos. Se concluyó que la inteligencia artificial no es incompatible, por sí sola, con la investigación criminal, pero que su utilización solo resulta jurídicamente legítima cuando va acompañada de transparencia suficiente, trazabilidad, control humano, posibilidad de verificación técnica y condiciones concretas para el ejercicio de la amplia defensa.

PALABRAS CLAVE: *Inteligencia artificial. Investigación criminal. Amplia defensa. Legalidad. Prueba algorítmica.*

1. INTRODUÇÃO

O uso de tecnologias digitais na segurança pública ampliou as formas de coletar, organizar e analisar informações nas investigações criminais, com ferramentas de inteligência artificial capazes de processar grande volume de dados, cruzar registros, identificar vínculos e auxiliar no reconhecimento de pessoas. Essas tecnologias trazem questões jurídicas sobre a

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

forma como os resultados são produzidos e utilizados pelo Estado, principalmente quando uma inferência algorítmica interfere na identificação de suspeitos, no direcionamento de diligências ou na adoção de medidas que podem atingir direitos individuais. Como destaca Guasque (2025), sistemas capazes de afetar direitos fundamentais devem estar sujeitos a mecanismos de transparência, supervisão e controle compatíveis com os efeitos de sua utilização.

Os resultados dessas ferramentas não são necessariamente neutros ou infalíveis. Moreira (2022), ao analisar o reconhecimento facial no Brasil, chama atenção para casos de identificações equivocadas e para as consequências que falhas tecnológicas podem produzir sobre pessoas submetidas à atuação estatal. Além disso, a dificuldade de compreender como alguns sistemas chegam a uma classificação, correspondência ou associação pode limitar a contestação desses resultados, situação que, segundo Oliveira e Bedê Jr. (2026), se torna ainda mais problemática quando as informações algorítmicas passam a ser utilizadas por diferentes instituições ao longo da persecução penal. A busca por maior eficiência na apuração, portanto, não autoriza o uso de resultados automatizados sem controle nem afasta garantias como a legalidade, o devido processo legal, o contraditório e a ampla defesa.

No Brasil, a regulamentação do tema ainda é fragmentada, embora já existam instrumentos voltados ao controle dessas tecnologias, como a Portaria MJSP nº 961/2025 (Brasil, 2025b).

Diante disso, o problema que orienta a pesquisa pode ser expresso pela seguinte questão: em que medida o uso da inteligência artificial na investigação criminal pode comprometer a legalidade dos atos investigativos e o exercício efetivo da ampla defesa quando o investigado não consegue compreender como o sistema chegou ao resultado, quais dados foram utilizados e se a conclusão apresentada é confiável? Parte-se da compreensão de que a inteligência artificial pode ser utilizada na investigação criminal, desde que seus resultados sejam transparentes, devidamente documentados, passíveis de reconstrução, submetidos à supervisão humana e acessíveis à contestação pela defesa.

A relevância do estudo decorre da expansão dessas tecnologias e da possibilidade de que elas interfiram na própria formação da suspeita, em um contexto de possível restrição de direitos e de desigualdade entre o poder investigativo estatal e os meios disponíveis ao investigado.

O objetivo geral foi analisar o uso da inteligência artificial na investigação criminal e sua relação com a legalidade e a ampla defesa. Como objetivos específicos, buscou-se identificar as principais formas de aplicação dessas tecnologias na atividade investigativa; examinar seus efeitos sobre a legalidade e os limites jurídicos impostos à atuação estatal; e analisar de que

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

modo a baixa transparência dos sistemas pode dificultar o acesso da defesa às informações, a compreensão dos resultados e sua contestação técnica.

2. REFERENCIAL TEÓRICO

2.1. Inteligência artificial e aprendizado de máquina na investigação criminal

A inteligência artificial (IA) pode ser conceituada como a simulação de funções cognitivas humanas por sistemas computacionais, permitindo a execução de tarefas que, tradicionalmente, dependem da inteligência humana, tais como reconhecimento de fala, visão computacional, tomada de decisões, aprendizado e resolução de problemas (Heidrich, 2020 *apud* Costa; Feller, 2025). Bonat e Peixoto (2020 *apud* Costa; Feller, 2025) acrescentam a possibilidade de os sistemas executarem funções cognitivas com certo nível de autonomia. Essa autonomia, contudo, não significa independência das escolhas humanas, pois o funcionamento da ferramenta continua condicionado à programação, aos dados utilizados e à finalidade estabelecida.

O aprendizado de máquina (*machine learning*) permite que o sistema melhore seu desempenho a partir da análise de dados anteriores, identificando padrões e ajustando seu funcionamento conforme as informações processadas. Russell e Norvig (2021 *apud* Amaral; Xavier, 2022) classificam esse aprendizado em três modalidades principais: supervisionado, não supervisionado e por reforço.

No aprendizado supervisionado, o sistema recebe dados previamente rotulados e aprende a relacionar características a respostas conhecidas. Sardana, Marwaha e Bhatnagar (2021) explicam que essa modalidade pode ser utilizada para estimar quais crimes tendem a ocorrer com maior frequência em determinada região, com base em registros anteriores de locais, horários e tipos de delitos. Hennig Leal e Moreschi Paulo (2023), porém, advertem que dados históricos marcados por desigualdades podem fazer com que os algoritmos reproduzam e ampliem os mesmos padrões discriminatórios, de modo que registros de uma atuação policial seletiva podem concentrar abordagens em determinados bairros ou grupos sociais, em prejuízo da presunção de inocência.

No aprendizado não supervisionado, os dados não possuem classificação prévia e o próprio sistema busca identificar relações e agrupamentos, utilizando técnicas como a clusterização para encontrar estruturas ainda não conhecidas (Russell; Norvig, 2021 *apud* Amaral; Xavier, 2022), o que pode ajudar a localizar redes de relacionamento ou movimentações atípicas. Pedroso e Santos (2024), contudo, demonstram que a dificuldade de compreender os

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

critérios utilizados pelos sistemas algorítmicos reduz a possibilidade de questionar os resultados por eles produzidos.

Já o aprendizado por reforço funciona por meio de recompensas e penalidades. Sardana, Marwaha e Bhatnagar (2021) apontam sua aplicação ao planejamento do patrulhamento, com a ferramenta modificando suas recomendações a partir das intervenções anteriores. Ao analisar a predição criminal no Brasil, Silva *et al.* (2026) observam que a utilização de dados históricos, somada à falta de transparência, pode favorecer a continuidade da seletividade penal e do racismo estrutural.

Em síntese, cada modalidade pode reproduzir classificações discriminatórias, converter correlações estatísticas em suspeitas ou perpetuar ciclos de vigilância, e o desconhecimento dos dados e critérios do sistema compromete a legalidade da investigação e a contestação da origem da suspeita.

2.2. Aplicações da inteligência artificial na atividade investigativa

De acordo com a Unesco (2018), o uso massivo de dados coletados por governos e empresas privadas, aliado aos fluxos contínuos de informação, gerou ferramentas com potencial não apenas para vigilância em larga escala, mas também para exclusão e repressão. Entre as aplicações investigativas estão o cruzamento de registros públicos e privados, a análise de movimentações financeiras, a identificação de vínculos entre pessoas e a busca por comportamentos fora do padrão, recursos que, segundo Costa e Feller (2025), podem facilitar a organização das informações e a descoberta de relações relevantes para a apuração. Como um vínculo pode ser familiar, profissional ou ocasional e uma movimentação atípica pode ter origem lícita, essas associações devem apenas orientar a apuração e ser confirmadas por outros elementos.

O reconhecimento facial exige cuidado especial. Segundo Moreira (2022), na segurança pública, imagens captadas por câmeras inteligentes são comparadas com registros armazenados em bancos de dados, e o sistema emite alertas quando há correspondência com pessoas com mandados ou pendências legais. Couto *et al.* (2025) esclarecem que o sistema localiza a face, analisa mais de 80 pontos nodais e transforma essas informações em uma representação matemática comparável aos perfis armazenados, distinguindo a autenticação facial (“1 para 1”) da correspondência facial (“1 para muitos”). Por ser probabilística, a correspondência depende da qualidade da imagem, das condições da captura e do banco consultado, de modo que o alerta não confirma a identidade e deve ser conferido por um agente.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Os erros registrados no Brasil mostram as consequências da confiança excessiva nesse tipo de resultado. Moreira (2022) relata que, em 2019, no Distrito Federal, um jovem de 23 anos foi apontado por laudo de reconhecimento facial como autor de roubo a ônibus, embora acompanhasse a mãe em um cartório no momento do crime; que, em 2021, um pedreiro de 52 anos foi preso em Ilha Grande (PI) e conduzido ao Distrito Federal após ser confundido com um fraudador de cartões de crédito, permanecendo detido durante três dias até o reconhecimento do engano; e que outros equívocos ocorreram no Rio de Janeiro e em Salvador. Os nomes, divulgados na fonte, foram omitidos em respeito à privacidade dos envolvidos. Esses casos mostram que, quando o resultado automatizado é aceito sem outra prova, o indivíduo precisa demonstrar que não é a pessoa indicada pelo sistema, em inversão da presunção de inocência e com restrição concreta da liberdade (Brasil, 1988).

Os episódios confirmam a observação de Couto *et al.* (2025) de que pessoas distintas podem gerar amostras semelhantes, surgindo falsos positivos e falsos negativos. A Unesco (2018) acrescenta que distorções na captura das imagens podem levar à classificação incorreta de pessoas e que os sistemas podem repetir os vieses presentes nos dados usados em seu desenvolvimento, estigmatizando determinados grupos.

Juridicamente, o reconhecimento facial deve ser tratado como um indício inicial, confirmado pela autoridade mediante a verificação da qualidade da imagem, da origem do banco consultado, do índice de correspondência, dos demais elementos do caso e do registro da conferência humana antes de qualquer abordagem ou prisão.

2.3. Riscos: opacidade, vieses, seletividade e direitos fundamentais

Um dos principais riscos é a opacidade algorítmica, também conhecida como efeito “caixa-preta” (*black box*), que ocorre quando o sistema apresenta um resultado sem demonstrar de maneira compreensível o caminho percorrido para produzi-lo. Pedroso e Santos (2024) explicam que, em muitos casos, não é possível identificar quais dados foram considerados, como foram avaliados e quais critérios levaram à classificação apresentada, sendo que até os desenvolvedores podem ter dificuldade para explicar esse processo. No âmbito jurídico, toda informação que direciona uma investigação precisa estar sujeita a controle e impugnação.

Outro risco decorre da qualidade dos dados. Hennig Leal e Moreschi Paulo (2023) explicam que, quando as informações de treinamento apresentam marcas de preconceito ou seletividade, a tecnologia tende a repetir e ampliar essas distorções com aparência de neutralidade, enquanto Pedroso e Santos (2024) chamam atenção para a interferência humana presente desde a construção do sistema, nas escolhas de quem programa a ferramenta e

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

seleciona os dados. No Brasil, a seletividade estrutural do sistema de justiça criminal agrava o problema, com maior impacto sobre grupos vulnerabilizados (Pessoa; Silva; Reis, 2025).

O COMPAS ilustra esse risco: conforme Pedroso e Santos (2024), o programa atribuía maior risco de reincidência a acusados negros do que a acusados brancos com histórico semelhante. O uso de critérios matemáticos, portanto, não impede a discriminação e pode encobrir o viés sob aparência de neutralidade, razão pela qual Hennig Leal e Moreschi Paulo (2023) defendem parâmetros de controle que permitam avaliar se as plataformas de IA produzem resultados justos e não discriminatórios.

Esses usos colocam em tensão garantias previstas na Constituição Federal de 1988, como a dignidade da pessoa humana (art. 1º, III), a privacidade e a intimidade (art. 5º, X), o devido processo legal (art. 5º, LIV), o contraditório e a ampla defesa (art. 5º, LV) e a presunção de inocência (art. 5º, LVII) (Brasil, 1988). Pedroso e Santos (2024) observam que o tratamento automatizado transmite uma neutralidade aparente, sobretudo quando características demográficas ou comportamentais antecipam um juízo desfavorável, expondo o indivíduo a uma investigação mais invasiva pela categoria em que o sistema o colocou, e não por sua conduta. Não por acaso, o Regulamento Europeu de Inteligência Artificial (*AI Act*) classifica como de risco elevado sistemas usados pelas autoridades de aplicação da lei, como os destinados a avaliar a fiabilidade de provas (art. 6º, n. 2, e Anexo III, ponto 6), por poderem prejudicar o direito de defesa, a presunção de inocência e o direito a um tribunal imparcial quando não forem suficientemente transparentes, explicáveis e documentados (União Europeia, 2024).

A privacidade também é afetada pelo cruzamento de dados bancários, de localização, de redes sociais e de câmeras públicas, cujo tratamento amplo e pouco transparente dificulta o controle e compromete a dignidade, a igualdade, o devido processo legal e a ampla defesa (Pessoa; Silva; Reis, 2025).

3. METODOLOGIA

A pesquisa adotou abordagem qualitativa, de caráter exploratório e descritivo, desenvolvida por meio do método dedutivo, partindo dos fundamentos constitucionais e processuais relacionados à atividade investigativa e às garantias fundamentais para examinar os problemas específicos decorrentes da incorporação da inteligência artificial nessa conjuntura.

O estudo foi desenvolvido a partir de fontes bibliográficas e documentais, reunindo obras doutrinárias, artigos científicos e estudos sobre inteligência artificial, processo penal, proteção de dados e prova digital, além da Constituição Federal, do Código de Processo Penal, de outras

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

normas pertinentes, atos administrativos, propostas legislativas, documentos nacionais e internacionais e decisões dos tribunais superiores relacionadas ao uso de tecnologias na persecução penal.

Os dados textuais foram examinados por meio de análise de conteúdo, em etapas de pré-análise, exploração do material e tratamento e interpretação, com categorização orientada por eixos como opacidade e explicabilidade, vieses e discriminação, confiabilidade técnica, governança e auditoria e possibilidades de contraditório técnico pela defesa (Bardin, 2016). Na seleção das fontes, foram considerados o recorte temporal, a aderência ao problema de pesquisa, a relevância e a confiabilidade da fonte (Creswell, 2014; Yin, 2016). O recorte temporal concentrou-se em estudos, documentos institucionais e obras publicados entre 2018 e 2026, acrescidos da doutrina de base e das normas e decisões que fundamentam o tema, entre as quais o Código de Processo Penal, de 1941. A legislação e os projetos de lei foram consultados em portais oficiais, com verificação da tramitação até novembro de 2026, e as decisões judiciais, nos repositórios do STJ e do STF.

A pesquisa foi delimitada ao uso da inteligência artificial na investigação criminal, com foco em reconhecimento facial, cruzamento automatizado de informações, identificação de vínculos e análise de padrões, examinando suas consequências jurídicas sem avançar para avaliações técnicas sobre a precisão dos algoritmos ou para aspectos próprios da engenharia de sistemas. A expressão “prova algorítmica” foi empregada para identificar elementos informativos ou probatórios produzidos com participação da inteligência artificial em sua obtenção, análise ou interpretação, respeitando a distinção prevista no art. 155 do Código de Processo Penal entre as informações reunidas durante a investigação e as provas produzidas sob contraditório judicial (Brasil, 1941).

4. RESULTADOS E DISCUSSÃO

4.1. Legalidade, reserva legal e controles normativos

A eficiência pode contribuir para a apuração criminal, desde que a tecnologia respeite as garantias constitucionais aplicáveis à fase investigativa, conforme defende Lopes Júnior (2025), e os limites impostos pela legalidade ao exercício do poder punitivo, segundo a concepção garantista de Ferrajoli (2002). A legalidade deve ser observada em suas dimensões formal e material, exigindo que a diligência seja autorizada por norma editada pela autoridade competente e respeite os direitos fundamentais e o devido processo, sob pena de ilegitimidade por excesso de competência, desvio de finalidade ou restrição desproporcional de direitos, e a reserva legal

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

exige lei formal para intervenções restritivas (Ferrajoli, 2002), o que alcança o acesso a dados sigilosos, o acompanhamento de deslocamentos, o reconhecimento de pessoas e a criação de perfis de risco (Guasque, 2025), cabendo aos atos administrativos apenas disciplinar procedimentos já autorizados pelo ordenamento.

Badaró (2026) ressalta que os atos da investigação precisam admitir controle jurídico quando influenciam cautelares, acusações ou decisões posteriores. Quando interfere no rumo da apuração, o sistema deixa de ser mero apoio operacional, e a autoridade deve esclarecer a origem dos dados e a finalidade do uso, tratando o resultado algorítmico como subsídio da análise humana, nunca como justificativa automática da atuação estatal.

A Portaria MJSP nº 961/2025 organiza o uso de soluções de tecnologia da informação na investigação criminal e na inteligência de segurança pública no âmbito dos órgãos federais indicados em seu art. 1º, § 1º, como a Polícia Federal e a Polícia Rodoviária Federal, e de iniciativas estaduais, distritais e municipais custeadas pelo Fundo Nacional de Segurança Pública ou pelo Fundo Penitenciário Nacional. Estabelece critérios de adequação, necessidade, proporcionalidade, segurança e auditabilidade (Brasil, 2025b), com alcance administrativo, de modo que não cria novas hipóteses de acesso a dados, vigilância ou restrição de direitos nem substitui a lei formal e a autorização judicial exigidas para limitar direitos fundamentais (Ferrajoli, 2002). Seu art. 5º estabelece a delimitação da finalidade como requisito:

> A utilização de soluções de tecnologia aplicadas às atividades de investigação criminal e inteligência de segurança pública deve respeitar direitos fundamentais e ser limitada ao estritamente necessário para alcançar finalidades compatíveis e circunscritas às competências e atribuições dos órgãos de segurança pública.
> Parágrafo único. É vedado o uso indiscriminado, sem objetivo certo ou declarado, das soluções de tecnologia da informação referidas no caput deste artigo (Brasil, 2025b, art. 5º).

A regra afasta consultas abertas destinadas a encontrar fatos ou pessoas de interesse eventual das autoridades e restringe o reaproveitamento de dados para objetivo diverso. O art. 10, por sua vez, determina o emprego proporcional das soluções de IA e exige a revisão da inferência algorítmica pelo agente responsável quando houver risco de lesão a direitos fundamentais (Brasil, 2025b). Essa revisão deve ser real: segundo Guasque (2025), o agente precisa considerar os limites e as taxas de erro da ferramenta, confrontar a inferência com outras informações e justificar sua aceitação ou rejeição. Já o art. 11, § 1º, proíbe, como regra, a identificação biométrica à distância e em tempo real em espaços acessíveis ao público, admitindo-a em situações específicas, como a instrução de inquérito ou processo criminal mediante autorização judicial prévia e motivada, a busca de vítimas e de pessoas desaparecidas,

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

o flagrante delito de crimes punidos com pena máxima superior a dois anos, a recaptura de evadidos e o cumprimento de mandados de prisão (Brasil, 2025b).

A disciplina, contudo, permanece fragmentada. A Resolução CNJ nº 615/2025 apresenta critérios de governança relacionados à supervisão humana, à explicabilidade, à contestabilidade e à auditoria (Brasil, 2025a), mas, como a Portaria, tem alcance restrito à sua área de atuação. O Projeto de Lei nº 2.338/2023, no qual Guasque (2025) identifica a importância da transparência, da avaliação dos riscos e da supervisão humana, permanecia, em novembro de 2026, aguardando parecer do relator na comissão especial da Câmara dos Deputados (Brasil, 2023), não criando deveres vigentes. Breier (2025), por sua vez, aponta efeitos dessas tecnologias sobre a paridade de armas, o sigilo das comunicações e a ampla defesa, e os procedimentos previstos na Portaria não esclarecem por completo como a defesa terá acesso aos resultados nem como poderá contestá-los.

Entende-se, por isso, que a Portaria MJSP nº 961/2025 é relevante, porém insuficiente, pois seu caráter administrativo e seu alcance limitado não substituem uma lei formal com regras gerais sobre o uso da IA, os direitos da pessoa atingida e o acesso da defesa ao resultado. Pedroso e Santos (2024) defendem, nesse sentido, regulamentação que assegure supervisão humana e avaliação prévia das ferramentas. O risco à legalidade surge quando uma inferência algorítmica orienta a investigação sem base legal suficiente, finalidade definida e decisão humana fundamentada.

4.2. Proteção de dados pessoais no contexto penal

Doneda (2021) relaciona a proteção de dados à capacidade de reunir informações dispersas e formar uma representação da vida pessoal, e Bioni (2021) acrescenta que dados combinados podem identificar pessoas, antecipar comportamentos e criar perfis detalhados. Na investigação criminal, ao combinar registros bancários, deslocamentos, imagens, comunicações e vínculos sociais, a IA pode produzir inferências que não aparecem isoladamente em nenhuma das bases consultadas.

A Emenda Constitucional nº 115/2022 incluiu a proteção dos dados pessoais, inclusive nos meios digitais, entre os direitos fundamentais, ao acrescentar o inciso LXXIX ao art. 5º da Constituição (Brasil, 2022a), e a Lei nº 13.709/2018 confere tratamento mais rigoroso aos dados pessoais sensíveis, entre eles os referentes à origem racial ou étnica, à convicção religiosa, à saúde e os dados genéticos ou biométricos (arts. 5º, II, e 11), devido ao risco de seu uso provocar discriminações (Brasil, 2018). O art. 4º, III, da LGPD, entretanto, exclui de sua aplicação direta os tratamentos voltados exclusivamente à segurança pública e à investigação ou repressão

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

penal, sem conferir liberdade irrestrita aos órgãos de segurança, pois o § 1º do mesmo artigo dispõe:

> O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei (Brasil, 2018, art. 4º, § 1º).

Essa legislação específica ainda não existe: o Projeto de Lei nº 1.515/2022 permanecia em tramitação em novembro de 2026, sem produzir efeitos jurídicos (Brasil, 2022b). A falta de regras nacionais sobre o acesso do investigado aos dados, as decisões automatizadas, a conservação, o compartilhamento e a atuação de fornecedores privados permite a adoção de procedimentos internos diferentes e dificulta que a defesa conheça a origem das informações, as bases consultadas e a influência desses dados na formação da suspeita.

As orientações da ANPD não incidem automaticamente nas hipóteses do art. 4º, III, da LGPD, mas servem de referência ao exigirem finalidade pública definida (ANPD, 2023), o que, na investigação, afasta buscas indiscriminadas e o reaproveitamento de dados biométricos para monitoramento permanente. A necessidade restringe o tratamento ao indispensável quanto às pessoas, às categorias de dados e ao período analisado. O consentimento, por sua vez, dificilmente constitui fundamento adequado, pois, segundo Bioni (2021), sua validade depende de uma escolha verdadeiramente livre, condição pouco presente em uma relação marcada pela autoridade estatal. Quanto à segurança, a ANPD (2023) recomenda controles contra acesso indevido e compartilhamento irregular, registro da finalidade e dos destinatários e, em operações de alto risco, relatório de impacto que identifique falhas nos dados, grupos atingidos e taxas de erro.

O uso de dados sem finalidade definida, em excesso ou sem segurança ameaça, assim, a legalidade e a ampla defesa, pois, sem o registro da origem, da coleta, do compartilhamento e das alterações das informações, não é possível verificar a licitude da suspeita.

4.3. Cadeia de custódia informacional

Como dados de entrada, versão do sistema, parâmetros e revisão humana interferem na conclusão, propõe-se denominar “cadeia de custódia informacional” o conjunto de registros que preserva e permite reconstruir o caminho dos dados processados por IA, incluindo a origem das informações, as bases consultadas, a ferramenta e sua versão, os parâmetros, o resultado e a validação humana anterior ao uso da inferência na investigação.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Essa categoria não substitui a cadeia de custódia prevista nos arts. 158-A a 158-F do Código de Processo Penal, incluídos pela Lei nº 13.964/2019 (Brasil, 2019) e definida no art. 158-A como o conjunto de procedimentos destinado a manter e documentar a história cronológica do vestígio e a rastrear sua posse e manuseio (Brasil, 1941). Enquanto a cadeia legal acompanha a trajetória do vestígio, a cadeia informacional acompanha também as transformações realizadas pela ferramenta até a produção de uma correspondência, classificação ou indicação de risco.

Badaró (2026) relaciona a confiabilidade da prova à possibilidade de conhecer e controlar sua formação, Prado (2021) compreende a cadeia de custódia como instrumento destinado a preservar a identidade do elemento probatório e Matida (2020) atribui-lhe uma função epistêmica, ligada à redução de erros e à avaliação da autenticidade, da integridade e da confiabilidade da prova, especialmente relevante nos elementos digitais, em que cópias e alterações podem ocorrer sem sinais físicos visíveis. Aplicadas à IA, essas perspectivas afastam a ideia de que a precisão estatística declarada pelo fornecedor baste para comprovar a confiabilidade de uma inferência no caso concreto.

A Portaria MJSP nº 961/2025 contempla parte desses cuidados: seu art. 7º, § 2º, determina, na obtenção de dados sigilosos, o registro do inquérito, da decisão judicial, da extensão e do período da medida, da solução utilizada, da execução e dos resultados, e o ato exige auditorias e registros de acesso (Brasil, 2025b). Essas previsões não detalham, porém, todos os elementos a preservar quando a própria IA transforma os dados, e os *logs* mostram quem acessou o sistema, mas não explicam os critérios da ferramenta nem a relevância atribuída ao resultado. Guasque (2025) relaciona a auditabilidade ao controle de sistemas que interferem em direitos fundamentais.

A jurisprudência do STJ sobre prova digital orienta as consequências da falta de documentação. Segundo o Informativo nº 838, a Quinta Turma considerou inadmissível prova digital composta por arquivos corrompidos que impossibilitavam a comparação entre o *hash* do espelhamento e o material juntado aos autos (Brasil, 2025c). No AgRg no HC nº 828.054/RN, a Quinta Turma considerou inadmissíveis dados extraídos de celular sem metodologia e documentação capazes de demonstrar sua correspondência com o conteúdo original (Brasil, 2024), e, no HC nº 653.515/RJ, a Sexta Turma afirmou que nem toda irregularidade gera nulidade automática, devendo-se examinar a confiabilidade do vestígio e o prejuízo à defesa (Brasil, 2021). A mesma lógica vale para a IA: alertas, pontuações e vínculos podem orientar diligências sem provar a autoria, e, quanto maior seu peso em cautelares ou na acusação, maior deve ser o rigor da documentação.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Assim, a opacidade algorítmica, somada à ausência dessa cadeia, impede o advogado de identificar erros e vieses e reduz sua atuação a uma manifestação formal.

4.4. Direito à explicação, acesso à prova algorítmica e paridade de armas

Badaró (2026) relaciona a efetividade do contraditório à possibilidade de participação e controle sobre os elementos capazes de influenciar a persecução penal, de modo que o simples conhecimento do resultado não substitui o acesso aos fundamentos que permitem sua contestação. Resende (2023) observa que a explicabilidade tem importância justamente por permitir maior compreensão e controle sobre os resultados de sistemas complexos, e Oliveira e Bedê Jr. (2026) apontam que alertas, pontuações e classificações podem adquirir aparência de confiabilidade ao circularem entre polícia, Ministério Público e Judiciário sem verificação independente de sua origem.

Não se afirma um direito irrestrito de conhecer todo o funcionamento interno dos sistemas estatais, mas a explicação como condição para que o contraditório alcance a informação algorítmica que produz consequências relevantes ao investigado. Resende (2023) distingue a compreensão do funcionamento do sistema da explicação necessária para avaliar determinado resultado, o que permite concentrar o controle nas informações relevantes para o caso concreto; no reconhecimento facial, por exemplo, a imagem analisada, a base consultada, o índice de correspondência e a conferência realizada pelo agente (Moreira, 2022; Couto *et al.*, 2025). Como referência comparativa, o *AI Act* impõe deveres de transparência aos sistemas de risco elevado, para que seus resultados possam ser adequadamente interpretados (art. 13) (União Europeia, 2024). A explicação deve abranger, ainda, a análise feita pelo agente responsável após a produção do resultado, conforme prevê a Portaria MJSP nº 961/2025 (Brasil, 2025b).

A explicação só permite controle efetivo quando a defesa também tem acesso aos dados e registros necessários para compreender como a conclusão foi produzida. Daguer, Borri e Soares (2025) apontam que a assimetria informacional decorre do maior acesso do Estado às fontes de prova e defendem o fortalecimento do contraditório como forma de reduzir esse desequilíbrio. A paridade de armas não exige poderes idênticos, mas condições suficientes para que o acusado conheça e enfrente os elementos utilizados contra ele.

A Súmula Vinculante nº 14 do Supremo Tribunal Federal assegura ao defensor acesso amplo aos elementos de prova já documentados no procedimento investigatório e relacionados ao exercício do direito de defesa (Brasil, 2009). Quando o procedimento reúne apenas um relatório com a indicação de uma correspondência, vínculo ou padrão suspeito, a defesa conhece

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

o resultado, mas encontra dificuldades para verificar como ele foi formado, aspecto relacionado à necessidade de mecanismos que permitam conferir a formação e a preservação das evidências digitais (Vieira; Santos, 2025). O acesso deve reunir, conforme a ferramenta, os dados de entrada, as bases consultadas, a versão do sistema, os parâmetros, o resultado completo, os registros da operação e a identificação de quem realizou a revisão humana, elementos que integram a cadeia de custódia informacional.

Quando a ferramenta é fornecida por empresa privada, a proteção de informações empresariais deve ser compatibilizada com esse acesso, para não ampliar a desigualdade entre as partes nem inviabilizar a contestação da inferência (Breier, 2025; Daguer; Borri; Soares, 2025).

4.5. Perícia técnica e efetividade da ampla defesa

Alguns sistemas exigem conhecimento técnico para que seus dados e procedimentos possam ser examinados. O art. 159 do Código de Processo Penal prevê a participação das partes na prova pericial por meio de quesitos, assistente técnico, pedidos de esclarecimento e pareceres, assegurando, em seu § 6º, mediante requerimento das partes, a disponibilização do material probatório que serviu de base à perícia para exame pelos assistentes técnicos (Brasil, 1941). Amaral e Bruni (2023) observam que a prova pericial não é manifestação infalível da ciência, pois o método técnico não elimina erros e incertezas, preocupação ainda mais intensa na IA, cuja aparência de precisão não substitui a demonstração de que a ferramenta era adequada à finalidade em que foi empregada.

No HC nº 1.059.475/SP, a Quinta Turma do STJ analisou relatório elaborado por investigador com auxílio das ferramentas de inteligência artificial generativa Gemini e Perplexity para examinar vídeo relacionado a uma imputação de injúria racial. A perícia oficial não havia confirmado, pelos parâmetros de fonética forense, a expressão atribuída ao acusado, mas as ferramentas de IA chegaram a conclusão diferente, utilizada na denúncia. O Tribunal concluiu que o relatório não tinha confiabilidade epistêmica mínima para servir como prova, dada a inadequação das ferramentas à análise fonética e a falta de fundamentação técnico-científica, e que não constituía prova pericial nos termos do art. 159 do CPP (Brasil, 2026b). O julgamento não impede o uso da IA na investigação, mas evidencia a necessidade de demonstrar a aptidão, o método e a confiabilidade da tecnologia utilizada.

No mesmo sentido, no AgRg no HC nº 1.014.212/ES, a Sexta Turma reconheceu que dúvida razoável sobre autenticidade e integridade do material digital exigia exame pericial capaz de verificar sua confiabilidade e assegurar o contraditório, não bastando a autorização de acesso

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

e a identificação do agente para suprir a ausência de documentação técnica (Brasil, 2026a). Exigir que a defesa demonstre o erro de um sistema cujo funcionamento é conhecido apenas pelo Estado ou pelo fornecedor cria, portanto, uma desvantagem difícil de superar.

A realização de perícia deve ser avaliada a partir das dúvidas existentes, da influência exercida pelo resultado e das informações já disponíveis. Quando a IA funciona como apoio e sua indicação é confirmada por outros elementos, a conferência pode ser feita a partir dos registros; quando a inferência participa diretamente da identificação de uma pessoa, da atribuição de autoria ou de uma medida restritiva, a verificação técnica exige maior cuidado. Seguindo o HC nº 653.515/RJ, que manda examinar irregularidades na cadeia de custódia conforme as circunstâncias concretas e o prejuízo à defesa (Brasil, 2021), falhas na documentação do resultado algorítmico devem ser avaliadas segundo a influência da inferência no caso e a existência de outros meios de confirmar sua origem, integridade e confiabilidade.

Diante do conjunto analisado, a proteção atualmente existente no Brasil mostra-se parcialmente efetiva e ainda insuficiente: a Constituição, o Código de Processo Penal, a jurisprudência e os atos administrativos oferecem meios de controle, mas não definem por completo como a defesa poderá conhecer, compreender e contestar a inferência, sobretudo quanto ao acesso às informações técnicas, ao segredo empresarial, à documentação necessária e às hipóteses de perícia. Sem esses meios, a ampla defesa (Brasil, 1988) permanece assegurada no plano normativo, mas de difícil exercício concreto.

5. CONSIDERAÇÕES FINAIS

A pesquisa examinou os efeitos do uso da inteligência artificial na investigação criminal sobre a legalidade e a ampla defesa, demonstrando que o risco está ligado às condições em que a tecnologia é utilizada, principalmente quando faltam registros, transparência e meios que permitam examinar a inferência produzida.

Quanto ao primeiro objetivo específico, foram identificadas aplicações como reconhecimento facial, cruzamento automatizado de dados, identificação de vínculos e análise de padrões, que podem auxiliar a apuração e orientar novas diligências, desde que suas indicações sejam avaliadas juntamente com outros elementos e não recebam, isoladamente, valor suficiente para atribuir autoria ou justificar uma restrição de direitos.

Quanto ao segundo objetivo, verificou-se que a IA não altera os limites jurídicos impostos à atuação estatal, que continuam a exigir finalidade definida, proporcionalidade, proteção dos dados, fundamentação e controle. Houve avanços em governança, auditoria e revisão humana,

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

mas permanecem indefinidos o acesso da defesa, o registro das operações e a contestação técnica, o que motivou a proposta da cadeia de custódia informacional: o registro das etapas acrescentadas pelo processamento algorítmico, complementar à cadeia de custódia do Código de Processo Penal, que permite acompanhar a origem dos dados, as transformações realizadas pela ferramenta e o uso do resultado pela autoridade.

Quanto ao terceiro objetivo, constatou-se que conhecer apenas a conclusão da ferramenta pouco contribui quando a defesa não dispõe de informações para entender sua formação, conferir os dados empregados e, se necessário, recorrer a exame técnico; os precedentes examinados mostraram que a aparência técnica de um relatório produzido com auxílio tecnológico não substitui a demonstração de que o método era adequado e de que o resultado pode ser conferido.

A tese proposta foi confirmada: a inteligência artificial pode atuar legitimamente como ferramenta de apoio à investigação quando existe documentação do procedimento, revisão humana e possibilidade de controle pela defesa, e o risco à legalidade e à ampla defesa aparece quando a opacidade do sistema, a falta de registros e a desigualdade no acesso às informações impedem que o resultado seja compreendido e questionado de forma efetiva. Conclui-se que a inovação tecnológica pode contribuir para a atividade investigativa sem retirar da defesa a possibilidade de conhecer o caminho percorrido pela informação, discutir sua confiabilidade e contestar aquilo que tenha influenciado uma medida adotada contra o investigado.

REFERÊNCIAS

AMARAL, Gustavo Rick; XAVIER, Fernando. A inteligência artificial e o novo patamar da interação humano-máquina. **TECCOGS:** Revista Digital de Tecnologias Cognitivas, São Paulo, n. 26, p. 6-43, jul./dez. 2022. DOI: 10.23925/1984-3585.2022i26p6-43. Disponível em: https://doi.org/10.23925/1984-3585.2022i26p6-43. Acesso em: 28 mar. 2026.

AMARAL, Maria Eduarda Azambuja; BRUNI, Aline Thaís. Prova pericial no processo penal: a compreensão e a mitigação dos erros forenses como mecanismo de respeito ao contraditório, à ampla defesa e ao direito à prova lícita. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 9, n. 2, p. 877-912, maio/ago. 2023. DOI: 10.22197/rbdpp.v9i2.819. Disponível em: https://doi.org/10.22197/rbdpp.v9i2.819. Acesso em: 27 ago. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Tratamento de dados pessoais pelo Poder Público:** guia orientativo. Versão 2.0. Brasília, DF: ANPD, jun. 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 12 maio 2026.

BADARÓ, Gustavo Henrique. **Processo penal**. 14. ed. São Paulo: Thomson Reuters Brasil, 2026.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

BARDIN, Laurence. **Análise de conteúdo**. São Paulo: Edições 70, 2016.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2021.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 16 jun. 2026.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Diário Oficial da União: seção 1, Rio de Janeiro, 13 out. 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 16 jun. 2026.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Diário Oficial da União: seção 1, Brasília, DF, 11 fev. 2022a. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 16 jun. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 jun. 2026.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Diário Oficial da União: seção 1, edição extra, Brasília, DF, 24 dez. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 16 jun. 2026.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 1.515, de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública e de investigação e repressão de infrações penais. Brasília, DF: Câmara dos Deputados, 2022b. Disponível em: https://www.camara.leg.br/propostas-legislativas/2326300. Acesso em: 21 nov. 2026.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 2.338, de 2023**. Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Brasília, DF: Câmara dos Deputados, 2023. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262. Acesso em: 21 nov. 2026.

BRASIL. Conselho Nacional de Justiça. **Resolução nº 615, de 11 de março de 2025**. Estabelece diretrizes para o desenvolvimento, a utilização e a governança de soluções desenvolvidas com recursos de inteligência artificial no Poder Judiciário. Diário da Justiça Eletrônico do CNJ, Brasília, DF, n. 54, p. 2-17, 14 mar. 2025a. Disponível em: https://atos.cnj.jus.br/atos/detalhar/6001. Acesso em: 12 maio 2026.

BRASIL. Ministério da Justiça e Segurança Pública. **Portaria MJSP nº 961, de 24 de junho de 2025**. Estabelece diretrizes sobre o uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública. Diário Oficial da União:

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

seção 1, Brasília, DF, n. 120, p. 104-105, 30 jun. 2025b. Disponível em: https://bibliotecadigital.mj.gov.br/bitstream/1/15324/1/PRT_GM_2025_961.pdf. Acesso em: 22 nov. 2026.

BRASIL. Superior Tribunal de Justiça (6. Turma). **Habeas Corpus nº 653.515/RJ**. Cadeia de custódia da prova; consequências de eventual descumprimento; necessidade de análise do prejuízo e da confiabilidade do vestígio. Relatora: Ministra Laurita Vaz. Relator para o acórdão: Ministro Rogerio Schietti Cruz, 23 de novembro de 2021. Brasília, DF: Superior Tribunal de Justiça, 2021. Disponível em: https://scon.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisar&aplicacao=informativo&livre=%40CNOT%3D%27018686%27. Acesso em: 16 jun. 2026.

BRASIL. Superior Tribunal de Justiça (5. Turma). **Agravo Regimental no Habeas Corpus nº 828.054/RN**. Prova digital; extração de dados de aparelho celular; ausência de metodologia e documentação; quebra da cadeia de custódia; inadmissibilidade. Relator: Ministro Joel Ilan Paciornik, 23 de abril de 2024. Diário da Justiça Eletrônico, Brasília, DF, 29 abr. 2024. Disponível em: https://scon.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisar&aplicacao=informativo&livre=%40CNOT%3D%27020706%27. Acesso em: 16 jun. 2026.

BRASIL. Superior Tribunal de Justiça. **Informativo de Jurisprudência nº 838**: prova digital; cadeia de custódia; necessidade de comparar o *hash* do arquivo espelhado com o apresentado no processo; arquivos corrompidos. Brasília, DF: STJ, 4 fev. 2025c. Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedicao&livre=0838.cod. Acesso em: 16 jun. 2026.

BRASIL. Superior Tribunal de Justiça (6. Turma). **Agravo Regimental no Habeas Corpus nº 1.014.212/ES**. Prova digital; dúvida sobre integridade e autenticidade; ausência de certificação por código *hash*; necessidade de perícia complementar. Relator: Ministro Carlos Pires Brandão, 10 de fevereiro de 2026. Diário de Justiça Eletrônico Nacional, Brasília, DF, 20 fev. 2026a. Disponível em: https://scon.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisar&aplicacao=informativo&livre=%40CNOT%3D%27022145%27. Acesso em: 16 jun. 2026.

BRASIL. Superior Tribunal de Justiça (5. Turma). **Habeas Corpus nº 1.059.475/SP**. Inteligência artificial generativa; relatório técnico policial elaborado com as ferramentas Gemini e Perplexity; ausência de confiabilidade epistêmica mínima; inadmissibilidade como prova. Relator: Ministro Reynaldo Soares da Fonseca, 7 de abril de 2026. Brasília, DF: Superior Tribunal de Justiça, 2026b. Disponível em: https://scon.stj.jus.br/SCON/GetPDFINFJ?edicao=0884. Acesso em: 27 ago. 2026.

BRASIL. Supremo Tribunal Federal. **Súmula Vinculante nº 14**. É direito do defensor, no interesse do representado, ter acesso amplo aos elementos de prova que, já documentados em procedimento investigatório realizado por órgão com competência de polícia judiciária, digam respeito ao exercício do direito de defesa. Aprovada em sessão plenária de 2 fev. 2009. Diário da Justiça Eletrônico, Brasília, DF, n. 26, p. 1, 9 fev. 2009. Disponível em: https://portal.stf.jus.br/jurisprudencia/sumariosumulas.asp?base=26&sumula=1230. Acesso em: 27 ago. 2026.

BREIER, Ricardo. O risco à defesa técnica e à paridade de armas no processo penal: análise crítica da Portaria MJSP nº 961/2025. **Abracrim**, São Paulo, 15 jul. 2025. Disponível em:

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

https://web.abracrim.adv.br/o-risco-a-defesa-tecnica-e-a-paridade-de-armas-no-processo-penal-analise-critica-da-portaria-mjsp-no-961-2025/. Acesso em: 15 abr. 2026.

COSTA, Mauir Victor da Silva da; FELLER, Thiago de Almeida. O uso da inteligência artificial na investigação criminal. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 11, n. 11, p. 2689-2703, nov. 2025. DOI: 10.51891/rease.v11i11.22095. Disponível em: https://periodicorease.pro.br/rease/article/view/22095. Acesso em: 31 mar. 2026.

COUTO, Alessandro Buarque; CONCEIÇÃO, Valdir Silva da; UCHOA, Fabio Oliveira; SANTOS, João Antonio Belmino dos; MEIRA, Matheus Brito; OLIVEIRA JUNIOR, Antonio Martins de. Uso da inteligência artificial por meio do reconhecimento facial na segurança pública de aeroportos. **Revista Eletrônica Científica Inovação e Tecnologia**, Medianeira, v. 16, n. 39, p. 50-70, jan./abr. 2025. Disponível em: https://periodicos.utfpr.edu.br/recit/article/view/19183. Acesso em: 25 mar. 2026.

CRESWELL, John W. **Investigação qualitativa e projeto de pesquisa**: escolhendo entre cinco abordagens. 3. ed. Porto Alegre: Penso, 2014.

DAGUER, Beatriz; BORRI, Luiz Antonio; SOARES, Rafael Junior. Assimetria informacional entre acusação e defesa: uma proposta de fortalecimento do contraditório. **Boletim IBCCRIM**, São Paulo, v. 33, n. 387, p. 18-20, 2025. DOI: 10.5281/zenodo.14079250. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1147. Acesso em: 27 ago. 2026.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** fundamentos da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

FERRAJOLI, Luigi. **Direito e razão:** teoria do garantismo penal. 3. ed. São Paulo: Revista dos Tribunais, 2002.

GUASQUE, Bárbara. Inteligência artificial e direitos fundamentais no Brasil: uma análise sobre vieses algorítmicos, transparência decisória e o Projeto de Lei nº 2.338/2023. **Emancipação**, Ponta Grossa, v. 25, p. 1-23, 2025. DOI: 10.5212/Emancipacao.v.25.2524134.025. Disponível em: https://revistas.uepg.br/index.php/emancipacao/article/view/24134. Acesso em: 15 abr. 2026.

HENNIG LEAL, Mônia Clarissa; MORESCHI PAULO, Lucas. Algoritmos discriminatórios e jurisdição constitucional: os riscos jurídicos e sociais do impacto dos vieses nas plataformas de inteligência artificial de amplo acesso. **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 24, n. 3, p. 165-187, set./dez. 2023. DOI: 10.18759/rdgf.v24i3.2311. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/2311. Acesso em: 15 abr. 2026.

LOPES JÚNIOR, Aury. **Direito processual penal**. 22. ed. São Paulo: Saraiva Jur, 2025.

MATIDA, Janaina. A cadeia de custódia é condição necessária para a redução dos riscos de condenações de inocentes. **Boletim IBCCRIM**, São Paulo, v. 28, n. 331, p. 6-9, jun. 2020. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/541. Acesso em: 12 maio 2026.

MOREIRA, Horrara. **Reconhecimento facial:** e quando a máquina erra? Miniguia para juristas sobre o uso de tecnologias de reconhecimento facial na segurança pública. Campanha Tire Meu

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Rosto da Sua Mira. [S. l.]: Coalizão Direitos na Rede, 2022. Disponível em: https://br.boell.org/sites/default/files/2023-04/tmr_cartilha_vfinal.pdf. Acesso em: 3 abr. 2026.

OLIVEIRA, Luciano Rocha de; BEDÊ JR., Américo. Confiança e opacidade: governança de sistemas integrados e IA preditiva no ciclo polícia, MP e Judiciário. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 12, n. 2, e1400, 2026. DOI: 10.22197/rbdpp.v12i2.1400. Disponível em: https://doi.org/10.22197/rbdpp.v12i2.1400. Acesso em: 27 ago. 2026.

PEDROSO, João; SANTOS, Andreia. Inteligência artificial e justiça criminal: riscos e desafios. **Sociologia On Line**, Lisboa, n. 35, p. 134-158, ago. 2024. DOI: 10.30553/sociologiaonline.2024.35.6. Disponível em: https://revista.aps.pt/pt/inteligencia-artificial-e-justica-criminal-riscos-e-desafios/. Acesso em: 15 abr. 2026.

PESSOA, Cirlene da Conceição; SILVA, Sandra Renata Alves da; REIS, Marcos Neemias Negrão. Inteligência artificial, prevenção de crimes e direitos fundamentais: uma abordagem criminológica. **Facit Business and Technology Journal**, [S. l.], v. 1, n. 63, p. 61-78, jun. 2025. DOI: 10.5281/zenodo.16423722. Disponível em: https://revistas.faculdadefacit.edu.br/index.php/JNT/article/view/3623. Acesso em: 15 abr. 2026.

PRADO, Geraldo. **A cadeia de custódia da prova no processo penal**. 2. ed. São Paulo: Marcial Pons, 2021.

RESENDE, Ana Paula Bougleux Andrade. **O processamento de imagens de vídeos por meio de inteligência artificial como forma de identificar a materialidade de delitos**: entre a eficiência e o incremento de novos riscos. 2023. 212 f. Dissertação (Mestrado em Direito) – Faculdade de Ciências Humanas e Sociais, Universidade Estadual Paulista “Júlio de Mesquita Filho”, Franca, 2023. Disponível em: https://hdl.handle.net/11449/255140. Acesso em: 27 ago. 2026.

SARDANA, Divya; MARWAHA, Shruti; BHATNAGAR, Raj. Supervised and unsupervised machine learning methodologies for crime pattern analysis. **International Journal of Artificial Intelligence and Applications**, [S. l.], v. 12, n. 1, p. 83-99, jan. 2021. DOI: 10.5121/ijaia.2021.12106. Disponível em: https://aircconline.com/ijaia/V12N1/12121ijaia06.pdf. Acesso em: 6 abr. 2026.

SILVA, Jonathan Gomes da; AGUIAR, Denison Melo de; LOPES, Flávio Humberto Pascarelli; CAMPOS, Bruno Patrício de Azevedo; SILVA, Diego Bernardino da; SILVA NETO, Newton Suassuna da. A utilização de algoritmos de predição criminal (*predictive policing*) no âmbito da Polícia Militar do Estado do Amazonas: uma análise da conformidade com a proteção de dados e o princípio da não discriminação. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 12, n. 4, p. 1-25, abr. 2026. DOI: 10.51891/rease.v12i4.24360. Disponível em: https://periodicorease.pro.br/rease/article/view/24360. Acesso em: 15 abr. 2026.

UNESCO. **Os riscos éticos da IA**. UNESCO, 7 ago. 2018. Disponível em: https://www.unesco.org/pt/articles/os-riscos-eticos-da-ia. Acesso em: 8 abr. 2026.

UNIÃO EUROPEIA. Parlamento Europeu; Conselho da União Europeia. **Regulamento (UE) 2024/1689, de 13 de junho de 2024**. Estabelece regras harmonizadas em matéria de inteligência artificial e altera determinados atos legislativos da União. Jornal Oficial da União Europeia, Luxemburgo, série L, 12 jul. 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ:L_202401689. Acesso em: 15 abr. 2026.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

VIEIRA, Andrey Bruno Cavalcante; SANTOS, Hugo Leonardo Rodrigues. Investigação criminal e tecnologias digitais: algumas reflexões sobre o policiamento preditivo e a admissibilidade de provas digitais. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 11, n. 1, e1072, jan./abr. 2025. DOI: 10.22197/rbdpp.v11i1.1072. Disponível em: https://doi.org/10.22197/rbdpp.v11i1.1072. Acesso em: 27 ago. 2026.

YIN, Robert K. **Pesquisa qualitativa do início ao fim**. Porto Alegre: Penso, 2016.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.