doi.org/ 10.51891/rease.v12i5.27151

INTELIGÊNCIA ARTIFICIAL E RECONHECIMENTO FACIAL NA INVESTIGAÇÃO CRIMINAL: ENTRE A EFICIÊNCIA INVESTIGATIVA E A PROTEÇÃO DOS DIREITOS FUNDAMENTAIS

Maria Augusta Ribeiro Guimarães[1]
Bianca Muniz Leite[2]

RESUMO:

A crescente utilização de tecnologias digitais, especialmente a inteligência artificial e o reconhecimento facial, tem transformado significativamente a investigação criminal no Brasil, ampliando a capacidade de análise de dados e a eficiência dos procedimentos investigativos. O objetivo deste estudo foi analisar os impactos dessas tecnologias na investigação criminal, considerando o equilíbrio entre eficiência investigativa e proteção dos direitos fundamentais. Trata-se de uma pesquisa de natureza bibliográfica e documental, com abordagem qualitativa e método indutivo, baseada na análise de artigos científicos, legislações e documentos institucionais publicados entre 2020 e 2026. Os resultados evidenciam que tais tecnologias contribuem para a celeridade e precisão na identificação de suspeitos, porém também apresentam riscos relevantes, como violação da privacidade, discriminação algorítmica e fragilização do devido processo legal. Observou-se, ainda, a existência de lacunas no ordenamento jurídico brasileiro quanto à regulamentação específica dessas ferramentas, o que pode comprometer a segurança jurídica e a transparência das investigações. Conclui-se que, embora as tecnologias analisadas representem avanços importantes para a persecução penal, sua utilização deve ser orientada por princípios constitucionais, exigindo mecanismos de controle, regulamentação adequada e garantia dos direitos fundamentais, de modo a assegurar um equilíbrio entre inovação tecnológica e justiça penal.

Palavras-chave: Investigação criminal. Inteligência artificial. Reconhecimento facial.

1 INTRODUÇÃO

A crescente incorporação de tecnologias digitais no âmbito da investigação criminal tem promovido profundas transformações na forma como o Estado conduz a persecução penal, especialmente diante do avanço de ferramentas como a inteligência artificial e o reconhecimento facial. Tais recursos tecnológicos ampliam significativamente a capacidade de coleta, processamento e análise de dados, permitindo maior celeridade e precisão na identificação de suspeitos e na elucidação de infrações penais. A relevância do tema reside na necessidade de compreender como essas tecnologias impactam a eficiência investigativa, ao

[1] Discente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia.
[2] Docente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia.

mesmo tempo em que suscitam importantes debates jurídicos relacionados à proteção dos direitos fundamentais (Costa; Feller, 2025).

A problematização que orienta a presente pesquisa consiste em analisar como o uso da inteligência artificial e do reconhecimento facial impacta a investigação criminal no Brasil, considerando o equilíbrio entre a eficiência investigativa e a proteção dos direitos fundamentais.

O objetivo geral deste estudo é analisar como o uso da inteligência artificial e do reconhecimento facial impacta a investigação criminal no Brasil, considerando seus efeitos sobre a eficiência investigativa e os desafios relacionados à proteção dos direitos fundamentais. Como objetivos específicos, pretende-se: examinar as principais aplicações dessas tecnologias no contexto investigativo; identificar os riscos jurídicos decorrentes de sua utilização, especialmente no que se refere à privacidade e à discriminação algorítmica; e avaliar a adequação do ordenamento jurídico brasileiro na regulamentação dessas práticas, verificando a existência de lacunas normativas e a necessidade de parâmetros para sua utilização responsável.

A justificativa da pesquisa fundamenta-se na crescente utilização de tecnologias digitais no campo da segurança pública e na ausência de regulamentação específica capaz de acompanhar esse avanço. A adoção de sistemas de inteligência artificial e reconhecimento facial, embora contribua para a modernização da investigação criminal, também pode gerar impactos negativos quando utilizada sem critérios claros de controle e supervisão. A pesquisa mostra-se relevante tanto do ponto de vista acadêmico quanto social, ao propor uma análise crítica sobre os limites e possibilidades dessas tecnologias, contribuindo para o desenvolvimento de práticas investigativas mais equilibradas e juridicamente seguras. Conforme apontam Negri e Winter (2025), a ausência de regulamentação adequada pode potencializar riscos de discriminação e comprometer a efetividade dos mecanismos de proteção de direitos.

No que se refere à metodologia, o estudo adota uma abordagem qualitativa, de natureza bibliográfica e documental, com base na análise de artigos científicos, legislações e produções acadêmicas recentes sobre o tema. O método de abordagem é indutivo, partindo da análise de estudos específicos para a construção de conclusões gerais acerca dos impactos das tecnologias na investigação criminal. A coleta de dados foi realizada por meio de levantamento em bases como Google Acadêmico e SciELO, priorizando publicações entre os anos de 2020 e 2026, de modo a garantir a atualidade das informações analisadas.

Como limitações, destaca-se o fato de a pesquisa não envolver coleta de dados empíricos, restringindo-se à análise de fontes secundárias, o que pode limitar a abrangência dos resultados. Além disso, a rápida evolução tecnológica pode tornar parte das discussões suscetíveis a

atualizações constantes. Por fim, como proposição, o estudo busca contribuir para o debate acadêmico e jurídico ao sugerir a necessidade de construção de marcos regulatórios mais específicos e eficazes, capazes de assegurar o uso responsável da inteligência artificial e do reconhecimento facial na investigação criminal, promovendo o equilíbrio entre eficiência investigativa e proteção dos direitos fundamentais.

2 REFERENCIAL TEÓRICO

2.1 Evolução da investigação criminal

A evolução da investigação criminal revela um processo contínuo de transformação, marcado pela adaptação das práticas investigativas às mudanças sociais, tecnológicas e jurídicas ao longo do tempo. Inicialmente, os métodos de apuração de delitos estavam fortemente baseados em confissões, testemunhos e evidências materiais obtidas de forma muitas vezes rudimentar, com limitada preocupação quanto à sistematização científica das provas. Com o avanço do Estado de Direito, consolidou-se a necessidade de observância de garantias fundamentais, o que impulsionou o desenvolvimento de técnicas mais estruturadas e juridicamente controladas (Dantas; Costa, 2021).

Ao longo do século XX, observa-se a crescente influência da ciência na investigação criminal, especialmente com o desenvolvimento da criminalística e das perícias técnicas. A utilização de métodos científicos, como análise de impressões digitais, exames laboratoriais e técnicas de balística, contribuiu significativamente para o aumento da confiabilidade das provas e para a redução da dependência exclusiva de depoimentos, essa transição representou um marco na evolução investigativa, ao permitir a reconstrução mais precisa dos fatos e a identificação de autores com maior grau de certeza (Machado et al., 2026).

Com o advento das tecnologias digitais, a investigação criminal passou por uma nova e significativa transformação, caracterizada pela incorporação de ferramentas capazes de lidar com grandes volumes de dados e com a complexidade dos crimes contemporâneos. O surgimento da internet, dos dispositivos móveis e das redes digitais ampliou não apenas as possibilidades de prática delitiva, mas também os meios de investigação, exigindo dos órgãos de segurança pública uma constante atualização de suas estratégias (Rezende, 2025).

Paralelamente a esses avanços, surgem novos desafios relacionados à compatibilização entre eficiência investigativa e respeito aos direitos fundamentais. A ampliação dos poderes investigativos, impulsionada pelo uso de tecnologias avançadas, levanta questionamentos

quanto aos limites da atuação estatal, sobretudo no que se refere à privacidade, à proteção de dados e à legalidade das provas obtidas. Além disso, a evolução do tema também abrange a discussão sobre a investigação defensiva, que busca equilibrar a atuação das partes no processo penal, ampliando as possibilidades de produção probatória pela defesa (Dantas; Costa, 2021).

2.2 A inserção das tecnologias digitais na persecução penal

A inserção das tecnologias digitais na persecução penal representa uma das transformações mais significativas no âmbito do Direito Processual Penal contemporâneo, refletindo a necessidade de adaptação das instituições frente às novas dinâmicas sociais e criminais. Com o avanço das tecnologias da informação, observa-se a ampliação dos instrumentos disponíveis para a investigação e produção de provas, permitindo maior agilidade na coleta e no processamento de dados. Esse cenário evidencia uma mudança paradigmática, na qual a persecução penal passa a depender, cada vez mais, de recursos digitais para a elucidação de infrações, especialmente aquelas praticadas em ambientes virtuais (Arigony; Botton; Arigony, 2025).

A digitalização da persecução penal também se manifesta na incorporação de ferramentas tecnológicas em diferentes fases do procedimento, incluindo mecanismos de negociação penal, como o Acordo de Não Persecução Penal (ANPP). A utilização de plataformas digitais, sistemas de gestão processual e bancos de dados interligados contribui para maior eficiência e celeridade, além de possibilitar a padronização de procedimentos. Contudo, essa modernização demanda cautela, uma vez que a automatização de decisões e a dependência de sistemas tecnológicos podem comprometer garantias fundamentais se não houver controle adequado (Bomfim; Silva, 2025).

No âmbito investigativo, destaca-se o uso crescente de tecnologias como o policiamento preditivo, que utiliza algoritmos e análise de dados para antecipar possíveis ocorrências criminais e direcionar a atuação estatal. A utilização de dados massivos e a interpretação automatizada de padrões comportamentais levantam preocupações relacionadas à confiabilidade das informações e ao risco de reforço de desigualdades estruturais (Vieira; Santos, 2025).

O policiamento preditivo, enquanto expressão da digitalização da persecução penal, deve ser compreendido dentro de um contexto mais amplo de transformação institucional, conforme destaca Balduino:

> O uso de algoritmos na segurança pública representa uma tentativa de racionalizar a atuação estatal, tornando-a mais eficiente e baseada em dados. Entretanto, a ausência de transparência nos critérios utilizados pelos sistemas e a dificuldade de auditoria dos resultados gerados levantam questionamentos relevantes acerca da legitimidade dessas ferramentas no âmbito da persecução penal, especialmente quando seus efeitos impactam diretamente direitos individuais e coletivos (Balduino, 2024, p. 143).

Embora as tecnologias digitais ampliem a capacidade investigativa do Estado, sua utilização não pode prescindir de mecanismos de controle e responsabilização. A modernização dos instrumentos investigativos e processuais contribui para maior eficiência e adaptação às novas formas de criminalidade, mas também exige uma reconfiguração dos parâmetros normativos e institucionais.

2.3 Prova penal e novas tecnologias

A prova penal, enquanto elemento central da persecução penal, tem passado por profundas transformações em razão da incorporação de novas tecnologias no contexto investigativo e processual. Tradicionalmente baseada em meios como testemunhos, documentos físicos e perícias materiais, a atividade probatória passou a incorporar evidências digitais, oriundas de dispositivos eletrônicos, sistemas informatizados e ambientes virtuais (Kist, 2024).

A admissibilidade da prova digital torna-se um dos principais pontos de debate no Direito Processual Penal contemporâneo. A obtenção de dados eletrônicos, muitas vezes realizada por meio de técnicas sofisticadas, deve respeitar os limites constitucionais, especialmente no que se refere à privacidade e à inviolabilidade das comunicações. Vieira e Santos (2025) destacam que o uso de tecnologias como o policiamento preditivo e a análise de dados massivos levanta questionamentos sobre a confiabilidade das informações utilizadas como base probatória, bem como sobre a transparência dos métodos empregados.

