

Inteligência artificial na investigação criminal: limites éticos e jurídicos do reconhecimento facial e dos sistemas preditivos

Artificial intelligence in criminal investigation: ethical and legal limits of facial recognition and predictive systems

João Augusto Castro Scatena¹

Diego Fernandes Beserra de Brito²

RESUMO

O uso de sistemas de inteligência artificial na segurança pública e na investigação criminal tem ampliado as possibilidades de processamento de dados, identificação de pessoas e elaboração de inferências destinadas a orientar a atuação estatal. Ao mesmo tempo, a utilização de tecnologias de reconhecimento facial e de sistemas preditivos suscita questionamentos quanto à sua compatibilidade com as garantias fundamentais que limitam o exercício do poder punitivo. O presente artigo analisa os limites éticos e jurídicos do emprego dessas tecnologias no contexto da persecução penal, com especial atenção aos riscos decorrentes de falsos positivos, opacidade algorítmica, tratamento de dados pessoais e reprodução de vieses e desigualdades presentes nos dados utilizados pelos sistemas. Examina-se, ainda, a repercussão dessas práticas sobre os direitos à privacidade e à proteção de dados, à igualdade e à não discriminação, à presunção de inocência e ao devido processo legal. A partir de pesquisa bibliográfica e documental, busca-se discutir em que medida a utilização da inteligência artificial pode ser admitida como instrumento auxiliar da atividade investigativa e quais salvaguardas jurídicas se mostram necessárias para assegurar transparência, auditabilidade, supervisão humana e possibilidade de contestação dos resultados algorítmicos.

Palavras-chave: Inteligência artificial. Investigação criminal. Reconhecimento facial. Policiamento preditivo. Direitos fundamentais.

¹ Bacharelando do 9º período em Direito pela Faculdade Integrada de Paranaíba, MS (FIPAR). E-mail: joaoaugustocastroscatena@gmail.com

² Mestrando em Direito pela Faculdade do Sul de Minas - FDSM. Pós-graduado em Educação em Direitos Humanos pela Universidade Federal do Estado de Mato Grosso do Sul - UFMS. Pós-graduado em Direito Processual Civil, Processual Penal e Processual Trabalhista pelas Faculdades Integradas de Paranaíba – FIPAR. Bacharel em Direito pela Universidade Estadual do Estado do Mato Grosso do Sul - UEMS. Advogado atuante com experiência em Direito Civil, Direito do Trabalho, Direito Previdenciário e Direito Penal em Paranaíba/Mato Grosso do Sul. Professor Universitário desde 2020 nas Faculdades Integradas de Paranaíba – FIPAR. Docente contratado pela Universidade Estadual do Mato Grosso do Sul - UEMS desde 2023. dfernandes.beserra@gmail.com

ABSTRACT

The use of artificial intelligence systems in public security and criminal investigations has expanded the possibilities for data processing, identification of individuals, and the generation of inferences intended to guide state action. At the same time, the use of facial recognition technologies and predictive systems raises questions regarding their compatibility with the fundamental guarantees that limit the exercise of punitive power. This article analyzes the ethical and legal limits of the use of such technologies within criminal prosecution, with particular attention to the risks arising from false positives, algorithmic opacity, personal data processing, and the reproduction of biases and inequalities embedded in the data used by these systems. It also examines the impact of these practices on the rights to privacy and data protection, equality and non-discrimination, the presumption of innocence, and due process of law. Based on bibliographic and documentary research, the study seeks to discuss the extent to which artificial intelligence may be admitted as an auxiliary tool in investigative activities and which legal safeguards are necessary to ensure transparency, auditability, human oversight, and the possibility of challenging algorithmic outputs.

Keywords: Artificial intelligence. Criminal investigation. Facial recognition. Predictive policing. Fundamental rights.

1 INTRODUÇÃO

O uso de inteligência artificial na segurança pública e na investigação criminal ampliou a capacidade de processamento de dados, identificação de padrões e produção de inferências destinadas a orientar a atuação estatal. Entre as aplicações mais relevantes para este estudo estão o reconhecimento facial, empregado na comparação automatizada de imagens, e os sistemas preditivos, que utilizam dados anteriormente registrados para indicar padrões, áreas ou situações de interesse policial. Essas ferramentas podem auxiliar a atividade investigativa, mas também alteram a forma pela qual informações são selecionadas e convertidas em elementos capazes de direcionar a atenção dos órgãos de persecução (VIEIRA; SANTOS, 2025, p. 7-8).

A análise dessas tecnologias não pode se restringir aos possíveis ganhos de eficiência. O reconhecimento facial possui caráter probabilístico e está sujeito a identificações equivocadas, enquanto sistemas preditivos dependem da qualidade e da origem dos dados utilizados. Bases produzidas em contextos marcados por práticas policiais enviesadas podem transportar tais distorções para as inferências subsequentes, e a própria atuação orientada pelo algoritmo pode influenciar os registros que alimentarão previsões futuras (RAPOSO, 2024, p. 1857-1858; RICHARDSON; SCHULTZ; CRAWFORD, 2019, p. 15-16; ENSIGN et al., 2018, p. 1-2).

Esses riscos assumem especial relevância quando resultados algorítmicos deixam de desempenhar função meramente administrativa e passam a influenciar a identificação de pessoas, a seleção de alvos, a formação de suspeitas ou a adoção de medidas que repercutam sobre direitos fundamentais. Nesse cenário, a sofisticação tecnológica não elimina os limites jurídicos incidentes sobre a persecução penal, sobretudo aqueles relacionados à privacidade e à proteção de dados, à igualdade e à não discriminação, à presunção de inocência e ao devido processo legal.

A tensão é ampliada pelo fato de que a informação algorítmica pode produzir efeitos antes mesmo da formação de uma prova em sentido estrito. Uma correspondência facial pode conduzir o investigador a determinada pessoa; um mapa de risco pode modificar a distribuição do patrulhamento; e um score pode influenciar a prioridade conferida a um indivíduo ou grupo. Oliveira e Bedê Jr. observam que a circulação de alertas, scores e mapas de risco entre instituições pode conferir aparência de confiabilidade às inferências automatizadas e dificultar sua contestação, com reflexos sobre devido processo, igualdade, privacidade e presunção de inocência (OLIVEIRA; BEDÊ JR., 2026, p. 4-9).

Por isso, a discussão não deve ser apresentada como escolha entre aceitação irrestrita da inovação e rejeição absoluta da inteligência artificial. O ponto central é determinar em quais condições a tecnologia pode auxiliar a atuação estatal sem converter probabilidades, correlações estatísticas ou resultados opacos em razões autônomas para vigilância, suspeição ou restrição de direitos. Essa perspectiva orienta a hipótese e permite avaliar a tecnologia a partir da função que efetivamente desempenha no percurso investigativo.

Diante disso, o problema de pesquisa consiste em verificar em que medida o uso de sistemas de inteligência artificial, especialmente de reconhecimento facial e de análise preditiva, na segurança pública e na investigação criminal brasileira é compatível com esses direitos fundamentais. Adota-se como hipótese que a inteligência artificial não é, por si só, incompatível com a atividade investigativa, mas sua legitimidade depende de limites que impeçam a transformação de resultados algorítmicos, sem controle crítico e confirmação por outros elementos, em fundamentos autônomos de suspeição, identificação ou restrição de direitos.

O objetivo geral é analisar os limites éticos e jurídicos aplicáveis ao emprego dessas tecnologias. Para tanto, o artigo delimita suas principais formas de utilização; examina os riscos de falsos positivos, vieses e ciclos de retroalimentação; relaciona esses problemas às garantias constitucionais; e discute parâmetros jurídicos destinados a assegurar que a

inteligência artificial permaneça instrumento auxiliar da investigação, submetido a controle humano, transparência, auditabilidade e possibilidade de contestação (LAWAND, 2026, p. 192-193).

A pesquisa é bibliográfica e documental, reunindo doutrina processual penal e de proteção de dados, estudos acadêmicos nacionais e estrangeiros, pesquisas técnicas sobre reconhecimento facial e policiamento preditivo e marcos normativos relacionados ao tema. A estrutura do trabalho acompanha esse percurso: inicialmente são apresentados os conceitos necessários; em seguida, os riscos da atuação algorítmica; depois, os direitos fundamentais afetados; e, por fim, o cenário regulatório e as salvaguardas para uma utilização juridicamente legítima.

2 INTELIGÊNCIA ARTIFICIAL APLICADA À SEGURANÇA PÚBLICA E À INVESTIGAÇÃO CRIMINAL

A inteligência artificial aplicada à segurança pública não corresponde a uma tecnologia única. Diferentes sistemas podem processar informações para identificar pessoas, estabelecer relações entre dados ou produzir classificações e previsões. Para delimitar o objeto deste artigo, interessa compreender como essas funcionalidades se relacionam com a atividade investigativa e, especialmente, distinguir o reconhecimento facial dos sistemas preditivos.

2.1 Inteligência artificial, big data e atividade investigativa

Para os fins deste estudo, é suficiente adotar uma concepção operacional de inteligência artificial. Lawand a relaciona a sistemas capazes de desempenhar tarefas que, quando realizadas por seres humanos, demandariam capacidades como reconhecimento de padrões, aprendizado e tomada de decisão. No campo criminal, ganham relevância os sistemas baseados em aprendizado de máquina, que identificam correlações a partir do processamento de dados (LAWAND, 2026, p. 193).

A expansão dessas aplicações está ligada à disponibilidade de grandes conjuntos de informações digitais. Vieira e Santos observam que o fenômeno do big data permite o processamento de volumes de dados que excedem as capacidades das ferramentas convencionais, favorecendo novas formas de análise no campo da segurança pública (VIEIRA; SANTOS, 2025, p. 6). Técnicas de mineração de dados podem, nesse contexto, localizar padrões, correlações e anomalias e cruzar registros provenientes de diferentes fontes (LAWAND, 2026, p. 193-194).

A mudança não consiste apenas em acelerar consultas anteriormente realizadas de forma manual. A agregação de bases e o processamento automatizado permitem selecionar relações e produzir inferências que não haviam sido previamente formuladas pelo investigador. É nesse ambiente que se inserem o reconhecimento facial e os sistemas preditivos, ambos dependentes de dados e processamento algorítmico, mas voltados a finalidades diferentes.

Nesse contexto, o algoritmo funciona como uma sequência de instruções destinada à realização de determinada tarefa, mas, nos sistemas de inteligência artificial, interessa especialmente sua capacidade de processar informações e produzir classificações, previsões ou outros resultados a partir dos dados fornecidos. Assim, falar em IA na atividade policial não significa tratar de um único programa, mas de diferentes soluções computacionais que podem desempenhar funções igualmente diversas (LAWAND, 2026, p. 193).

A relevância do big data também não decorre apenas do volume de informações. O ponto decisivo está na possibilidade de estabelecer relações entre registros que, observados isoladamente, poderiam não revelar determinado padrão. Essa capacidade altera a posição da informação na investigação: bancos de dados deixam de servir somente à consulta de elementos já procurados e passam a ser utilizados para descobrir conexões e selecionar informações consideradas relevantes para novas linhas de apuração.

2.2 Reconhecimento facial

O reconhecimento facial é utilizado para identificar ou verificar a identidade de indivíduos por meio da análise computacional de imagens da face. A tecnologia detecta características faciais, converte-as em uma representação matemática ou modelo biométrico e realiza comparações com outras representações (RAPOSO, 2024, p. 1857-1858). As National Academies descrevem processo semelhante, no qual o sistema extrai características e atribui graus de similaridade às imagens analisadas (NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, 2024, p. 1).

A comparação pode ocorrer na modalidade de um para um, destinada a verificar se a imagem corresponde à identidade declarada, ou de um para muitos, em que uma imagem é pesquisada em uma base contendo diversas referências para localizar possíveis correspondências. Esta segunda modalidade possui especial interesse para a investigação criminal, pois pode gerar candidatos e linhas investigativas a partir de imagens disponíveis (NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, 2024, p. 1-2).

O resultado de uma busca desse tipo decorre de cálculo de similaridade e não deve ser tratado, apenas por sua origem tecnológica, como confirmação automática de identidade. A própria estrutura do sistema pressupõe limiares de decisão e admite falsos positivos e falsos negativos. Essa característica é decisiva para a análise jurídica posterior, pois o significado atribuído à correspondência depende da confiabilidade do sistema e da forma como o resultado será utilizado.

É necessário distinguir o reconhecimento facial de outras formas de análise automatizada de imagens. As National Academies observam que sistemas destinados a estimar características de uma pessoa a partir de uma única imagem não se confundem tecnicamente com o reconhecimento facial, que pressupõe comparação entre representações para verificação ou identificação (NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, 2024, p. 20). Essa delimitação evita atribuir à tecnologia funções distintas sob uma mesma denominação.

No contexto policial, a modalidade um para muitos é particularmente sensível porque a imagem pesquisada pode provir de câmeras de segurança e ser comparada com bases extensas. O sistema retorna candidatos de acordo com níveis de similaridade, de modo que o resultado depende não apenas do algoritmo, mas também da qualidade da imagem de entrada, da composição da base pesquisada e do limiar adotado para selecionar correspondências.

2.3 Sistemas preditivos de criminalidade

Os sistemas preditivos seguem lógica distinta: utilizam dados anteriores para identificar regularidades e produzir inferências sobre situações futuras. No policiamento preditivo, algoritmos e métodos estatísticos podem processar registros policiais e outras informações para orientar estratégias e a distribuição de recursos. Vieira e Santos descrevem esse emprego como análise de dados pretéritos destinada a extrair tendências capazes de influenciar práticas de policiamento (VIEIRA; SANTOS, 2025, p. 7-8).

Essas aplicações podem ser orientadas ao lugar, indicando áreas ou períodos considerados mais associados a determinados eventos, ou concentrar-se em pessoas, vínculos ou características relacionadas a uma estimativa de risco. Em ambos os casos existe uma etapa de processamento que ultrapassa a simples consulta a um banco de dados e produz uma classificação ou previsão destinada a influenciar uma atuação posterior.

Ensign et al. observam que determinados modelos utilizam dados históricos de criminalidade para definir onde os recursos policiais serão empregados e incorporam novamente ao sistema informações obtidas durante o patrulhamento (ENSIGN et al., 2018, p.

1). Por isso, o presente estudo considera não apenas a investigação criminal já instaurada, mas também aplicações de segurança pública capazes de interferir na formação de suspeitas ou no direcionamento da atividade investigativa.

A utilização de técnicas estatísticas para orientar a segurança pública é anterior à expansão contemporânea da inteligência artificial. O elemento novo está sobretudo na capacidade de processar volumes muito maiores de informações, na velocidade das análises e na automatização da identificação de padrões (VIEIRA; SANTOS, 2025, p. 6-8). Essa diferença de escala ajuda a compreender por que os efeitos desses sistemas podem ultrapassar o simples apoio administrativo e alcançar a maneira como a atividade estatal seleciona locais e pessoas para maior atenção.

3 OS RISCOS DA ATUAÇÃO ALGORÍTMICA NA PERSECUÇÃO PENAL

A atuação algorítmica introduz uma etapa de inferência entre os dados coletados e a decisão estatal que deles poderá decorrer. Seus riscos podem estar no desempenho técnico do sistema, na qualidade das bases utilizadas ou na forma como os resultados são incorporados às práticas institucionais. Para o recorte adotado, três problemas são centrais: falsos positivos no reconhecimento facial, vieses e discriminação algorítmica e ciclos de retroalimentação no policiamento preditivo.

3.1 Falsos positivos e falibilidade do reconhecimento facial

No reconhecimento facial, falso negativo ocorre quando o sistema deixa de estabelecer uma associação que deveria ocorrer, enquanto falso positivo corresponde à associação equivocada entre pessoas diferentes (GROTHER; NGAN; HANAOKA, 2019, p. 1-2). Para a investigação criminal, o falso positivo é particularmente sensível porque pode inserir indevidamente uma pessoa no campo de atenção dos órgãos de persecução.

O estudo do NIST analisou 189 algoritmos de 99 desenvolvedores, mediante o processamento de 18,27 milhões de imagens correspondentes a 8,49 milhões de indivíduos. Os resultados evidenciaram grande variação de desempenho entre os algoritmos. Também foram identificadas diferenças demográficas nas taxas de falsos positivos que, em muitos casos, variaram entre grupos por fatores de dez a mais de cem vezes. O relatório ressalva, contudo, que a magnitude e a direção dessas diferenças dependem do algoritmo e do conjunto de imagens, havendo sistemas de elevada acurácia nos quais determinadas diferenças não foram detectadas (GROTHER; NGAN; HANAOKA, 2019, p. 1-3).

A avaliação de confiabilidade, portanto, não comporta generalizações. O desempenho depende do sistema utilizado, dos dados operacionais e das condições das imagens. As National Academies destacam que capturas controladas tendem a favorecer a acurácia, ao passo que imagens de vigilância, obtidas sem posicionamento e iluminação adequados, podem apresentar qualidade inferior. O relatório também observa que a revisão humana dos candidatos retornados pelo sistema pode introduzir erros adicionais (NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, 2024, p. 1; 49-50).

As consequências tornam-se juridicamente relevantes quando uma correspondência equivocada orienta atos policiais. As National Academies registram seis casos de grande repercussão nos Estados Unidos em que o reconhecimento facial esteve relacionado a prisões posteriormente consideradas equivocadas, todos envolvendo pessoas negras, mas advertem que não existem dados abrangentes que permitam calcular a prevalência do fenômeno (NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, 2024, p. 3; 83-84). Assim, os casos demonstram a possibilidade de dano, sem autorizar a construção de uma taxa geral de prisões indevidas.

A questão central não é apenas saber se o sistema erra, mas qual valor será atribuído à correspondência. Quanto mais grave a consequência decorrente do resultado, maior deve ser a cautela para que uma indicação probabilística não seja convertida em identificação incontroversa.

Os resultados do NIST recomendam cautela com conclusões generalizantes em sentidos opostos. Não é correto pressupor que todos os sistemas apresentem a mesma taxa de erro ou o mesmo padrão de diferença demográfica; ao mesmo tempo, não se pode considerar a origem tecnológica da comparação como garantia de desempenho uniforme. O próprio relatório recomenda que o responsável conheça especificamente o algoritmo utilizado e meça sua acurácia sobre os dados operacionais pertinentes à aplicação concreta (GROTHER; NGAN; HANAOKA, 2019, p. 3).

Raposo também ressalta que as identificações equivocadas decorrem de um conjunto de fatores, entre os quais o caráter probabilístico da tecnologia, a qualidade das imagens, a composição dos dados e a forma de utilização do sistema. Isso reforça a necessidade de analisar o reconhecimento facial como processo sociotécnico, no qual o resultado algorítmico é apenas uma etapa e pode ser ampliado ou corrigido pelas práticas institucionais posteriores (RAPOSO, 2024, p. 1857-1858; 1864-1865).

3.2 Viés e discriminação algorítmica

A discriminação algorítmica não se limita às diferenças de acurácia. Um sistema pode produzir efeitos assimétricos porque os dados, critérios ou práticas que estruturam sua utilização refletem desigualdades anteriores. Os resultados do NIST demonstram que uma medida global de desempenho pode ocultar diferenças entre grupos e reforçam a necessidade de avaliar o algoritmo no contexto específico em que será empregado (GROTHER; NGAN; HANAOKA, 2019, p. 2-3).

No policiamento preditivo, o problema aparece sobretudo na origem dos dados. Brayne observa que bases apresentadas como objetivas permanecem produtos sociais, formados nos contextos em que são coletadas (BRAYNE, 2021, p. 52). Richardson, Schultz e Crawford denominam *dirty data* os registros incorretos, incompletos ou produzidos sob influência de práticas policiais corruptas, ilegais ou discriminatórias. Quando utilizados para alimentar modelos preditivos, esses dados podem transportar as distorções do processo que os produziu para novas inferências (RICHARDSON; SCHULTZ; CRAWFORD, 2019, p. 18-20).

A pesquisa desses autores examinou treze jurisdições norte-americanas nas quais havia sobreposição entre a adoção de ferramentas preditivas e constatações oficiais de práticas policiais problemáticas. Em nove delas, dados produzidos durante esses períodos estavam disponíveis para treinar ou informar sistemas preditivos. O estudo não afirma que toda previsão resultante tenha sido discriminatória, mas identifica risco de reprodução dos problemas incorporados às bases (RICHARDSON; SCHULTZ; CRAWFORD, 2019, p. 20-21).

A distinção entre dados sobre criminalidade e dados sobre atuação policial é, portanto, essencial. Registros de abordagens, prisões e ocorrências documentam também escolhas institucionais sobre onde e sobre quem a atividade estatal se concentrou. No contexto brasileiro, Coimbra, Moraes e Silva relacionam a adoção acrítica de tecnologias pretensamente neutras à possibilidade de reprodução de desigualdades raciais já presentes na estrutura social e na segurança pública (COIMBRA; MORAES; SILVA, 2023, p. 136-138; 150-151).

O problema não exige que o sistema utilize expressamente uma categoria sensível. Informações aparentemente neutras podem guardar correlação com desigualdades anteriormente existentes. Quando essas classificações são apresentadas como *outputs* técnicos, podem ainda adquirir aparência adicional de objetividade, fenômeno associado por

Oliveira e Bedê Jr. a uma presunção de confiabilidade dos resultados algorítmicos (OLIVEIRA; BEDÊ JR., 2026, p. 13-14).

Os próprios dados policiais não constituem uma representação integral de todos os crimes praticados em determinada sociedade. Eles refletem também prioridades institucionais, locais em que houve maior presença estatal, condutas mais fiscalizadas e fatos que chegaram ao conhecimento das autoridades. Richardson, Schultz e Crawford ressaltam que essas bases incorporam práticas, políticas e vieses institucionais, razão pela qual tratá-las como retrato neutro da criminalidade pode ocultar a maneira pela qual foram produzidas (RICHARDSON; SCHULTZ; CRAWFORD, 2019, p. 22-23).

Esse aspecto é particularmente importante quando variáveis aparentemente neutras funcionam como substitutas de características sensíveis. Localização territorial, histórico de abordagens ou registros anteriores podem guardar relação com desigualdades sociais e raciais sem que o modelo utilize diretamente uma categoria protegida. A discriminação algorítmica deve, portanto, ser examinada a partir dos efeitos das classificações e não apenas da intenção do desenvolvedor ou da presença explícita de determinada variável.

A automatização pode ainda deslocar a percepção do viés. Uma seleção produzida diretamente por um agente é reconhecida como decisão humana e, em princípio, pode ser questionada como tal. Quando a mesma seleção aparece na forma de score, alerta ou mapa de risco, o resultado tende a adquirir uma aparência adicional de objetividade. A crítica jurídica deve impedir que a linguagem quantitativa transforme escolhas anteriores e limitações do modelo em conclusões aparentemente incontroversas.

3.3 Policiamento preditivo e ciclos de retroalimentação

Nos sistemas preditivos, a própria previsão pode alterar o ambiente do qual serão extraídos os dados futuros. Ensign et al. distinguem incidentes comunicados à polícia daqueles descobertos diretamente pelos agentes. Estes últimos dependem da presença policial no território e, quando são reutilizados para atualizar o modelo, podem produzir um ciclo em que maior patrulhamento gera mais registros, os registros reforçam a classificação de risco e a classificação justifica nova concentração policial (ENSIGN et al., 2018, p. 1-4).

A modelagem desenvolvida pelos autores demonstra a suscetibilidade de determinados sistemas a feedback loops capazes de reconduzir repetidamente recursos aos mesmos locais independentemente da taxa real de criminalidade. Richardson, Schultz e Crawford identificam risco semelhante quando estatísticas anteriores devolvem agentes às comunidades que já

concentram a atuação policial, fazendo com que padrões de policiamento passado influenciem decisões futuras (RICHARDSON; SCHULTZ; CRAWFORD, 2019, p. 19-20).

Quando esse mecanismo se combina a vieses históricos, a desigualdade pode deixar de ser apenas reproduzida e passar a ser continuamente reforçada. Oliveira e Bedê Jr. observam que a retroalimentação pode afetar onde a polícia atua, quem será abordado e quais ocorrências receberão prioridade, contribuindo para consolidar narrativas institucionais de risco e periculosidade (OLIVEIRA; BEDÊ JR., 2026, p. 14-15).

Isso não significa que todo sistema preditivo opere da mesma forma nem que registros policiais sejam, por definição, inutilizáveis. O ponto demonstrado pelas pesquisas é a necessidade de compreender como os dados foram produzidos e de avaliar se a intervenção orientada pelo sistema influencia a própria amostra que posteriormente servirá como confirmação da previsão.

Forma-se, assim, um problema epistemológico relevante: o sistema pode utilizar como confirmação de sua previsão um resultado que foi parcialmente produzido pela decisão anterior. Quanto maior o policiamento em determinada área, maior a possibilidade de detecção de fatos; quanto mais registros são produzidos, maior pode se tornar a classificação de risco; e essa classificação, por sua vez, pode justificar nova concentração de recursos. A correlação estatística adquire, então, potencial autorreferente.

O reconhecimento desse risco não autoriza concluir que todo modelo preditivo necessariamente produzirá retroalimentação. Ensign et al. analisam objeto específico e demonstram a suscetibilidade de determinados sistemas ao problema. A consequência metodológica é mais restrita: dados produzidos pela própria atividade orientada pelo algoritmo precisam ser avaliados com cautela para que a intervenção estatal não seja confundida com evidência independente da previsão que a desencadeou.

4 DIREITOS FUNDAMENTAIS E LIMITES CONSTITUCIONAIS AO USO DA INTELIGÊNCIA ARTIFICIAL

Os riscos descritos tornam-se problemas constitucionais quando resultados algorítmicos passam a influenciar a identificação de pessoas, a seleção de alvos, a formação de suspeitas ou decisões com efeitos concretos. A utilização da inteligência artificial integra o exercício do poder estatal e, por isso, permanece submetida às garantias que limitam a persecução penal. O controle jurídico deve alcançar não apenas a decisão final, mas também a

forma como dados e inferências foram produzidos e incorporados ao percurso investigativo (OLIVEIRA; BEDÊ JR., 2026, p. 16).

4.1 Privacidade e proteção de dados

Reconhecimento facial e sistemas preditivos dependem de coleta, agregação e tratamento de informações. Bioni demonstra que a proteção de dados não se limita à ideia tradicional de segredo: em ambientes de processamento automatizado, informações isoladas podem ser combinadas para produzir perfis e inferências sobre o indivíduo, afetando sua liberdade e possibilitando práticas discriminatórias (BIONI, 2019, p. 118-119; 160-164).

No Brasil, a proteção de dados pessoais possui dimensão constitucional autônoma. Vieira e Santos recordam que, mesmo antes de sua inclusão expressa no catálogo constitucional, o Supremo Tribunal Federal já havia relacionado a autodeterminação informativa à liberdade, à privacidade e ao devido processo informacional (VIEIRA; SANTOS, 2025, p. 7). Essa proteção adquire especial relevância diante de dados biométricos, utilizados para individualizar pessoas de modo automatizado.

A utilização do reconhecimento facial em espaços públicos amplia a capacidade de transformar imagens dispersas em informação estruturada. As National Academies observam que a tecnologia pode operar sem percepção do indivíduo e que correspondências realizadas ao longo do tempo podem ser agregadas para reconstruir atividades e relações (NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, 2024, p. 2-3). Estar em espaço público, portanto, não elimina a necessidade de limites sobre finalidade, coleta, conservação, compartilhamento e reutilização dos dados.

A LGPD possui regime específico para tratamentos destinados à segurança pública e à investigação e repressão de infrações penais, remetendo a disciplina da matéria a legislação própria. Essa peculiaridade não afasta o direito fundamental à proteção de dados nem autoriza tratamento indiscriminado. Lawand sustenta que o emprego de IA na persecução permanece submetido à finalidade, necessidade e proporcionalidade da intervenção (VIEIRA; SANTOS, 2025, p. 25; LAWAND, 2026, p. 195-196).

Dados biométricos merecem cautela específica porque se vinculam de maneira permanente às características físicas utilizadas para identificar o indivíduo. No reconhecimento facial, a questão jurídica não está apenas na fotografia originalmente capturada, mas no tratamento automatizado que extrai e compara características capazes de individualizar a pessoa. A expansão de bases interoperáveis pode aumentar a capacidade de localização e perfilamento para além do contexto em que a imagem foi inicialmente obtida.

Existe, ainda, diferença qualitativa entre a simples possibilidade de ser visto em espaço público e a submissão contínua de características faciais a processamento automatizado. A tecnologia permite relacionar imagens dispersas e produzir informação estruturada sobre uma mesma pessoa em diferentes momentos. Por isso, a inexistência de anonimato absoluto em locais públicos não equivale a consentimento ou autorização geral para identificação biométrica permanente.

4.2 Igualdade e não discriminação

O princípio da igualdade exige que a análise dos sistemas não se restrinja à existência de comandos expressamente discriminatórios. Efeitos desiguais podem decorrer da composição das bases, dos critérios do modelo ou da utilização de variáveis aparentemente neutras que funcionem como substitutas de características sensíveis. Oliveira e Bedê Jr. destacam que impactos discriminatórios podem ocorrer mesmo sem intenção discriminatória, razão pela qual os efeitos concretos das classificações também devem ser examinados (OLIVEIRA; BEDÊ JR., 2026, p. 17-18).

No campo penal, a preocupação aumenta porque registros utilizados pelos sistemas podem refletir a seletividade da própria atuação estatal. Se determinados grupos ou territórios foram submetidos a vigilância mais intensa, os dados resultantes não são independentes desse histórico. A automação pode transformar padrões anteriores de fiscalização em classificações estatísticas apresentadas como objetivas.

A ausência de uma variável racial explícita, por exemplo, não elimina necessariamente efeitos racialmente assimétricos quando outras informações se relacionam com desigualdades existentes. O problema jurídico deve concentrar-se na origem dos dados, nos critérios de classificação e nos impactos da utilização do sistema, e não em atribuir à máquina uma intenção equivalente ao preconceito humano.

Quando uma classificação algorítmica influencia a intensidade da vigilância ou a formação de suspeitas, eventual desigualdade deixa de ser abstrata e passa a repercutir sobre a atuação estatal. Igualdade e não discriminação exigem, por isso, mecanismos capazes de identificar, testar e contestar esses impactos.

A aparente objetividade matemática não afasta a incidência do princípio da igualdade. Resultados numéricos dependem de decisões sobre quais dados serão coletados, quais variáveis serão consideradas, qual objetivo será perseguido e como a saída será utilizada. A automação modifica a forma da seleção, mas não elimina as escolhas humanas presentes na construção e na aplicação do sistema.

No âmbito da persecução penal, a preocupação é concreta: classificações podem influenciar quem receberá maior vigilância, quem será abordado e quais ocorrências serão consideradas prioritárias. Se os efeitos se distribuem de modo sistematicamente desigual, a ausência de intenção discriminatória não é suficiente para afastar o problema constitucional. A igualdade exige possibilidade de identificar e corrigir impactos desproporcionais.

4.3 Presunção de inocência e suspeição algorítmica

A presunção de inocência assume especial importância diante de ferramentas preditivas, que operam com probabilidades sobre eventos ou comportamentos não comprovados. Lopes Jr. identifica a garantia como norma de tratamento, norma probatória e norma de julgamento, com efeitos ao longo da persecução penal, e não apenas no momento da sentença (LOPES JR., 2022, p. 118-120).

Uma classificação de risco não demonstra que determinada pessoa praticou um crime. A probabilidade estatística de comportamento futuro possui natureza distinta da demonstração individualizada de um fato pretérito. Lawand observa que escores de risco podem deslocar a atenção da comprovação do fato para a previsão de uma possível periculosidade, enquanto Oliveira e Bedê Jr. assinalam o risco de outputs preditivos funcionarem como sinais antecipados de suspeição (LAWAND, 2026, p. 195; OLIVEIRA; BEDÊ JR., 2026, p. 19-20).

Nesse ponto surge o que se pode denominar suspeição algorítmica: a passagem de uma informação probabilística baseada em padrões coletivos para uma consequência concreta dirigida ao indivíduo. O problema não está em o investigador receber informação produzida por tecnologia, mas em permitir que ela substitua a individualização dos fundamentos exigidos para a atuação estatal.

A lógica preditiva torna-se especialmente problemática quando atributos coletivos passam a influenciar a avaliação individual. Residir ou circular em área estatisticamente classificada como de maior risco, manter relações com pessoas inseridas em determinado conjunto ou coincidir com um perfil não comprova participação em atividade criminosa. A passagem da análise agregada para uma intervenção concreta precisa encontrar fundamento próprio no caso individual.

Por isso, a presunção de inocência também impede uma inversão prática da lógica constitucional. O investigado não pode ser colocado na posição de provar que a classificação de risco ou a previsão a seu respeito estava errada. Compete ao Estado justificar suas intervenções mediante elementos juridicamente adequados, sem deslocar para o indivíduo o ônus de afastar uma suspeita criada por correlações algorítmicas.

4.4 Devido processo, transparência e auditabilidade

O devido processo e o contraditório exigem condições reais para conhecer e questionar elementos desfavoráveis. Badaró identifica informação e possibilidade de reação como componentes fundamentais do contraditório, enquanto Lopes Jr. ressalta a participação efetiva das partes na formação da decisão (BADARÓ, 2021, p. 84-85; LOPES JR., 2022, p. 121-122).

A opacidade algorítmica pode comprometer essa relação quando a defesa recebe apenas a conclusão do sistema sem informações suficientes para compreender como ela foi produzida. Lawand sustenta que a impugnação técnica requer conhecimento sobre metodologia, dados utilizados, taxas de erro e vieses identificados, de modo que a complexidade tecnológica não transforme o resultado em elemento imune ao contraditório (LAWAND, 2026, p. 195-197).

Transparência, rastreabilidade e auditabilidade cumprem funções complementares. Deve ser possível reconstruir o percurso relevante do resultado, identificar os dados e parâmetros utilizados e avaliar a confiabilidade do sistema no contexto concreto. A origem científica ou tecnológica da informação não autoriza presumir sua validade. Ao tratar da prova científica, Badaró destaca a importância de critérios como testabilidade, revisão, taxas de erro e aceitação do método, premissa que reforça a necessidade de escrutínio sobre resultados técnicos utilizados na persecução penal (BADARÓ, 2019, p. 192).

O controle deve alcançar também a utilização humana do output. A mera existência de um agente encarregado de confirmar a recomendação não garante supervisão efetiva se a validação for acrítica. A decisão que produz efeitos sobre direitos fundamentais precisa permanecer fundamentada e atribuível a responsáveis humanos capazes de compreender as limitações relevantes da ferramenta.

Assim, mesmo sistemas tecnicamente precisos podem gerar tensões constitucionais quando tratam dados de modo desproporcional, produzem impactos discriminatórios, convertem perfis de risco em critérios de suspeição ou impedem a contestação das inferências utilizadas. A questão seguinte consiste em transformar esses limites em regras concretas de governança e utilização.

A auditabilidade possui função distinta da simples confiança no fornecedor ou no órgão público que adquiriu a ferramenta. Deve permitir verificar se o sistema efetivamente opera conforme o funcionamento declarado, quais limitações são relevantes e se o desempenho observado é compatível com a finalidade investigativa. Não basta afirmar que a

tecnologia é eficiente em abstrato quando o resultado concreto não pode ser submetido a avaliação crítica.

A possibilidade de controle também não pode ser afastada automaticamente por sigilo comercial. Quando o Estado escolhe empregar sistema proprietário em atividade capaz de afetar direitos fundamentais, a contratação não deve produzir, como efeito, a criação de uma inferência inacessível à defesa. A proteção de interesses empresariais pode demandar soluções procedimentais específicas, mas não autoriza transformar a tecnologia em zona de imunidade ao contraditório.

Transparência não significa necessariamente divulgação irrestrita de código-fonte. O ponto é assegurar informação suficiente para reconstruir a trajetória relevante do resultado, conhecer os dados e parâmetros essenciais, as limitações conhecidas e o papel efetivamente desempenhado pela inferência na decisão estatal. A extensão dessa informação deve ser compatível com a consequência jurídica atribuída ao output.

5 PARÂMETROS JURÍDICOS PARA O USO DA INTELIGÊNCIA ARTIFICIAL NA INVESTIGAÇÃO CRIMINAL

A compatibilidade da inteligência artificial com a persecução penal depende de condições concretas de uso. O desafio regulatório é converter legalidade, necessidade, proporcionalidade, não discriminação, contraditório e presunção de inocência em exigências verificáveis, capazes de acompanhar o ciclo de utilização da tecnologia, desde a definição de sua finalidade e das bases de dados até a interpretação e o eventual emprego do resultado na investigação.

5.1 O cenário regulatório brasileiro

O quadro brasileiro permanece fragmentado. A Constituição fornece o núcleo de proteção dos direitos envolvidos, enquanto leis, atos administrativos e projetos legislativos disciplinam aspectos específicos. A LGPD, em seu art. 4º, III, afasta do regime geral os tratamentos realizados para fins exclusivos de segurança pública e investigação ou repressão de infrações penais, mas determina que essas operações sejam objeto de legislação específica, observados o devido processo legal, os princípios de proteção de dados e medidas proporcionais e estritamente necessárias ao interesse público (BRASIL, 2018).

A necessidade de disciplina setorial aparece no Projeto de Lei nº 1.515/2022, relativo à proteção de dados para essas finalidades. Em paralelo, o Projeto de Lei nº 2.338/2023 trata do marco geral de inteligência artificial e o Projeto de Lei nº 3.069/2022 aborda o

reconhecimento facial automatizado pelas forças de segurança pública. As propostas ainda integram o processo legislativo e, por isso, não substituem o regime jurídico vigente.

O Projeto de Lei nº 3.069/2022 expressa preocupação semelhante ao prever confirmação por agente público de indicações positivas produzidas por reconhecimento facial e ao afastar medidas policiais restritivas da liberdade baseadas apenas na indicação automatizada sem confirmação especializada. Embora se trate de proposta legislativa e não de norma vigente, o dispositivo evidencia a distinção entre a saída do sistema e o fundamento necessário à atuação estatal.

No plano administrativo, a Portaria MJSP nº 961/2025 estabelece diretrizes para soluções de tecnologia da informação aplicadas à investigação criminal e à inteligência de segurança pública em seu âmbito de incidência. O ato inclui sistemas de inteligência artificial e prevê respeito a direitos fundamentais, finalidade determinada, necessidade, proporcionalidade, proteção de dados, transparência, responsabilização, registros de acesso e revisão humana de inferências quando houver risco de lesão a direitos (BRASIL, 2025).

A Portaria também restringe a identificação biométrica à distância em tempo real em espaços acessíveis ao público a hipóteses determinadas. No reconhecimento facial, a Resolução CNDH nº 17/2025 acrescenta parâmetros de não discriminação, proporcionalidade, contestabilidade, avaliação de vieses e governança, além de estabelecer que a ferramenta não deve ser utilizada como prova única em decisões que afetem direitos fundamentais e deve permanecer sob revisão humana (CNDH, 2025).

Em 2026, a Portaria MJSP nº 1.122 instituiu o Protocolo Nacional de Reconhecimento de Pessoas em Procedimentos Criminais no âmbito da polícia judiciária e fez referência à Portaria nº 961/2025 e à Resolução CNJ nº 484/2022 (BRASIL, 2026). O conjunto dessas iniciativas evidencia avanços institucionais, mas não elimina a relevância de uma disciplina legislativa abrangente para tecnologias capazes de afetar direitos fundamentais na persecução penal.

5.2 A inteligência artificial como instrumento auxiliar da investigação

A primeira premissa para o uso legítimo da inteligência artificial é que o resultado algorítmico desempenhe função auxiliar e não substitua a formação juridicamente controlável da decisão humana. Lawand sustenta que essas ferramentas podem orientar a atividade investigativa desde que permaneçam submetidas a controle humano qualificado e a mecanismos de transparência e fiscalização (LAWAND, 2026, p. 200-201).

No reconhecimento facial, uma busca de um para muitos produz candidatos segundo níveis de similaridade. Por isso, a correspondência pode justificar verificações adicionais, mas não deve ser convertida automaticamente em identificação definitiva. A Resolução CNDH nº 17/2025 e a Portaria MJSP nº 961/2025 convergem ao exigir revisão humana e ao rejeitar o uso isolado da inferência quando houver repercussão sobre direitos fundamentais.

A supervisão humana deve ser substancial. A simples confirmação protocolar do output não resolve os problemas da automação se o responsável não possui condições de compreender suas limitações, questionar o resultado e, quando necessário, afastá-lo. A decisão que restringe direitos precisa manter fundamento próprio e responsabilidade humana identificável.

O mesmo vale para sistemas preditivos: previsões territoriais podem auxiliar o planejamento administrativo, mas a adoção de medidas contra uma pessoa exige elementos individualizados. Correlações estatísticas não criam, por sua mera existência, justa causa autônoma para buscas, prisões ou outras intervenções. Essa separação entre informação auxiliar e fundamento jurídico suficiente impede que o perfil estatístico substitua a suspeita concretamente fundamentada.

Como referência comparativa, o Regulamento (UE) 2024/1689 confere tratamento restritivo à identificação biométrica remota em tempo real para fins de aplicação da lei e impede que decisões com efeitos jurídicos adversos sejam tomadas exclusivamente com base no resultado do sistema. Embora não se aplique diretamente ao Brasil, o modelo reforça a ideia de que maior impacto sobre direitos exige menor autonomia do output algorítmico (UNIÃO EUROPEIA, 2024).

A distinção entre informação auxiliar e fundamento jurídico suficiente é especialmente importante para evitar a criação do “suspeito estatístico”. A ferramenta pode contribuir para indicar uma linha de investigação, mas medidas invasivas continuam sujeitas aos requisitos legais próprios. A existência de um score, de uma correspondência facial ou de uma previsão territorial não modifica, por si só, os pressupostos necessários para busca, prisão ou outras formas de restrição de direitos.

5.3 Salvaguardas, limites e hipóteses de restrição

A caracterização da IA como instrumento auxiliar precisa ser acompanhada de mecanismos de governança. A primeira exigência é a finalidade determinada: sistemas e bases não devem ser reutilizados indistintamente para novos propósitos sem avaliação jurídica.

Também são indispensáveis necessidade e proporcionalidade, de modo que a intensidade do tratamento e da vigilância corresponda ao objetivo legítimo perseguido.

A rastreabilidade deve permitir reconstruir a origem dos dados, os acessos, as versões das bases e dos modelos e as operações relevantes. Oliveira e Bedê Jr. relacionam esse controle à possibilidade de contestar as inferências e identificar responsabilidades. Registros de logs e auditorias, previstos pela Portaria nº 961/2025, são instrumentos concretos dessa exigência (OLIVEIRA; BEDÊ JR., 2026, p. 21).

A confiabilidade também precisa ser avaliada antes e durante a utilização. Alterações nas bases, no contexto operacional ou na população submetida ao sistema podem afetar seu desempenho. Por isso, testes de acurácia e de vieses, avaliações de impacto e monitoramento periódico são necessários, sobretudo em aplicações capazes de produzir consequências relevantes para indivíduos ou grupos.

Outro requisito é a contestabilidade. A pessoa atingida deve ter acesso suficiente às informações relevantes para compreender quais dados e premissas influenciaram o resultado e quais limitações são conhecidas. Sigilo comercial ou complexidade técnica não podem transformar uma tecnologia adquirida pelo Estado em fonte imune à fiscalização quando sua saída é utilizada na persecução penal (OLIVEIRA; BEDÊ JR., 2026, p. 22-23).

A supervisão humana qualificada deve ser acompanhada de responsabilidades institucionais claras. Falhas podem decorrer da base de dados, do modelo, da configuração, da contratação ou da interpretação do resultado, e a multiplicidade de participantes não pode produzir diluição de responsabilidade. Do mesmo modo, sistemas preditivos devem ser acompanhados quanto a possíveis ciclos de retroalimentação e à reutilização de registros produzidos pela própria atividade orientada pelo modelo.

Nem toda aplicação disponível pode ser legitimada apenas com transparência ou revisão humana. Sistemas cuja confiabilidade não seja demonstrável, que apresentem vieses relevantes não mitigados, impeçam auditoria necessária ou sejam utilizados de modo incompatível com necessidade e proporcionalidade podem justificar restrição ou suspensão. O reconhecimento biométrico remoto em tempo real e a vigilância generalizada são particularmente sensíveis pela amplitude de pessoas potencialmente alcançadas.

Como núcleo mínimo, o uso legítimo da inteligência artificial na persecução penal exige finalidade determinada, necessidade e proporcionalidade, qualidade dos dados, avaliação de impacto, testes de desempenho e vieses, rastreabilidade, transparência suficiente para controle, auditabilidade, contestabilidade, supervisão humana qualificada, limitação da

reutilização das informações e responsabilização institucional. A tecnologia pode indicar caminhos; a decisão estatal que afeta direitos deve permanecer individualizada, fundamentada e juridicamente controlável.

A avaliação de impacto deve considerar não apenas a acurácia média do sistema, mas também diferenças de desempenho entre grupos, qualidade das bases, finalidade do tratamento e consequências associadas a falsos positivos e falsos negativos. Testes periódicos são relevantes porque mudanças no banco de dados ou no contexto de operação podem alterar o comportamento observado da ferramenta.

A responsabilização institucional também exige identificar o papel de cada participante. O resultado pode ser afetado por escolhas do desenvolvedor, do fornecedor, do órgão contratante e do operador, além da qualidade dos dados utilizados. A multiplicidade de etapas não deve permitir que falhas relevantes sejam atribuídas abstratamente ao “algoritmo”, sem possibilidade de localizar decisões e responsabilidades humanas.

A intensidade das salvaguardas deve acompanhar a intensidade do risco. Aplicações meramente organizacionais não apresentam a mesma capacidade de interferência que tecnologias destinadas a identificar pessoas em espaços públicos ou a classificá-las segundo risco criminal. Quanto maior a possibilidade de repercussão sobre liberdade, privacidade, igualdade ou formação da suspeita, maior deve ser a exigência de legalidade, documentação, auditoria e supervisão.

6 CONSIDERAÇÕES FINAIS

O estudo procurou verificar em que medida o reconhecimento facial e os sistemas preditivos podem ser utilizados na segurança pública e na investigação criminal sem violar direitos fundamentais. A análise permite concluir que a inteligência artificial não é, em abstrato, incompatível com a persecução penal, mas sua legitimidade é condicionada à finalidade do uso, à confiabilidade da ferramenta, à intensidade de seus efeitos e à existência de mecanismos de controle.

No reconhecimento facial, a natureza probabilística das comparações, a possibilidade de falsos positivos e as diferenças de desempenho entre algoritmos e grupos impedem que uma correspondência seja tratada como confirmação automática de identidade. Nos sistemas preditivos, a dependência de dados históricos e a possibilidade de ciclos de retroalimentação demonstram que a automação não elimina os vieses presentes no processo de produção das informações.

Esses riscos repercutem diretamente sobre privacidade e proteção de dados, igualdade e não discriminação, presunção de inocência e devido processo. Correlações e classificações estatísticas não equivalem à demonstração individualizada de um fato e não devem converter o indivíduo em um “suspeito estatístico”. Da mesma forma, a complexidade tecnológica não pode tornar os outputs imunes ao contraditório ou impedir a avaliação de sua confiabilidade.

A hipótese formulada foi, portanto, confirmada: a inteligência artificial pode atuar como ferramenta auxiliar da investigação, desde que o resultado algorítmico não constitua fundamento autônomo para identificação definitiva ou restrição de direitos. A supervisão humana deve ser efetiva, permitindo compreender, questionar e afastar a recomendação quando necessário, e as decisões estatais devem conservar fundamento jurídico próprio e responsabilidade identificável.

Nesse sentido, finalidade determinada, necessidade, proporcionalidade, qualidade dos dados, testes de desempenho e vieses, avaliação de impacto, rastreabilidade, auditabilidade, contestabilidade e supervisão humana qualificada integram o conjunto de salvaguardas necessárias. Quando tais condições não possam ser satisfeitas ou os riscos não sejam adequadamente mitigados, a restrição ou suspensão da tecnologia constitui consequência compatível com a proteção constitucional.

A inovação tecnológica, portanto, não substitui os critérios jurídicos que legitimam o exercício do poder punitivo. A inteligência artificial pode ampliar a capacidade estatal de encontrar e organizar informações, mas não reduzir a exigência de justificá-las. Quanto maior o poder da tecnologia de interferir sobre direitos fundamentais, maior deve ser o grau de controle jurídico sobre sua utilização.

O cenário regulatório brasileiro revela avanços importantes por meio de atos administrativos e propostas legislativas, mas permanece fragmentado. A existência de diretrizes sobre revisão humana, rastreabilidade, finalidade, proporcionalidade e não discriminação demonstra que a questão já não pode ser tratada apenas como escolha técnica de gestão. Tecnologias capazes de interferir sobre direitos demandam regras claras sobre hipóteses de uso, responsabilidades e mecanismos de controle.

A conclusão central não é, portanto, a rejeição da inovação, mas sua subordinação às garantias que legitimam a própria investigação criminal. Eficiência não transforma correlação em prova, probabilidade em certeza ou classificação estatística em fundamento suficiente para intervenção. O algoritmo pode auxiliar a localizar informações e organizar prioridades; a

decisão estatal permanece submetida à legalidade, à individualização dos fundamentos, ao contraditório e à responsabilidade humana.

REFERÊNCIAS

BADARÓ, Gustavo Henrique. **Epistemologia judiciária e prova penal**. São Paulo: Thomson Reuters Brasil, 2019.

BADARÓ, Gustavo Henrique. **Processo penal**. 9. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2021.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 1.515, de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília, DF: Câmara dos Deputados, 2022a.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 3.069, de 2022**. Dispõe sobre o uso de tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública e dá outras providências. Brasília, DF: Câmara dos Deputados, 2022b.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988.

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.

BRASIL. Ministério da Justiça e Segurança Pública. **Portaria MJSP nº 961, de 24 de junho de 2025**. Estabelece diretrizes sobre uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública. Diário Oficial da União: seção 1, Brasília, DF, 30 jun. 2025, p. 104-105.

BRASIL. Ministério da Justiça e Segurança Pública. **Portaria MJSP nº 1.122, de 5 de janeiro de 2026**. Institui o Protocolo Nacional de Reconhecimento de Pessoas em Procedimentos Criminais no âmbito da polícia judiciária. Diário Oficial da União: seção 1, Brasília, DF, 6 jan. 2026, p. 189-193.

BRASIL. Senado Federal. **Projeto de Lei nº 2.338, de 2023**. Dispõe sobre o uso da Inteligência Artificial. Brasília, DF: Senado Federal, 2023.

BRAYNE, Sarah. **Predict and surveil: data, discretion, and the future of policing**. New York: Oxford University Press, 2021.

COIMBRA, Jéssica Pérola Melo; MORAES, Liliane Correia; SILVA, Adrian Barbosa e. Interseções entre racismo algorítmico, reconhecimento facial e segurança pública no Brasil. **Revista Jurídica do CESUPA**, v. 4, n. 2, p. 136-160, 2023.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução nº 484, de 19 de dezembro de 2022**. Estabelece diretrizes para a realização do reconhecimento de pessoas em procedimentos e processos criminais e sua avaliação no âmbito do Poder Judiciário. DJe/CNJ, n. 317/2022, 21 dez. 2022, p. 4-6.

CONSELHO NACIONAL DOS DIREITOS HUMANOS. **Resolução nº 17, de 10 de novembro de 2025**. Dispõe sobre o uso de tecnologias de reconhecimento facial em espaços públicos dos estados e do Distrito Federal. Brasília, DF: CNDH, 2025.

ENSIGN, Danielle; FRIEDLER, Sorelle A.; NEVILLE, Scott; SCHEIDEGGER, Carlos; VENKATASUBRAMANIAN, Suresh. Runaway feedback loops in predictive policing. **Proceedings of Machine Learning Research**, v. 81, p. 1-12, 2018.

GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. **Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects**. Gaithersburg, MD: National Institute of Standards and Technology, 2019. NISTIR 8280. Disponível em: <https://doi.org/10.6028/NIST.IR.8280>. Acesso em: 28 jul. 2026.

LANGUAGETOOL. **LanguageTool**. [Software de revisão linguística on-line]. [S. l.]: LanguageTool, [2026]. (Utilizado exclusivamente como ferramenta auxiliar de correção ortográfica, gramatical e de estilo, sem emprego como fonte bibliográfica ou de conteúdo.) Disponível em: <https://languagetool.org/pt-BR>. Acesso em: 28 jul. 2026.

LAWAND, Jorge José. