

Novas tecnologias em investigação criminal: o uso da inteligência artificial.

New technologies in criminal investigation: the use of artificial intelligence.

Mayara Alves¹

Marcos Silva Leles

Rildo José do Nascimento

João Batista Lindolfo

RESUMO

A incorporação da inteligência artificial (IA) às atividades de segurança pública, investigação criminal e ciências forenses vem modificando a forma como grandes volumes de dados são coletados, organizados, correlacionados e interpretados. Este estudo apresenta uma revisão de literatura sobre as principais aplicações da IA na investigação criminal, com ênfase em reconhecimento facial, análise de imagens e vídeos, identificação humana, genética forense, toxicologia, perícia digital, análise de padrões criminais e apoio à tomada de decisão. A revisão foi construída a partir de literatura científica indexada e de revisões sistemáticas e de escopo publicadas em periódicos especializados, priorizando estudos recentes e trabalhos de referência sobre inteligência artificial, aprendizado de máquina e ciências forenses. Os achados indicam que a IA pode ampliar a velocidade de triagem de evidências, auxiliar na identificação de padrões e apoiar especialistas em tarefas repetitivas ou de elevada complexidade. Entretanto, a literatura também evidencia limitações relacionadas à qualidade e representatividade dos bancos de dados,

¹ Posto de Atendimento da Polícia Técnico-Científica – Brasil. ORCID: 0009-0006-7623-9685.

validação externa, explicabilidade, vieses algorítmicos, segurança cibernética, proteção de dados e necessidade de supervisão humana. Na investigação criminal, portanto, a IA deve ser compreendida como ferramenta de apoio à atividade investigativa e pericial, e não como substituta do julgamento técnico, científico ou jurídico. Conclui-se que a adoção responsável dessas tecnologias exige protocolos de validação, rastreabilidade, auditoria, transparência, capacitação profissional e integração interdisciplinar entre especialistas em investigação, perícia, direito e ciência de dados.

Palavras-chave: Inteligência artificial. Investigação criminal. Ciências forenses. Aprendizado de máquina. Perícia criminal. Evidência digital.

ABSTRACT

The incorporation of artificial intelligence (AI) into public security, criminal investigation and forensic science is changing the way large volumes of data are collected, organized, correlated and interpreted. This study presents a literature review on the main applications of AI in criminal investigation, focusing on facial recognition, image and video analysis, human identification, forensic genetics, toxicology, digital forensics, crime pattern analysis and decision support. The review was based on indexed scientific literature and systematic and scoping reviews published in specialized journals, prioritizing recent studies and reference works on artificial intelligence, machine learning and forensic sciences. The findings indicate that AI can increase the speed of evidence screening, assist in pattern identification and support experts in repetitive or highly complex tasks. However, the literature also highlights limitations related to the quality and representativeness of databases, external validation, explainability, algorithmic bias, cybersecurity, data protection and the need for human oversight. In criminal investigation, therefore, AI should be understood as a support tool for investigative and forensic activities rather than a substitute for technical, scientific or legal judgment. Responsible adoption requires validation protocols, traceability, auditing, transparency, professional training and interdisciplinary integration among investigators, forensic experts, legal professionals and data scientists.

Keywords: Artificial intelligence. Criminal investigation. Forensic science. Machine learning. Criminalistics. Digital evidence.

1 INTRODUÇÃO

A transformação digital das relações sociais produziu uma expansão sem precedentes da quantidade de informação potencialmente relevante para a investigação criminal. Registros de câmeras, fotografias, vídeos, mensagens, arquivos armazenados em dispositivos, dados de localização, informações biométricas, perfis genéticos e registros de transações constituem apenas parte do universo de dados que pode integrar uma investigação. O desafio contemporâneo não consiste apenas em obter essas informações, mas em examiná-las de maneira rápida, tecnicamente fundamentada, reproduzível e juridicamente legítima.

Nesse contexto, a inteligência artificial passou a ocupar posição de destaque. Técnicas de aprendizado de máquina, visão computacional, processamento de linguagem natural e redes neurais profundas permitem reconhecer padrões em grandes conjuntos de dados que seriam difíceis de examinar manualmente. Revisões recentes mostram crescimento acelerado das aplicações de IA nas ciências forenses e na segurança pública, abrangendo desde identificação humana até análise de evidências digitais e apoio à análise de padrões criminais (Ketsekioulafis et al., 2024; Farber, 2026).

Na investigação criminal, a utilidade da IA não está necessariamente em produzir uma resposta definitiva, mas em reduzir o tempo necessário para localizar informações relevantes, priorizar evidências, estabelecer conexões e auxiliar o especialista na interpretação de dados. Essa distinção é fundamental porque resultados algorítmicos podem apresentar incerteza, depender da qualidade dos dados de treinamento e reproduzir vieses presentes nas bases utilizadas. Berk (2021), ao analisar IA, policiamento preditivo e avaliação de risco, destaca que questões de precisão, justiça e transparência não possuem solução exclusivamente técnica.

As ciências forenses apresentam exigências adicionais. Uma ferramenta destinada a auxiliar uma investigação precisa demonstrar desempenho adequado em condições próximas às encontradas nos casos reais, apresentar documentação sobre sua validação e permitir que o resultado seja interpretado dentro dos limites científicos do método. A recente revisão sistemática de Bugelli et al. (2026), dedicada à identificação pessoal, evidencia o crescimento das aplicações de IA, mas também a necessidade de avaliar desempenho, aplicabilidade e limitações dos modelos antes de sua incorporação ao trabalho forense.

Diante desse cenário, esta revisão de literatura tem como objetivo analisar as principais aplicações da inteligência artificial na investigação criminal e nas ciências forenses, discutir seus benefícios e limitações e identificar requisitos para uma adoção responsável. Busca-se responder à seguinte questão: de que maneira as tecnologias de IA podem contribuir para a investigação criminal e quais fatores limitam sua utilização segura, confiável e juridicamente adequada? No cenário brasileiro, essa abordagem dialoga com estudos dos autores sobre a atuação da Polícia Científica na elucidação de crimes, especialmente quanto à produção da prova material, cadeia de custódia e incorporação de tecnologias forenses (ALVES et al., 2026).

A relevância do tema decorre da crescente digitalização da atividade criminosa e da própria investigação. O volume de imagens, dados digitais e informações biométricas cresce mais rapidamente que a capacidade humana de realizar triagens manuais. Ao mesmo tempo, a utilização de algoritmos em decisões relacionadas à segurança pública pode afetar direitos fundamentais. Assim, discutir a tecnologia sem discutir validação, governança e responsabilidade seria insuficiente.

2 METODOLOGIA

Trata-se de uma revisão narrativa de literatura, com abordagem qualitativa e caráter descritivo-analítico. A pesquisa bibliográfica foi orientada pela combinação dos termos “artificial intelligence”, “machine learning”, “criminal investigation”, “forensic science”, “digital forensics”, “facial recognition”, “forensic DNA”, “forensic toxicology” e “predictive policing”, considerando publicações científicas disponíveis em bases e periódicos indexados.

Foram priorizados artigos de revisão sistemática, revisões de escopo e revisões críticas publicados em periódicos científicos, especialmente entre 2020 e 2026, além de estudos de referência necessários para contextualizar o tema. Foram incluídos trabalhos que abordassem aplicações da IA diretamente relacionadas à investigação criminal, segurança pública, identificação humana, perícia criminal, medicina legal, genética forense, toxicologia forense, análise de imagens ou perícia digital.

Foram excluídos textos sem caráter científico, materiais predominantemente opinativos e publicações sem relação direta com investigação criminal ou ciências forenses. A análise temática foi organizada em categorias: identificação e biometria; análise de imagens e vídeos;

perícia digital; genética e DNA forense; toxicologia; análise criminal e policiamento preditivo; limitações técnicas; aspectos éticos e jurídicos; e perspectivas de implementação.

A estratégia não pretendeu realizar uma revisão sistemática com metanálise, mas sintetizar criticamente a literatura científica disponível para compreender o estado atual das aplicações de IA na investigação criminal. A seleção de revisões recentes permitiu incorporar resultados consolidados e, simultaneamente, identificar desafios metodológicos recorrentes, como validação insuficiente, datasets pequenos, falta de padronização e dificuldade de generalização dos modelos.

3 INTELIGÊNCIA ARTIFICIAL E TRANSFORMAÇÃO DA INVESTIGAÇÃO CRIMINAL

Inteligência artificial é um termo abrangente utilizado para designar sistemas capazes de executar tarefas que, em diferentes graus, envolvem percepção, classificação, aprendizagem, previsão ou tomada de decisão. No contexto das ciências forenses, é especialmente relevante o aprendizado de máquina, no qual algoritmos identificam relações em dados e constroem modelos capazes de classificar ou estimar resultados.

A aplicação da IA modifica principalmente a etapa de triagem. Um investigador ou perito pode receber milhares de imagens, documentos, registros ou sinais digitais. A análise manual de todo esse material pode ser demorada e sujeita à fadiga. Sistemas automatizados podem selecionar objetos, rostos, padrões, palavras-chave ou eventos potencialmente relevantes, permitindo que o especialista concentre sua atenção nas informações de maior interesse.

Ketsekioulafis et al. (2024), em revisão sistemática das aplicações de IA nas ciências forenses, identificaram aplicações desde identificação humana até estimativas relacionadas à medicina legal. O estudo enfatiza que a IA deve auxiliar o especialista e não substituí-lo. Essa conclusão é particularmente importante em investigação criminal, pois a existência de uma correlação algorítmica não equivale, por si só, à prova de autoria.

A revisão sistemática de Farber (2026) demonstra que a utilização de IA na polícia e na justiça criminal já abrange detecção de padrões criminais, policiamento preditivo, análise de redes criminosas e outras ferramentas. O crescimento dessas aplicações representa uma mudança de escala: a investigação passa a ser capaz de processar grandes volumes de informação de forma

automatizada, mas também passa a depender mais fortemente da qualidade dos dados e dos critérios de construção dos modelos.

A investigação criminal tradicional utiliza raciocínio indutivo, dedutivo e análise de evidências. A IA introduz uma camada computacional adicional. Em vez de substituir o raciocínio investigativo, pode funcionar como mecanismo de descoberta de padrões. O resultado ideal é uma relação complementar: a máquina realiza tarefas de processamento e classificação em escala, enquanto o profissional avalia contexto, pertinência, cadeia de custódia, coerência probatória e significado jurídico.

Essa complementaridade também reduz o risco de interpretar a IA como uma “testemunha digital”. Um algoritmo não possui compreensão jurídica do caso. Ele opera segundo dados, parâmetros e objetivos definidos por seres humanos. Consequentemente, qualquer resultado deve ser contextualizado e submetido a critérios de validação e revisão independente.

É importante distinguir inteligência artificial de simples automação. Uma rotina determinística executa regras previamente definidas, enquanto modelos de aprendizado de máquina podem identificar relações a partir de exemplos. Essa diferença afeta a forma como o sistema deve ser testado. Em uma automação tradicional, verifica-se se a regra foi implementada corretamente; em aprendizado de máquina, também é necessário avaliar se o conjunto de treinamento representa adequadamente o problema.

Na prática institucional, a escolha da tecnologia deve começar pela pergunta investigativa e não pela ferramenta disponível. A adoção de IA apenas porque determinada tecnologia é nova pode produzir processos complexos sem ganho real. O fluxo mais adequado identifica primeiro o gargalo — por exemplo, triagem de vídeos ou classificação documental — e então avalia se um modelo automatizado apresenta desempenho suficiente para aquele problema.

4 IDENTIFICAÇÃO HUMANA, BIOMETRIA E RECONHECIMENTO FACIAL

A identificação humana constitui uma das áreas mais promissoras para o uso de IA em investigação criminal. Sistemas de visão computacional podem extrair características de imagens e compará-las com bancos de dados, permitindo acelerar processos de triagem e geração de candidatos. A identificação pode envolver face, impressões digitais, características antropométricas e outras modalidades biométricas.

No reconhecimento facial, modelos de aprendizado profundo transformam imagens em representações matemáticas que podem ser comparadas com outras imagens. Em investigações, essa capacidade pode ser aplicada a imagens obtidas de câmeras de segurança, fotografias e vídeos. Entretanto, a identificação algorítmica deve ser diferenciada da confirmação pericial. Um sistema pode apontar que determinada pessoa possui alta similaridade com uma imagem de referência, mas essa indicação não elimina a necessidade de análise do contexto, da qualidade da imagem e das condições de aquisição.

A revisão de Stiernströmer (2026) sobre reconhecimento facial em segurança pública mostra que o tema vem recebendo crescente atenção empírica. A tecnologia apresenta potencial para identificação e investigação, mas envolve desafios relacionados a desempenho, condições de uso e impactos sobre direitos individuais. A literatura jurídica também destaca que dados biométricos possuem natureza especialmente sensível e que a utilização de reconhecimento facial por autoridades deve estar apoiada em bases legais, salvaguardas e critérios de proporcionalidade.

Outro problema é a dependência da qualidade dos dados. Iluminação, ângulo facial, resolução, oclusões, envelhecimento e diferenças entre equipamentos podem alterar o desempenho. Um modelo treinado em determinado contexto pode não apresentar a mesma performance em outro. Por isso, métricas de acurácia obtidas em bancos controlados não devem ser automaticamente generalizadas para situações reais.

Na identificação por impressões digitais, técnicas de aprendizado profundo vêm sendo utilizadas para aprimorar etapas de detecção e comparação de impressões latentes. A revisão de Peng e Huang (2026) aponta avanços do deep learning na inteligência e eficiência do reconhecimento de impressões digitais, ressaltando a crescente capacidade de adaptação dos modelos. Na prática forense, entretanto, o ganho de velocidade precisa ser acompanhado de controle de qualidade e interpretação especializada.

A revisão de Bugelli et al. (2026) sobre identificação pessoal também mostra que a IA vem sendo aplicada a diferentes modalidades de identificação, incluindo imagens e estimativas antropológicas. O cenário indica uma tendência de integração de múltiplos indicadores, na qual sistemas computacionais podem atuar como ferramentas de triagem e classificação.

O principal benefício investigativo é a capacidade de reduzir o universo de candidatos e localizar rapidamente possíveis correspondências. O principal risco é a falsa confiança no

resultado automatizado. Quanto maior a consequência da decisão, maior deve ser o nível de validação e supervisão humana. Em investigação criminal, um resultado de IA deve ser considerado uma informação a ser investigada, e não uma conclusão automática de autoria.

Outro aspecto relevante é a diferença entre identificação e verificação. Na verificação, o sistema testa se duas representações correspondem à mesma pessoa. Na identificação, uma imagem pode ser comparada contra uma grande base para produzir uma lista de candidatos. O aumento do tamanho da base pode elevar a quantidade de candidatos falsamente semelhantes, tornando necessária uma etapa posterior de confirmação.

Em ambientes reais, a qualidade da imagem é um dos fatores determinantes. Uma fotografia obtida em movimento, com baixa iluminação ou com o rosto parcialmente oculto pode produzir resultados diferentes daqueles observados em imagens controladas. Por essa razão, o profissional deve registrar as condições de aquisição e evitar interpretar uma correspondência algorítmica isoladamente.

5 ANÁLISE DE IMAGENS E VÍDEOS

A expansão das câmeras de segurança, dispositivos móveis e plataformas digitais transformou imagens e vídeos em fontes frequentes de evidência. A análise manual de horas de gravações é uma atividade intensiva em tempo. Técnicas de visão computacional podem auxiliar na localização de pessoas, veículos, objetos, movimentos e eventos específicos.

Redes neurais convolucionais e modelos de visão podem realizar detecção e classificação de objetos, rastreamento de indivíduos e análise de características visuais. Em contexto forense, essas ferramentas podem auxiliar o investigador a localizar rapidamente trechos relevantes de uma gravação, organizar grandes acervos e comparar padrões.

A análise de vídeo também apresenta desafios particulares. Uma câmera pode produzir imagens de baixa resolução, com compressão, ruído, iluminação inadequada ou movimento. A IA pode melhorar a triagem, mas não necessariamente recuperar informação que não está presente no arquivo original. Técnicas de aprimoramento de imagem devem ser utilizadas com cautela para evitar a criação de detalhes inexistentes.

Outro desafio contemporâneo é a manipulação de imagens por inteligência artificial generativa. A mesma tecnologia capaz de analisar evidências pode produzir conteúdos sintéticos

convincentes. Isso aumenta a necessidade de métodos de autenticação, análise de metadados, verificação de origem e avaliação de integridade.

A literatura recente em análise forense de imagens e vídeos aponta que o deep learning ocupa papel crescente, mas que transparência e validação continuam sendo desafios. Em investigação criminal, a autenticidade da mídia é tão importante quanto sua capacidade de apontar uma pessoa ou evento. Uma imagem manipulada pode gerar uma hipótese investigativa equivocada e contaminar etapas posteriores.

Por isso, o fluxo ideal combina ferramentas automatizadas com preservação do arquivo original, documentação de processamento, registro das versões e análise por profissional habilitado. A IA deve facilitar a localização e comparação de evidências, sem apagar a distinção entre dado original, dado processado e interpretação.

6 INTELIGÊNCIA ARTIFICIAL NA PERÍCIA DIGITAL

A perícia digital enfrenta um problema de escala particularmente intenso. Computadores, smartphones, servidores, veículos conectados, serviços em nuvem e dispositivos de Internet das Coisas podem armazenar enormes quantidades de informação. A extração desses dados não significa que todos sejam relevantes para a investigação.

Modelos de aprendizado de máquina podem auxiliar na classificação de arquivos, agrupamento de documentos, identificação de padrões, detecção de anomalias e priorização de informações. A revisão de Nayerifard et al. (2023) destaca que o crescimento do volume de evidências digitais impulsiona o uso de aprendizado de máquina em diferentes domínios da perícia digital, com destaque para análise de imagens e métodos baseados em redes neurais convolucionais.

A utilização de IA pode reduzir o tempo necessário para examinar grandes conjuntos de dados. Em uma investigação envolvendo milhares de documentos, por exemplo, sistemas de classificação podem identificar grupos temáticos ou conteúdos potencialmente relevantes. Em dispositivos com grande volume de imagens, modelos de visão podem auxiliar na triagem inicial.

Entretanto, a automação precisa respeitar a preservação da evidência. O sistema deve permitir rastrear quais dados foram analisados, qual modelo foi utilizado, quais parâmetros foram

empregados e como os resultados foram produzidos. A ausência dessa documentação dificulta a reprodução do procedimento e a avaliação posterior.

A explicabilidade também é relevante. Um modelo pode apresentar alta capacidade preditiva sem fornecer uma justificativa facilmente compreensível. Em contexto criminal, a possibilidade de questionar o método e compreender suas limitações é fundamental para a confiabilidade da prova.

Outro ponto é a segurança. Ferramentas de IA aplicadas à perícia digital podem ser alvos de manipulação ou ataques adversariais. Dados de entrada alterados de forma intencional podem influenciar classificações. Portanto, além da precisão, sistemas forenses precisam considerar robustez e segurança.

A utilização adequada da IA na perícia digital tende a ocorrer como uma camada de priorização: o algoritmo reduz a quantidade de material que precisa ser examinado inicialmente, enquanto o perito mantém responsabilidade pela interpretação e documentação do achado. Isso pode gerar ganhos de produtividade sem transformar o algoritmo em decisor final.

Em investigações com dispositivos móveis, o problema de escala pode ser ainda maior devido à multiplicidade de aplicativos, formatos e serviços em nuvem. Modelos de IA podem auxiliar a localizar conteúdos semanticamente relacionados, mas o investigador precisa distinguir a ausência de evidência de falha de recuperação. Um arquivo não encontrado pelo algoritmo não significa necessariamente que nunca tenha existido.

A preservação do contexto também é importante. Um documento ou mensagem isolada pode apresentar significado diferente quando relacionada a outras comunicações. Sistemas de processamento de linguagem podem agrupar conteúdos, mas a interpretação contextual exige leitura humana e conhecimento do caso.

7 GENÉTICA FORENSE E ANÁLISE DE DNA

A genética forense é uma área em que a complexidade dos dados favorece a aplicação de métodos computacionais. Perfis de DNA podem envolver múltiplos indivíduos, diferentes níveis de contribuição e sinais analíticos que exigem interpretação estatística sofisticada.

Barash e McNevin (2024) apresentam uma revisão crítica das aplicações de aprendizado de máquina na análise de DNA forense. Os autores destacam possibilidades relacionadas à

genotipagem, interpretação de misturas e análise de dados produzidos por tecnologias de sequenciamento. O potencial da IA decorre de sua capacidade de trabalhar com estruturas complexas e grandes volumes de dados.

Em misturas de DNA, por exemplo, a interpretação pode exigir avaliação simultânea de múltiplas hipóteses. Modelos computacionais podem auxiliar na classificação e na avaliação de padrões, mas a validação é indispensável. Um sistema desenvolvido em laboratório específico pode apresentar desempenho diferente quando aplicado a amostras, equipamentos ou populações diferentes.

A questão da reprodutibilidade é especialmente importante. Métodos de IA precisam ser testados em conjuntos de dados independentes, preferencialmente representativos das condições de utilização. Também é necessário estabelecer critérios claros para controle de qualidade, taxa de erro e situações em que o sistema não deve produzir uma conclusão.

A IA pode ainda contribuir para a identificação de características fenotípicas e ancestralidade a partir de dados genéticos. Essas aplicações, porém, possuem implicações éticas adicionais, pois inferências probabilísticas sobre características individuais podem ser interpretadas de forma inadequada. O resultado deve ser apresentado com incerteza e limites claramente definidos.

No contexto investigativo, a principal contribuição da IA na genética forense é aumentar a capacidade de processamento e interpretação, sobretudo quando os dados são complexos. A tecnologia não modifica os princípios fundamentais da genética forense: a evidência deve ser preservada, o método deve ser validado e a conclusão deve ser expressa dentro das limitações estatísticas.

8 INTELIGÊNCIA ARTIFICIAL NA TOXICOLOGIA FORENSE

A toxicologia forense envolve identificação e interpretação de substâncias químicas, medicamentos, drogas e metabólitos em matrizes biológicas. A crescente variedade de substâncias psicoativas e a complexidade dos dados analíticos aumentam a necessidade de ferramentas capazes de processar informações em escala.

Revisões recentes mostram aplicações de aprendizado de máquina em bioanálise, metabolômica, toxicodinâmica e triagem de substâncias desconhecidas. Grafinger et al. (2026)

destacam que a qualidade dos modelos depende fortemente da disponibilidade de conjuntos de dados adequados e da integração entre conhecimento químico, bioquímico, farmacológico e computacional.

Uma aplicação relevante envolve dados produzidos por espectrometria de massas de alta resolução. Esses instrumentos geram grande quantidade de informação que pode ser difícil de interpretar manualmente. Modelos de aprendizado de máquina podem auxiliar na classificação de espectros, identificação de padrões e priorização de hipóteses.

Swan et al. (2026) discutem especificamente o uso de IA e aprendizado de máquina na análise de dados de espectrometria de massas de alta resolução para triagem de substâncias desconhecidas. A literatura aponta potencial para tornar os fluxos de trabalho mais eficientes, mas ressalta problemas como dados limitados, uso de múltiplas substâncias e necessidade de validação.

A toxicologia forense demonstra, de forma clara, que a IA não substitui o conhecimento especializado. Um modelo pode indicar uma provável substância, mas a confirmação analítica e a interpretação toxicológica dependem de procedimentos laboratoriais e conhecimento científico. A integração adequada é, portanto, híbrida: algoritmos auxiliam na triagem e interpretação, enquanto métodos analíticos e especialistas sustentam a conclusão.

No âmbito criminal, essa capacidade pode acelerar investigações relacionadas a intoxicações, mortes suspeitas, uso de novas substâncias e exposição a agentes químicos. Entretanto, resultados automatizados devem ser tratados como parte de uma cadeia probatória maior, evitando que uma classificação algorítmica seja confundida com confirmação definitiva.

9 MEDICINA LEGAL E ESTIMATIVA DO INTERVALO POST MORTEM

A medicina legal também vem incorporando IA em tarefas relacionadas à análise de imagens, estimativas antropológicas, reconhecimento de padrões e avaliação do intervalo post mortem. A complexidade biológica da decomposição torna essa área particularmente adequada para modelos que consigam combinar múltiplas variáveis.

Bugelli et al. (2026) realizaram uma revisão sistemática sobre IA aplicada à identificação pessoal, enquanto outro estudo dos mesmos autores analisou a estimativa de intervalo post mortem a longo prazo. A revisão publicada em 2026 identificou dezenas de estudos envolvendo

microbioma, metabolômica, proteômica e imagens, indicando uma tendência de utilização de modelos multimodais.

A estimativa do intervalo post mortem é um problema complexo porque depende de temperatura, ambiente, condições corporais, microbiota, estágio de decomposição e outros fatores. Modelos de aprendizado de máquina podem identificar relações que não são facilmente observáveis por métodos lineares, mas precisam ser validados em diferentes ambientes.

O benefício potencial é a combinação de múltiplos indicadores em um único modelo. A limitação é que um modelo pode funcionar bem em um conjunto de dados específico e apresentar desempenho menor quando transportado para outra região ou condição ambiental.

Para a investigação de mortes suspeitas, uma estimativa mais refinada do intervalo post mortem pode contribuir para confrontar álbis, reconstruir cronologias e orientar a busca por informações. Contudo, a estimativa continua sendo probabilística. A IA deve apresentar intervalos de incerteza e não uma falsa precisão.

Essa área ilustra uma regra geral: quanto maior a complexidade do fenômeno biológico, maior a necessidade de validação externa e transparência sobre a incerteza. A utilidade da IA está em apoiar o raciocínio pericial, e não em eliminar a natureza probabilística da ciência forense.

10 ANÁLISE CRIMINAL E POLICIAMENTO PREDITIVO

Além das ciências forenses, a IA pode ser utilizada para analisar registros criminais e identificar padrões espaço-temporais. O chamado policiamento preditivo busca estimar locais, períodos ou condições associados à ocorrência de determinados crimes.

A revisão de Berk (2021) demonstra que parte dessas aplicações pode ser compreendida como estatística espacial ou modelos preditivos aplicados a dados criminais. O autor ressalta que existem preocupações relevantes quanto à precisão, ao viés e à transparência.

Uma questão central é que os dados policiais não representam necessariamente a ocorrência real de todos os crimes. Eles refletem também onde a polícia esteve, quais ocorrências foram registradas e quais grupos foram mais frequentemente abordados. Se um algoritmo aprende a partir desses registros, pode reproduzir padrões históricos de policiamento em vez de refletir exclusivamente padrões de criminalidade.

A revisão sistemática de Farber (2026) reforça que IA aplicada à polícia e justiça criminal oferece possibilidades de eficiência e alocação de recursos, mas também apresenta desafios de viés algorítmico, opacidade e devido processo. Portanto, uma previsão deve ser entendida como uma ferramenta de planejamento e não como prova de que uma pessoa cometerá um crime.

Na investigação criminal, a análise de redes também pode auxiliar na identificação de relações entre indivíduos, eventos e organizações. Grafos e modelos computacionais permitem visualizar conexões que seriam difíceis de detectar em grandes bancos de dados. Porém, uma relação estatística não necessariamente significa relação criminosa. A interpretação contextual permanece essencial.

O uso responsável dessas ferramentas exige transparência sobre as variáveis utilizadas, auditoria de desempenho, análise de impactos distributivos e mecanismos de contestação. O objetivo deve ser apoiar o trabalho policial e investigativo, evitando transformar probabilidades em decisões automáticas sobre indivíduos.

11 BENEFÍCIOS DA INTELIGÊNCIA ARTIFICIAL NA INVESTIGAÇÃO CRIMINAL

A literatura analisada permite identificar benefícios recorrentes. O primeiro é a velocidade. Algoritmos podem examinar milhares ou milhões de registros em tempo inferior ao necessário para uma análise manual.

O segundo benefício é a capacidade de reconhecer padrões. Sistemas de aprendizado de máquina conseguem trabalhar com relações complexas entre variáveis, permitindo identificar agrupamentos, anomalias e similaridades.

O terceiro é a escalabilidade. Uma equipe pequena pode utilizar ferramentas automatizadas para realizar uma primeira triagem de grandes acervos, concentrando o trabalho especializado nos itens mais relevantes.

O quarto é a padronização de tarefas repetitivas. Em atividades como classificação inicial de imagens, organização documental ou triagem de dados, algoritmos podem reduzir variações relacionadas à fadiga e ao volume de trabalho.

O quinto benefício é a integração de fontes. Modelos computacionais podem relacionar informações de diferentes bases, desde que a integração seja juridicamente autorizada e tecnicamente controlada.

O sexto é o apoio à tomada de decisão. A IA pode apresentar probabilidades, classificações ou prioridades para auxiliar o profissional. Essa função é especialmente útil quando existe excesso de informação e recursos humanos limitados.

Apesar dessas vantagens, o benefício não deve ser medido apenas pela acurácia do algoritmo. Em contexto forense, uma ferramenta precisa ser adequada ao propósito, reproduzível, validada e integrada a um fluxo de trabalho que preserve a cadeia de custódia. Um modelo muito preciso em laboratório pode ser pouco útil se não for robusto diante de dados reais.

Assim, a principal vantagem da IA não é “substituir o investigador”, mas ampliar sua capacidade de processar informação. A tecnologia aumenta o alcance cognitivo e operacional da equipe, desde que permaneça subordinada a critérios científicos e jurídicos.

Do ponto de vista organizacional, a IA pode reduzir o tempo gasto em tarefas de baixo valor interpretativo. Isso pode liberar profissionais para atividades que exigem conhecimento especializado, como reconstrução de eventos, entrevistas, interpretação de laudos e integração de diferentes fontes de evidência. O ganho institucional, portanto, não deve ser medido somente pela velocidade do algoritmo, mas pelo tempo total economizado no fluxo de trabalho.

Há ainda potencial para melhoria da consistência em tarefas repetitivas. Entretanto, consistência não significa necessariamente correção. Um algoritmo pode produzir o mesmo erro de maneira sistemática. Por isso, indicadores de desempenho precisam ser acompanhados por avaliações de erro e revisão independente.

12 LIMITAÇÕES, ERROS E VIESES ALGORÍTMICOS

O principal risco da IA em investigação criminal é a transformação de uma ferramenta probabilística em uma autoridade aparentemente objetiva. A existência de um resultado numérico pode criar uma sensação de precisão maior do que aquela efetivamente sustentada pelos dados.

Um algoritmo aprende a partir de dados. Se esses dados forem incompletos, enviesados ou pouco representativos, o modelo poderá reproduzir essas características. Em reconhecimento facial, por exemplo, diferenças na qualidade das imagens e na composição do banco podem alterar o desempenho.

Outro problema é o overfitting, quando o modelo aprende excessivamente as características do conjunto de treinamento e apresenta desempenho inferior em dados novos. A validação externa é, portanto, essencial.

A literatura recente sobre ciências forenses também chama atenção para a escassez de datasets grandes e representativos. Na toxicologia, por exemplo, a disponibilidade limitada de dados reais e a heterogeneidade analítica podem dificultar a generalização dos modelos (Grafinger et al., 2026).

A explicabilidade constitui outro desafio. Alguns modelos complexos funcionam como “caixas-pretas”, dificultando a compreensão das razões que levaram a determinada classificação. Em uma investigação, essa limitação pode ser relevante quando o resultado precisa ser questionado ou apresentado em ambiente judicial.

Também existe o risco de automação excessiva. Se o profissional confiar cegamente no sistema, pode deixar de considerar informações contraditórias. A supervisão humana funciona, portanto, como uma barreira de segurança.

A literatura indica ainda a necessidade de auditorias periódicas. O desempenho de um modelo pode mudar conforme mudam as câmeras, equipamentos, padrões criminais, características populacionais e tipos de dados. Uma validação realizada uma única vez não garante desempenho permanente.

Por isso, a adoção de IA deve incluir métricas de erro, documentação, testes independentes, atualização controlada e procedimentos para situações em que o sistema não possua confiança suficiente para produzir uma classificação.

Uma preocupação adicional é a mudança de distribuição dos dados. Um modelo treinado em determinada população, período ou equipamento pode encontrar condições diferentes quando implantado. Esse fenômeno, conhecido como mudança de distribuição, pode reduzir o desempenho sem que o sistema apresente um erro evidente. Monitoramento contínuo é, portanto, necessário.

A literatura contemporânea também chama atenção para a necessidade de calibrar probabilidades. Um modelo pode classificar corretamente muitos casos e, ainda assim, apresentar

probabilidades mal calibradas. Em contexto forense, essa diferença é relevante porque a interpretação de um resultado depende da confiabilidade da medida de incerteza.

13 ASPECTOS ÉTICOS, JURÍDICOS E DE PROTEÇÃO DE DADOS

A utilização de IA na investigação criminal possui implicações que ultrapassam a esfera técnica. Sistemas que processam biometria, localização, comunicações ou dados pessoais podem afetar privacidade, liberdade, igualdade e devido processo.

O reconhecimento facial é um exemplo evidente. A tecnologia cria uma forma de análise biométrica capaz de vincular imagens a identidades. A literatura jurídica destaca que essa utilização exige base legal adequada, proporcionalidade, transparência e salvaguardas específicas. A simples existência de uma tecnologia capaz de identificar pessoas não significa que sua utilização seja automaticamente legítima.

No Brasil, a discussão deve considerar, entre outros elementos, os princípios de proteção de dados pessoais, as regras processuais aplicáveis à obtenção e utilização de provas e as garantias constitucionais. A tecnologia deve ser incorporada ao procedimento investigativo sem afastar direitos fundamentais.

A questão da explicabilidade também possui dimensão jurídica. Se um resultado algorítmico contribuir para uma decisão relevante, a possibilidade de avaliar sua confiabilidade e seus limites é importante para o contraditório e para a revisão do procedimento.

Outro aspecto é a responsabilidade. Quando um algoritmo produz um resultado incorreto, deve existir clareza sobre quem definiu o sistema, quem autorizou seu uso, quem interpretou o resultado e quem tomou a decisão. A responsabilidade não pode ser transferida para uma ferramenta.

A governança de IA deve incluir políticas de acesso, registro de uso, segurança da informação, controle de versões e auditoria. Dados utilizados para treinamento também precisam ser tratados de maneira compatível com as regras de proteção e finalidade.

O princípio orientador deve ser a proporcionalidade: quanto maior o potencial de interferência em direitos fundamentais, maior deve ser o nível de controle, transparência e justificativa. O avanço tecnológico não elimina a necessidade de garantias jurídicas; ao contrário, torna essa necessidade mais evidente.

14 VALIDAÇÃO, RASTREABILIDADE E PAPEL DO PERITO

A adoção de inteligência artificial em investigação criminal exige mudança não apenas tecnológica, mas também organizacional. Antes de uma ferramenta ser utilizada em casos reais, é necessário demonstrar que ela funciona para a finalidade pretendida.

A validação deve incluir testes com dados representativos, comparação com métodos de referência, avaliação de taxas de falso positivo e falso negativo e análise de desempenho em diferentes condições. Quando possível, devem ser utilizados conjuntos de validação independentes.

A rastreabilidade é igualmente importante. O fluxo deve permitir identificar a versão do software, modelo utilizado, parâmetros relevantes, dados de entrada e resultado produzido. Alterações posteriores precisam ser documentadas.

Em perícia criminal, o profissional deve compreender não apenas o funcionamento operacional da ferramenta, mas também seus limites. Capacitação em ciência de dados, estatística básica e avaliação crítica de algoritmos pode tornar-se cada vez mais relevante.

A literatura sobre IA nas ciências forenses converge para a ideia de colaboração interdisciplinar. Especialistas em computação conhecem os modelos, enquanto peritos conhecem a natureza da evidência, os procedimentos laboratoriais e os requisitos probatórios. A integração desses conhecimentos aumenta a segurança da aplicação.

O perito permanece responsável pela interpretação técnica. A IA pode auxiliar na identificação de padrões, mas não deve ser tratada como fonte autônoma de verdade. A conclusão pericial deve considerar o conjunto de evidências, a qualidade dos dados e a incerteza do método.

Esse modelo de “humano no circuito” é particularmente importante quando o resultado pode influenciar decisões que afetam liberdade, imputação de responsabilidade ou reconhecimento de identidade. A automação deve aumentar a capacidade do profissional sem eliminar sua responsabilidade técnica.

15 PERSPECTIVAS FUTURAS

As tendências identificadas na literatura apontam para sistemas cada vez mais multimodais. Em vez de analisar isoladamente uma fotografia, um perfil genético ou um documento, modelos futuros poderão combinar diferentes tipos de evidência.

A IA generativa também deverá modificar a investigação criminal. Sistemas de linguagem podem auxiliar na organização documental, resumo de autos, pesquisa em grandes acervos e extração de entidades. Contudo, o risco de geração de informações incorretas exige mecanismos de verificação e uso controlado.

Na perícia, espera-se maior integração entre visão computacional, genética, química analítica e análise digital. A tendência é de aumento da automação das etapas de triagem, enquanto decisões conclusivas permanecem sob supervisão especializada.

Outra perspectiva é a criação de bancos de dados forenses mais estruturados e interoperáveis. Quanto melhor a qualidade dos dados, maior o potencial de modelos de IA. Porém, a interoperabilidade deve ser acompanhada de governança e segurança.

A validação externa provavelmente será um dos principais temas da próxima fase de desenvolvimento. A literatura atual apresenta muitos modelos experimentais, mas sua transposição para o trabalho operacional exige demonstração de desempenho em condições reais.

Também deverá crescer a preocupação com segurança contra ataques adversariais e manipulação de dados. Sistemas utilizados em investigações podem se tornar alvos estratégicos, o que exige proteção cibernética.

No futuro, a competência profissional poderá incluir capacidade de interpretar resultados algorítmicos, reconhecer limitações e questionar métricas de desempenho. O investigador e o perito não precisarão necessariamente programar os modelos, mas deverão compreender o suficiente para utilizá-los criticamente.

Portanto, o futuro da IA na investigação criminal tende a ser menos marcado pela substituição humana e mais pela cooperação entre inteligência humana e computacional.

16 DISCUSSÃO

A incorporação do estudo nacional *A atuação da polícia científica na elucidação do crime* (ALVES et al., 2026) fortalece a discussão por estabelecer uma ponte entre a base tradicional da perícia criminal e as novas tecnologias analisadas nesta revisão. O trabalho destaca que genética forense, toxicologia, informática forense e inteligência pericial ampliam a capacidade de produção de prova, ao mesmo tempo em que dependem de infraestrutura, capacitação, preservação de vestígios e padronização metodológica. Essa base é particularmente relevante

para a inteligência artificial: modelos computacionais só podem produzir resultados confiáveis quando os dados de entrada são adequadamente coletados, preservados, documentados e interpretados por profissionais habilitados.

A literatura analisada demonstra que a inteligência artificial já deixou de ser apenas uma possibilidade teórica no campo da investigação criminal. No contexto brasileiro, essa discussão se articula com a atuação da Polícia Científica na produção e interpretação de vestígios, destacada por Alves et al. (2026) como componente essencial da investigação criminal e da confiabilidade da prova material. Aplicações concretas aparecem em identificação humana, reconhecimento facial, análise de impressões digitais, perícia digital, DNA, toxicologia, medicina legal, análise de imagens e policiamento orientado por dados.

Entretanto, os diferentes campos apresentam níveis distintos de maturidade. Algumas aplicações possuem histórico maior de pesquisa e validação, enquanto outras ainda estão em estágio experimental. Essa diferença impede uma avaliação única da “IA na investigação criminal”. Cada aplicação deve ser analisada segundo seu objetivo, tipo de dado, população de interesse, consequências do erro e nível de validação.

A principal convergência da literatura é que a IA pode ampliar a eficiência sem necessariamente substituir o especialista. Essa visão aparece de forma explícita em revisões de ciências forenses e é coerente com as necessidades de interpretação contextual da investigação.

Também existe convergência quanto aos riscos. Viés, transparência, qualidade dos dados e validação aparecem repetidamente. Isso sugere que os desafios atuais não são apenas tecnológicos. Mesmo um modelo matematicamente sofisticado pode ser inadequado quando utilizado fora das condições para as quais foi desenvolvido.

No âmbito da investigação criminal, um princípio importante é separar “indício produzido por algoritmo” de “prova científica”. O primeiro pode orientar a investigação; o segundo precisa atender aos requisitos científicos e processuais aplicáveis. Essa distinção reduz o risco de automatização indevida.

A IA pode ainda alterar a organização do trabalho pericial. Atividades repetitivas tendem a ser automatizadas, enquanto tarefas de interpretação, validação e integração de evidências

ganham importância. Isso não significa redução da relevância do perito, mas mudança no perfil das competências necessárias.

Outro ponto é a necessidade de protocolos institucionais. Órgãos de segurança e perícia que adotarem IA precisarão estabelecer regras sobre aquisição, validação, atualização, auditoria e uso dos resultados. A ausência de governança pode transformar uma ferramenta potencialmente útil em fonte de risco.

Assim, a questão central não é decidir entre “usar” ou “não usar” inteligência artificial. O desafio é definir em quais situações seu uso é cientificamente justificável, juridicamente permitido e operacionalmente seguro.

17 CONSIDERAÇÕES FINAIS

A inteligência artificial apresenta potencial significativo para transformar a investigação criminal ao ampliar a capacidade de análise de grandes volumes de dados, acelerar a identificação de padrões e apoiar atividades periciais. As evidências científicas analisadas indicam aplicações relevantes em identificação humana, reconhecimento facial, impressões digitais, análise de imagens e vídeos, perícia digital, genética forense, toxicologia, medicina legal e análise criminal.

Os benefícios mais consistentes estão relacionados à velocidade, escalabilidade e capacidade de triagem. A IA pode permitir que investigadores e peritos encontrem informações relevantes em conjuntos de dados que seriam excessivamente extensos para análise exclusivamente manual.

Entretanto, a literatura também demonstra que a adoção da tecnologia não é isenta de riscos. Modelos dependem da qualidade dos dados, podem reproduzir vieses, podem apresentar desempenho inferior fora do ambiente de treinamento e nem sempre são facilmente explicáveis. Em áreas sensíveis, como reconhecimento facial e análise criminal preditiva, os impactos sobre direitos fundamentais tornam indispensáveis mecanismos de governança e controle.

No âmbito forense, a IA deve ser utilizada como instrumento de apoio ao especialista. A conclusão deve continuar fundamentada em métodos validados, evidências preservadas, interpretação técnica e análise crítica. O resultado de um algoritmo não deve ser confundido com uma determinação automática de autoria, identidade ou culpabilidade.

Conclui-se que a utilização responsável da inteligência artificial na investigação criminal depende de cinco pilares: qualidade dos dados; validação científica; transparência e rastreabilidade; supervisão humana qualificada; e conformidade ética e jurídica. A tecnologia tende a desempenhar papel cada vez mais relevante, mas sua efetividade dependerá menos da promessa de automação total e mais da capacidade institucional de integrá-la de maneira crítica, segura e cientificamente fundamentada.

Como agenda futura, recomenda-se o desenvolvimento de estudos brasileiros que avaliem ferramentas de IA em condições reais da perícia criminal, considerando características dos bancos de dados nacionais, diferenças regionais, infraestrutura disponível e requisitos do processo penal. Também são necessários protocolos de validação, auditorias independentes e capacitação continuada dos profissionais que utilizarão essas ferramentas.

REFERÊNCIAS

ALVES, Mayara; NASCIMENTO, Rildo José do; LINDOLFO, João Batista; LELES, Marcos Silva. A atuação da polícia científica na elucidação do crime. *Revista FT*, v. 30, n. 158, 2026, p. 01-15. DOI: 10.69849/d7a0kn61.

BARASH, Mark; MCNEVIN, Dennis. Machine learning applications in forensic DNA profiling: A critical review. *Forensic Science International: Genetics*, v. 69, 102994, 2024. DOI: 10.1016/j.fsigen.2023.102994.

BERK, Richard A. Artificial intelligence, predictive policing, and risk assessment for law enforcement. *Annual Review of Criminology*, v. 4, p. 209–237, 2021. DOI: 10.1146/annurev-criminol-051520-012342.

BUGELLI, Valentina et al. Artificial intelligence in forensic science: a systematic review. Part I: personal identification. *International Journal of Legal Medicine*, v. 140, p. 3317–3329, 2026. DOI: 10.1007/s00414-026-03855-5.

BUGELLI, Valentina et al. Artificial intelligence in forensic science: a systematic review. Part II: long-range postmortem interval estimation. *International Journal of Legal Medicine*, v. 140, p. 3331–3343, 2026. DOI: 10.1007/s00414-026-03856-4.

FARBER, Shai. Machines of justice: A systematic review of AI applications in policing and criminal justice. *International Journal of Law, Crime and Justice*, 2026. DOI: 10.1177/0032258X261439572.

GRAFINGER, Katharina Elisabeth et al. Machine learning in forensic toxicology: Concepts, applications and challenges in bioanalysis, ADME, and toxicodynamics. *Forensic Science International*, v. 383, 112883, 2026. DOI: 10.1016/j.forsciint.2026.112883.

KETSEKIOULAFIS, Ioannis et al. Artificial Intelligence in Forensic Sciences: A Systematic Review of Past and Current Applications and Future Perspectives. *Cureus*, v. 16, n. 9, e70363, 2024. DOI: 10.7759/cureus.70363.

NAYERIFARD, Tahereh et al. Machine Learning in Digital Forensics: A Systematic Literature Review. 2023. DOI/Preprint record: arXiv:2306.04965.

PENG, An; HUANG, Rui. Research progress on the application of deep learning in fingerprint recognition. *Pattern Recognition*, v. 171, 112216, 2026. DOI: 10.1016/j.patcog.2025.112216.

STIERNSTRÖMER, Emelie. Facial recognition technology in law enforcement: a scoping review of existing empirical studies. *Journal of Crime and Justice*, 2026. DOI: 10.1080/15614263.2026.2627208.

SWAN, Samantha et al. Applications of machine learning for the general unknown screening of HRMS data within forensic toxicology. *Journal of Analytical Toxicology*, v. 50, n. 3, bkaf109, 2026. DOI: 10.1093/jat/bkaf109.

TAGELDIN, Laila; VENTER, Hein. Machine-Learning Forensics: State of the Art in the Use of Machine-Learning Techniques for Digital Forensic Investigations within Smart Environments. *Applied Sciences*, v. 13, n. 18, 10169, 2023.

TOURNOIS, Laurent et al. Artificial intelligence in the practice of forensic medicine: a scoping review. *International Journal of Legal Medicine*, v. 138, p. 1023–1037, 2024. DOI: 10.1007/s00414-023-03140-9.