Além disso, a cadeia de custódia assume papel ainda mais relevante no contexto das provas tecnológicas, uma vez que a manipulação inadequada de dados digitais pode comprometer sua validade jurídica. Segundo Arigony, Botton e Arigony (2025), a rastreabilidade dos vestígios digitais é fundamental para assegurar a confiabilidade da prova, exigindo protocolos rigorosos de coleta, armazenamento e análise. A volatilidade das informações digitais, aliada à facilidade de alteração ou exclusão de dados, reforça a necessidade de procedimentos técnicos especializados e de profissionais capacitados.

A influência das novas tecnologias no Direito Penal amplia as possibilidades de produção probatória, mas também intensifica os riscos de violação de direitos fundamentais.

Botelho et al. (2023) ressaltam que a utilização indiscriminada de ferramentas tecnológicas pode resultar em práticas invasivas, como monitoramento excessivo e coleta massiva de dados, comprometendo garantias como a intimidade e a proteção de dados pessoais. No meio do debate, evidencia-se que a eficiência investigativa não pode se sobrepor aos limites jurídicos estabelecidos pelo ordenamento, sob pena de invalidar a prova obtida e comprometer a legitimidade da persecução penal.

2.4 Inteligência artificial na investigação criminal

A inteligência artificial (IA) tem se consolidado como uma das principais inovações tecnológicas aplicadas à investigação criminal, redefinindo a forma como dados são coletados, analisados e utilizados pelas autoridades responsáveis pela persecução penal. Em termos conceituais, a IA pode ser compreendida como um conjunto de sistemas computacionais capazes de simular processos cognitivos humanos, como aprendizado, reconhecimento de padrões e tomada de decisões, por meio de algoritmos e modelos estatísticos. No contexto jurídico-penal, seu funcionamento está diretamente associado ao uso de grandes volumes de dados (big data), que são processados para identificar correlações relevantes à investigação. Ferreira e Jacob (2025) destacam que a aplicação da IA no processo penal representa uma evolução significativa, ao permitir maior precisão e rapidez na análise de informações complexas, embora também imponha novos desafios à interpretação jurídica.

No âmbito da investigação criminal, a inteligência artificial tem sido amplamente utilizada em diversas aplicações práticas, que vão desde a análise de dados até a previsão de comportamentos delitivos. Sistemas de policiamento preditivo, por exemplo, utilizam algoritmos para identificar áreas com maior probabilidade de ocorrência de crimes, orientando a atuação das forças de segurança pública. Segundo Costa e Feller (2025), essas ferramentas ampliam significativamente a capacidade investigativa do Estado, tornando os processos mais ágeis e baseados em evidências empíricas, o que contribui para a eficiência da persecução penal.

Outro campo de destaque na aplicação da IA refere-se à investigação de crimes cibernéticos, nos quais a complexidade técnica exige soluções igualmente sofisticadas. Filho, Rodrigues e Cruz (2026) ressaltam que a utilização da inteligência artificial nesses casos permite não apenas a identificação mais rápida de delitos, mas também a antecipação de comportamentos criminosos, o que fortalece a atuação preventiva do Estado.

A inteligência artificial proporciona ganhos significativos em termos de eficiência, precisão e capacidade analítica. A automatização de tarefas repetitivas e a possibilidade de

processamento de grandes volumes de dados em curto espaço de tempo permitem que os investigadores concentrem seus esforços em atividades mais estratégicas. Entretanto, como apontam Bichara, Cascardo e Perazzoni (2024), tais benefícios devem ser analisados com cautela, uma vez que os sistemas de IA podem reproduzir vieses existentes nos dados utilizados, resultando em discriminação algorítmica e reforço de desigualdades estruturais.

2.5 Reconhecimento facial na investigação criminal

O reconhecimento facial constitui uma tecnologia baseada em inteligência artificial voltada à identificação ou verificação de indivíduos por meio da análise de características biométricas do rosto. Seu funcionamento ocorre a partir da captura de imagens por câmeras ou dispositivos digitais, seguida da extração de pontos nodais da face, como distância entre olhos, formato do nariz e contorno facial, que são convertidos em dados matemáticos e comparados com bancos de dados previamente armazenados. Conforme destacam Scopel e Puhl (2024), a utilização do reconhecimento facial como meio de prova no processo penal exige cautela, uma vez que sua validade depende da confiabilidade dos sistemas e da observância de garantias legais.

No Brasil, a adoção do reconhecimento facial tem se expandido significativamente nos últimos anos, especialmente em grandes centros urbanos e eventos de grande porte. Órgãos de segurança pública passaram a implementar sistemas de monitoramento com câmeras inteligentes capazes de identificar suspeitos em tempo real, integrando dados de diferentes bases institucionais. Martino (2022) observa que, no cenário internacional e nacional, o reconhecimento facial tem sido empregado como instrumento estratégico no combate ao crime organizado e ao terrorismo, embora sua aplicação levante questionamentos quanto aos limites jurídicos e à necessidade de regulamentação específica.

A eficiência do reconhecimento facial reside, sobretudo, na sua capacidade de processar grandes volumes de dados em curto espaço de tempo, oferecendo respostas rápidas às demandas investigativas. A automatização do reconhecimento de indivíduos reduz a dependência de métodos tradicionais, como reconhecimento pessoal por testemunhas, que frequentemente estão sujeitos a falhas humanas. No entanto, essa eficiência não é absoluta, sendo condicionada à qualidade dos algoritmos utilizados, à precisão dos bancos de dados e às condições ambientais de captação das imagens.

> [...] o reconhecimento facial, embora represente um avanço significativo na segurança pública, não pode ser compreendido como uma ferramenta infalível, uma vez que sua eficácia

> depende de múltiplos fatores técnicos e operacionais, incluindo a qualidade das imagens, a atualização dos bancos de dados e a ausência de vieses nos algoritmos utilizados, fatores estes que podem comprometer a precisão dos resultados e gerar consequências jurídicas relevantes (Mezzomo, 2024).

A tecnologia deve ser utilizada com cautela, especialmente no contexto da produção de provas penais. As limitações do reconhecimento facial digital têm sido amplamente discutidas na literatura, sobretudo no que se refere aos riscos de erros judiciais e discriminação algorítmica. Cani e Nunes (2022) destacam que os sistemas de reconhecimento facial podem apresentar taxas de erro mais elevadas em relação a determinados grupos populacionais, em razão de vieses presentes nos dados utilizados para treinamento dos algoritmos

2.6 Riscos e desafios jurídicos

A incorporação da inteligência artificial e do reconhecimento facial na investigação criminal suscita relevantes reflexões acerca da proteção dos direitos fundamentais no Estado Democrático de Direito. Conforme destacam Costa e Feller (2025), o uso da inteligência artificial no âmbito investigativo deve ser orientado por critérios jurídicos que garantam a legalidade e a proporcionalidade das intervenções, evitando abusos decorrentes da ampliação do poder estatal.

A utilização de sistemas de reconhecimento facial, em especial, intensifica o debate sobre a proteção de dados pessoais e a vigilância massiva. A coleta de informações biométricas sem o devido controle pode configurar violação à intimidade e à autodeterminação informativa dos indivíduos, sobretudo quando realizada de forma indiscriminada em espaços públicos. Santos e Jacob (2025) ressaltam que a identificação criminal em meios eletrônicos, embora eficiente, apresenta desafios significativos quanto à garantia da confiabilidade dos dados e à prevenção de erros que possam comprometer direitos fundamentais.

Outro aspecto relevante refere-se à possibilidade de discriminação algorítmica, decorrente do uso de sistemas de inteligência artificial treinados com bases de dados enviesadas. Tais sistemas podem reproduzir e até amplificar desigualdades estruturais, afetando de maneira desproporcional determinados grupos sociais. Hermes e Leal (2025) apontam que a integração entre inteligência artificial e políticas públicas de segurança deve considerar a necessidade de proteção dos direitos fundamentais, evitando que a busca por eficiência resulte em práticas discriminatórias ou em violações sistemáticas de garantias individuais.

Além disso, a utilização de provas obtidas por meio dessas tecnologias levanta questionamentos quanto ao devido processo legal, ao contraditório e à ampla defesa. A

opacidade dos algoritmos, muitas vezes classificados como “caixas-pretas”, dificulta a compreensão dos critérios utilizados para a tomada de decisões automatizadas, o que pode comprometer a possibilidade de contestação por parte da defesa. Costa e Feller (2025) destacam que a legitimidade da prova tecnológica depende da sua auditabilidade e da possibilidade de verificação por peritos independentes, garantindo que o acusado tenha pleno acesso aos elementos que fundamentam a acusação.

A proteção de dados pessoais no contexto da investigação criminal ganhou centralidade com a crescente utilização de tecnologias como a inteligência artificial e o reconhecimento facial. Essas ferramentas, ao operarem por meio da coleta, armazenamento e processamento de grandes volumes de informações, frequentemente lidam com dados sensíveis, incluindo informações biométricas e comportamentais dos indivíduos, sendo de extrema importância assegurar que o uso dessas tecnologias esteja em conformidade com os princípios que regem a proteção de dados, especialmente no que se refere à privacidade e à autodeterminação informativa, uma vez que, a atividade de inteligência em segurança pública deve buscar um equilíbrio entre a eficiência investigativa e a preservação dos direitos individuais (Costa, 2024).

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece um marco normativo fundamental para a regulamentação do tratamento de dados pessoais no Brasil, incluindo aqueles utilizados no âmbito da segurança pública. A legislação prevê hipóteses específicas de tratamento para fins de investigação e repressão penal, mas também impõe limites claros, como a observância dos princípios da finalidade, necessidade, adequação e segurança. O uso de inteligência artificial e reconhecimento facial deve estar alinhado a esses parâmetros, garantindo que a coleta e o processamento de dados sejam realizados de forma proporcional e justificada, assegurando que o avanço tecnológico não comprometa direitos fundamentais (Brasil, 2018).

Sistemas de reconhecimento facial, por exemplo, dependem de bancos de dados extensos e atualizados, o que pode gerar riscos de vazamento, uso indevido ou compartilhamento não autorizado de informações. Santos e Jacob (2025) ressaltam que a identificação criminal em meios eletrônicos exige mecanismos rigorosos de controle e validação, a fim de garantir a confiabilidade dos dados e prevenir erros que possam resultar em prejuízos aos indivíduos.

O devido processo legal representa um dos fundamentos estruturantes do processo penal, assegurando que a atuação estatal na persecução criminal ocorra dentro de limites previamente estabelecidos, com respeito às garantias individuais e aos direitos fundamentais. A utilização de dados digitais, algoritmos e sistemas automatizados exige não apenas eficiência

técnica, mas também conformidade com os princípios constitucionais que regem o processo penal. A admissibilidade das provas digitais deve ser analisada à luz do devido processo legal, considerando a legalidade de sua obtenção e a confiabilidade dos meios utilizados (Vieira; Santos, 2025).

A prova tecnológica, por sua natureza imaterial e altamente volátil, demanda cuidados específicos quanto à sua coleta, preservação e análise, especialmente no que se refere à cadeia de custódia. A integridade dos dados digitais pode ser facilmente comprometida por manipulações indevidas ou falhas nos sistemas utilizados, o que impacta diretamente sua validade no processo penal. Arigony, Botton e Arigony (2025) destacam que a persecução penal na era da informação exige protocolos rigorosos que garantam a rastreabilidade dos vestígios digitais, assegurando que a prova apresentada em juízo seja autêntica e confiável.

Outro aspecto relevante refere-se à possibilidade de contestação das provas tecnológicas pela defesa, elemento essencial para a efetivação do contraditório e da ampla defesa. A complexidade dos sistemas utilizados na produção de provas digitais, muitas vezes baseados em algoritmos de difícil compreensão, pode dificultar o acesso pleno às informações necessárias para a impugnação. Conforme apontam Moreira, Ferracini e Sandaniel (2025), os avanços tecnológicos no Direito Penal impõem a necessidade de adaptação das estruturas processuais, de modo a garantir que o acusado tenha condições reais de compreender e contestar os elementos probatórios apresentados contra si.

Além disso, a obtenção de provas por meio de tecnologias digitais deve respeitar limites legais claros, especialmente no que se refere à proteção da privacidade e à inviolabilidade das comunicações. A utilização de ferramentas como interceptações telemáticas, monitoramento de dados e análise de informações pessoais deve estar condicionada à autorização judicial e à observância do princípio da proporcionalidade. Vieira e Santos (2025) enfatizam que a busca por eficiência investigativa não pode justificar a adoção de práticas que violem direitos fundamentais, sob pena de comprometer a legitimidade do processo penal.

2.7 Regulamentação no ordenamento jurídico brasileiro

A regulamentação do uso de inteligência artificial e reconhecimento facial na investigação criminal no ordenamento jurídico brasileiro ainda se encontra em processo de consolidação, refletindo o descompasso entre o avanço tecnológico e a evolução normativa. Embora tais tecnologias já sejam amplamente utilizadas por órgãos de segurança pública, o arcabouço jurídico existente não foi originalmente concebido para lidar com as especificidades

desses instrumentos digitais. Scopel e Puhl (2024) destacam que a utilização do reconhecimento facial como meio de prova exige uma regulamentação mais específica, capaz de garantir sua validade sem comprometer direitos fundamentais.

No plano normativo, a legislação brasileira dispõe de instrumentos relevantes que tangenciam o uso de tecnologias digitais na investigação criminal, como normas relativas à proteção de dados, à interceptação de comunicações e à produção de provas. Contudo, tais dispositivos não abordam de forma direta as particularidades da inteligência artificial e do reconhecimento facial, especialmente no que se refere à transparência dos algoritmos e à auditabilidade dos sistemas utilizados (Santos; Jacob, 2025).

A ausência de regulamentação específica sobre o uso dessas tecnologias contribui para a ampliação de riscos relacionados à discriminação algorítmica e à violação de direitos fundamentais. Sistemas de reconhecimento facial, quando utilizados sem critérios rigorosos, podem reproduzir vieses presentes nos dados utilizados para seu treinamento, afetando de maneira desproporcional determinados grupos sociais. As falhas na regulamentação da inteligência artificial dificultam o enfrentamento dessas distorções, comprometendo a efetividade de mecanismos de controle e responsabilização (Negri; Winter, 2025).

Outro aspecto relevante refere-se à necessidade de estabelecimento de parâmetros claros para o uso legítimo da inteligência artificial e do reconhecimento facial na investigação criminal. A definição de critérios como proporcionalidade, finalidade e necessidade torna-se essencial para assegurar que a utilização dessas ferramentas ocorra dentro dos limites constitucionais. Scopel e Puhl (2024) ressaltam que a admissibilidade da prova obtida por meio de reconhecimento facial deve estar condicionada à observância de garantias processuais, incluindo a possibilidade de contestação pela defesa e a verificação da confiabilidade do sistema utilizado.

3 MATERIAL E MÉTODOS

A presente pesquisa caracteriza-se como um estudo de natureza bibliográfica e documental, voltado à análise do uso da inteligência artificial e do reconhecimento facial na investigação criminal, com enfoque nos impactos sobre a eficiência investigativa e na proteção dos direitos fundamentais. A investigação fundamenta-se em produções acadêmicas recentes, legislações vigentes e documentos institucionais, permitindo a construção de uma análise crítica e sistematizada do tema proposto. Trata-se de um estudo de caráter exploratório e descritivo,

na medida em que busca aprofundar a compreensão sobre fenômenos contemporâneos ainda em consolidação no campo jurídico.

Quanto à abordagem, a pesquisa adota o método qualitativo, uma vez que se dedica à interpretação de conteúdos normativos, doutrinários e científicos, com o objetivo de identificar padrões, categorias e relações entre os elementos analisados. O método de abordagem utilizado é o indutivo, partindo da análise de estudos específicos sobre tecnologias aplicadas à investigação criminal para a formulação de conclusões mais amplas acerca de seus impactos no ordenamento jurídico brasileiro.

No que se refere aos materiais utilizados, o estudo baseia-se em artigos científicos, livros, legislações e documentos oficiais, selecionados a partir de critérios de relevância temática, atualidade e confiabilidade. As fontes foram obtidas por meio de bases de dados como Google Acadêmico e SciELO, priorizando publicações entre os anos de 2020 e 2026, de modo a garantir a contemporaneidade das discussões. Também foram analisadas normas jurídicas pertinentes, como a legislação de proteção de dados e dispositivos relacionados à persecução penal, com o intuito de compreender o arcabouço normativo aplicável ao uso das tecnologias investigativas.

A coleta de dados foi realizada por meio de levantamento bibliográfico sistematizado, utilizando palavras-chave relacionadas à inteligência artificial, reconhecimento facial, investigação criminal, prova digital e direitos fundamentais. Após a seleção das fontes, procedeu-se à leitura exploratória, seletiva e analítica dos materiais, com organização das informações em fichamentos temáticos. Essa etapa permitiu identificar os principais argumentos, conceitos e contribuições dos autores, facilitando a construção do referencial teórico e da análise crítica desenvolvida ao longo do trabalho.

A análise dos dados foi conduzida por meio da técnica de análise de conteúdo, possibilitando a categorização das informações em eixos temáticos, como eficiência tecnológica, riscos jurídicos e proteção de direitos fundamentais. Essa sistematização favoreceu a articulação entre teoria e prática, permitindo a interpretação crítica dos dados à luz dos objetivos da pesquisa. Dessa forma, a metodologia adotada assegura rigor científico e coerência analítica, contribuindo para a produção de um estudo consistente e alinhado às exigências acadêmicas.

4 RESULTADOS E DISCUSSÃO

4.1 Eficiência das tecnologias

A análise dos dados e da literatura evidencia que a incorporação da inteligência artificial e do reconhecimento facial na investigação criminal tem contribuído significativamente para o

aumento da eficiência dos procedimentos investigativos. Essas tecnologias permitem o processamento de grandes volumes de informações em tempo reduzido, viabilizando a identificação de padrões, a localização de suspeitos e a antecipação de condutas criminosas com maior precisão, sendo possível observar uma mudança no paradigma investigativo, que passa a ser orientado por dados e por ferramentas automatizadas de análise, ampliando a capacidade de resposta das instituições de segurança pública. Conforme destacam Costa e Feller (2025), o uso da inteligência artificial possibilita uma atuação mais estratégica e baseada em evidências, reduzindo a dependência exclusiva de métodos tradicionais.

O reconhecimento facial tem se mostrado um instrumento relevante para a identificação de indivíduos em espaços públicos e para a localização de pessoas procuradas pela justiça, a sua utilização em tempo real integrada a bancos de dados, contribui para a celeridade das investigações e para o aumento da taxa de resolução de crimes. A aplicação dessa tecnologia como meio de prova pode fortalecer a persecução penal, desde que observados critérios técnicos que assegurem sua confiabilidade. Assim, os resultados indicam que essas tecnologias desempenham papel relevante na modernização da investigação criminal, tornando-a mais eficiente e adaptada às dinâmicas contemporâneas (Scopel; Puhl, 2024).

4.2 Riscos identificados

Apesar dos benefícios observados, a utilização de inteligência artificial e reconhecimento facial na investigação criminal apresenta riscos significativos que impactam diretamente a proteção dos direitos fundamentais. Um dos principais problemas identificados refere-se à possibilidade de discriminação algorítmica, decorrente de vieses presentes nos dados utilizados para o treinamento dos sistemas. Bichara, Cascardo e Perazzoni (2024) alertam que o uso indiscriminado da inteligência artificial pode reforçar desigualdades estruturais, especialmente quando não há mecanismos adequados de controle e auditoria.

Outro risco relevante diz respeito à violação da privacidade e à coleta excessiva de dados pessoais, especialmente no caso do reconhecimento facial em espaços públicos. A ausência de regulamentação específica e de transparência nos processos de tratamento de dados pode resultar em práticas de vigilância massiva, incompatíveis com os princípios constitucionais. A identificação criminal em meios eletrônicos exige limites claros e mecanismos de responsabilização, a fim de evitar abusos e garantir a proteção dos indivíduos (Santos; Jacob, 2025).

4.3 Equilíbrio entre eficiência e direitos fundamentais

A partir da análise realizada, verifica-se que o principal desafio na utilização de inteligência artificial e reconhecimento facial na investigação criminal consiste em estabelecer um equilíbrio entre a busca por eficiência e a preservação dos direitos fundamentais. Embora essas tecnologias ofereçam vantagens operacionais relevantes, sua utilização deve estar condicionada ao respeito aos princípios constitucionais, como legalidade, proporcionalidade e devido processo legal. A eficiência investigativa não pode ser considerada um valor absoluto, devendo ser ponderada à luz das garantias individuais. Conforme afirmam Hermes e Leal (2025), a incorporação de tecnologias na segurança pública deve estar alinhada à promoção dos direitos fundamentais, evitando que o avanço tecnológico resulte em violações sistemáticas.

Ademais, a construção desse equilíbrio depende da implementação de marcos regulatórios adequados, bem como de mecanismos de controle que assegurem a transparência e a auditabilidade dos sistemas utilizados. A possibilidade de contestação das provas tecnológicas pela defesa e a garantia de acesso às informações que fundamentam as decisões automatizadas são elementos essenciais para a legitimidade da persecução penal. Assim, os resultados indicam que a adoção responsável dessas tecnologias exige uma atuação integrada entre inovação técnica e rigor jurídico, de modo a assegurar que a eficiência investigativa não comprometa os fundamentos do Estado Democrático de Direito (Vieira; Santos, 2025).

4.4 O Projeto de Lei da Inteligência Artificial e a necessidade de regulamentação específica na investigação criminal.

O avanço da inteligência artificial aplicada à investigação criminal evidencia a necessidade de construção de mecanismos normativos capazes de compatibilizar inovação tecnológica e proteção dos direitos fundamentais. Embora o ordenamento jurídico brasileiro possua dispositivos relevantes relacionados à proteção de dados pessoais e às garantias processuais penais, verifica-se a inexistência de regulamentação específica suficientemente detalhada acerca da utilização de sistemas de inteligência artificial e reconhecimento facial na persecução penal.

Nesse contexto, destaca-se o Projeto de Lei nº 2.338/2023, em tramitação no Congresso Nacional cujo autor é o Senador Rodrigo Pacheco, dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana e na proteção dos direitos fundamentais. A proposta legislativa busca instituir o marco regulatório da inteligência artificial no Brasil, estabelecendo princípios relevantes para o

desenvolvimento e utilização dessas tecnologias, dentre eles a supervisão humana, a transparência algorítmica, a prevenção da discriminação, a responsabilização dos agentes envolvidos e a proteção dos direitos fundamentais. Observa-se que o projeto adota uma perspectiva baseada em riscos, classificando determinados sistemas de inteligência artificial como de "alto risco", especialmente aqueles utilizados pelo Poder Público em atividades relacionadas à segurança pública e persecução penal.

A relevância dessa regulamentação torna-se ainda mais evidente diante dos riscos identificados na utilização da inteligência artificial aplicada à investigação criminal. Conforme observa O'Neil (2017 apud BICHARA; CASCARDO; PERAZZONI,2024) a utilização de estatísticas como fundamento para decisões policiais pode resultar na automatização de preconceitos já existentes na sociedade, intensificando desigualdades no tratamento jurídico conferido aos indivíduos. Isso ocorre porque sistemas algorítmicos operam a partir de padrões extraídos de bancos de dados historicamente marcados por seletividades sociais e raciais.

Nessa mesma perspectiva, Bichara, Cascardo e Perazzoni (2024) ressaltam que o chamado racismo algorítmico constitui um dos principais desafios éticos e jurídicos decorrentes da utilização da inteligência artificial na segurança pública. Segundo os autores, determinados sistemas automatizados apresentam maior incidência de erros em relação a grupos racialmente vulnerabilizados, comprometendo princípios fundamentais como igualdade, dignidade da pessoa humana e presunção de inocência. Os autores destacam, ainda, que a inteligência artificial, ao contrário do que muitas vezes se acredita, não consiste em ferramenta plenamente neutra ou isenta de vieses, uma vez que opera a partir de dados produzidos socialmente, refletindo e até mesmo reforçando desigualdades estruturais já existentes. No contexto da investigação criminal, tal problemática torna-se especialmente alarmante, considerando o elevado potencial de produção de injustiças decorrentes da automatização de decisões e da reprodução de padrões discriminatórios.

Além disso, Bichara, Cascardo e Perazzoni (2024) afirmam que o racismo algorítmico não deve ser compreendido apenas como falha técnica passível de correção mediante simples ajustes computacionais, mas como expressão de desigualdades sociais historicamente consolidadas. Nesse sentido, o enfrentamento desses vieses exige abordagem interdisciplinar envolvendo direito, ética, tecnologia e políticas públicas, bem como a inclusão de perspectivas diversas nos processos de desenvolvimento e implementação dos sistemas de inteligência artificial, visando assegurar maior transparência, equidade e respeito aos direitos fundamentais no âmbito da investigação criminal.

Sob essa perspectiva, verifica-se que a regulamentação da inteligência artificial na investigação criminal não possui apenas finalidade técnica, mas também constitucional e processual penal. A criação de parâmetros jurídicos claros é essencial para assegurar que o uso dessas tecnologias respeite princípios como legalidade, proporcionalidade, igualdade e devido processo legal, além de garantir o contraditório, a ampla defesa e a presunção de inocência. Dessa forma, busca-se evitar práticas abusivas e assegurar equilíbrio entre eficiência investigativa e proteção das garantias fundamentais no âmbito do processo penal.

5 CONSIDERAÇÕES FINAIS

A presente pesquisa analisou os impactos da inteligência artificial e do reconhecimento facial na investigação criminal no Brasil, evidenciando que essas tecnologias contribuem significativamente para o aumento da eficiência investigativa, especialmente na análise de dados e identificação de suspeitos. Observa-se que a inovação tecnológica tem potencial para modernizar a persecução penal e torná-la mais ágil e estratégica.

Entretanto, também foram identificados riscos relevantes, sobretudo no que se refere à privacidade, à proteção de dados pessoais, à possibilidade de discriminação algorítmica e às garantias do devido processo legal. A ausência de regulamentação específica e a opacidade dos sistemas tecnológicos podem comprometer a transparência e a segurança jurídica, reforçando a necessidade de controle sobre o uso dessas ferramentas.

Além disso, verificou-se que o ordenamento jurídico brasileiro ainda apresenta lacunas quanto à regulamentação dessas tecnologias, o que evidencia a necessidade de atualização normativa. A aplicação da inteligência artificial e do reconhecimento facial deve observar princípios como legalidade, proporcionalidade e transparência, garantindo compatibilidade com os direitos fundamentais.

Conclui-se, portanto, que o desafio central consiste em equilibrar a eficiência investigativa com a proteção dos direitos fundamentais. Para isso, é essencial o desenvolvimento de marcos regulatórios específicos e mecanismos de fiscalização, de modo a assegurar que o uso dessas tecnologias ocorra de forma legítima, responsável e compatível com o Estado Democrático de Direito.

REFERÊNCIAS

ARIGONY, Marcelo Mendes; BOTTON, Letícia Thomasi Jahnke; ARIGONY, Ana Luiza Ortiz. Persecução penal digital: a prova na era da informação. **Direito & TI**, v. 1, n. 20, p. 1-22, 2025. Disponível em: https://direitoeti.com.br/direitoeti/article/download/268/173

BALDUINO, Ederson Silva. **O Impacto do Policiamento Preditivo na Persecução Penal: uma breve análise**. Editora Dialética, p. 143, 2024.

BICHARA, Anderson Andrade; CASCARDO, Agostinho Gomes; PERAZZONI, Franco. Racismo algorítmico, reforço de preconceitos e uso de IA: perspectivas e desafios para a investigação criminal digital. **Boletim IBCCRIM**, v. 32, n. 379, p. 23-26, 2024. Disponível em: https://www.publicacoes.ibccrim.org.br/index.php/boletim_1993/article/download/1069/403

BOMFIM, Sérgio Henrique Tenório; SILVA, Ivan Luiz Rufino. Acordo de não persecução penal (anpp) e a possibilidade de aplicação de ferramentas tecnológicas. **Seminário Internacional Estado, Regulação e Transformação Digital**, v. 4, p. e562-e562, 2025. Disponível em: https://periodicos.univel.br/ojs/index.php/siert/article/download/562/421

BOTELHO, Daniela Garcia et al. A influência das novas tecnologias no direito penal–desafios e perspectivas. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 9, n. 11, p. 2713-2726, 2023. Disponível em: https://periodicorease.pro.br/rease/article/download/12347/5898

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.

CANI, Luiz Eduardo; NUNES, João Alcantara. Erros judiciários em tempos de digital surveillance: os algoritmos de reconhecimento facial em questão. **Revista Brasileira de Direito Processual Penal**, v. 8, p. 679-712, 2022. Disponível em: https://www.scielo.br/j/rbdpp/a/6SKBnyRpzzB9C8ZZnBLZYLb/?format=html&lang=pt

COSTA, Mauir Victor da Silva; FELLER, Thiago. O uso da inteligência artificial na investigação criminal. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 11, n. 11, p. 2689-2703, 2025. Disponível em: https://periodicorease.pro.br/rease/article/download/22095/13668

COSTA, Rafael Di Lorenzo. Lei geral de proteção de dados e a atividade de inteligência em segurança pública: uma análise profícua entre a privacidade individual e a segurança coletiva. **RECIMA21- Revista Científica Multidisciplinar**-ISSN 2675-6218, v. 5, n. 10, p. e5105813-e5105813, 2024. Disponível em: https://recima21.com.br/index.php/recima21/article/download/5813/3960

DANTAS, Marcelo Navarro Ribeiro; COSTA, João Carlos Faria. Investigação defensiva: a evolução do tema e os problemas de sua aplicabilidade. **Prisma Juridico**, v. 20, n. 2, p. 351-374, 2021. Disponível em: https://uninove.emnuvens.com.br/prisma/article/download/21010/9420

FERREIRA, Gabriel Marchiori; JACOB, Alexandre. O uso da inteligência artificial no processo penal: avanços, limites e desafios na investigação criminal. **Revista Multidisciplinar do Nordeste Mineiro**, v. 19, n. 1, p. 1-12, 2025. Disponível em: https://remunom.ojsbr.com/multidisciplinar/article/download/4656/4437

FILHO, Antônio Ferreira; RODRIGUES, Andrezza; CRUZ, Hajime Hattori Xaud. A aplicação da inteligência artificial na investigação de crimes cibernéticos: avanços tecnológicos e impactos no sistema jurídico-forense. **REMUNOM**, v. 13, n. 05, p. 1-28, 2026. Disponível em: https://remunom.ojsbr.com/multidisciplinar/article/download/6039/5558

HERMES, Pedro Henrique; LEAL, Rogério. Inteligência artificial, políticas públicas e segurança pública: aproximações e sinergias para a tutela de direitos fundamentais. **Direito UNIFACS–Debate Virtual-Qualis A2 em Direito**, n. 298, 2025. Disponível em: https://revistas.unifacs.br/index.php/redu/article/viewFile/9600/5397

KIST, Dario José. **Prova digital no processo penal**. Editora Mizuno, p. 87, 2024.

MACHADO, Rodrigo Prestes et al. Investigação forense e perícia criminal: revisão sistemática da literatura e análise de estudos. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 12, n. 3, p. 1-60, 2026. Disponível em: https://periodicorease.pro.br/rease/article/download/24292/15855

MARTINO, Fabio Nunes. A Utilização do Reconhecimento Facial como Instrumento de Combate ao Crime Organizado Transnacional e ao Terrorismo: Limites e Perspectivas. **Revista Judicial Brasileira**, v. 2, n. 1, 2022. Disponível em: https://revistadaenfam.emnuvens.com.br/renfam/article/download/186/54

MEZZOMO, Maria Luiza. **O uso do reconhecimento facial na investigação criminal e na segurança pública**. Almedina, p. 204, 2024. Disponível em: https://www.almedina.net/o-uso-do-reconhecimento-facial-na-investigacao-criminal-e-na-seguranca-publica-1716602475.html?utm_source=chatgpt.com

MOREIRA, Mayume Caires; FERRACINI, Gabriela Sanches; SANDANIEL, Pietra. A Tecnologia no direito penal e como os avanços tecnológicos impactam nas investigações criminais. In: **Anais do CDU-Congresso de Direito UniCesumar**. 2025. p. 980-988. Disponível em: https://lgpublica.com/index.php/anaiscdu/article/download/366/382

NEGRI, A.; WINTER, L. Falhas Da Regulamentação Da Inteligência Artificial No Combate À Discriminação Algorítmica Realizada Pelo Reconhecimento Facial. **Revista Rede De Direito Digital, Intelectual & Sociedade**, v. 3, 2025. Disponível em: https://revistas.ufpr.br/rrddis/article/download/99342/75018

REZENDE, Mateus. Avanço tecnológico na investigação criminal e seus impactos no direito penal. **Anais Colóquio Estadual de Pesquisa Multidisciplinar.** ISSN-2527-2500, 2025. Disponível em: http://publicacoes.unifimes.edu.br/index.php/coloquio/article/download/4679/2761

SANTOS, Hárnefer Wagmacker; JACOB, Alexandre. Desafios na identificação criminal em meios eletrônicos: o papel da inteligência artificial na investigação e prevenção de crimes digitais. **Revista Multidisciplinar do Nordeste Mineiro**, v. 18, n. 1, p. 1-12, 2025. Disponível em: https://remunom.ojsbr.com/multidisciplinar/article/download/4563/4355

SCOPEL, Bruna Gonçalves; PUHL, Eduardo. A tecnologia de reconhecimento facial e sua utilização como prova no processo penal. **Academia de Direito**, v. 6, p. 3678-3700, 2024. Disponível em: https://periodicos.unc.br/index.php/acaddir/article/download/5587/2405

VIEIRA, Andrey Bruno Cavalcante; SANTOS, Hugo Leonardo Rodrigues. Investigação criminal e tecnologias digitais: algumas reflexões sobre o policiamento preditivo ea admissibilidade de provas digitais. **Revista Brasileira de Direito Processual Penal**, v. 11, n. 1, p. e1072, 2025. Disponível em: https://www.scielo.br/j/rbdpp/a/MkHbcfkX7SNpg4pBK5kvHGb/?format=pdf&lang=pt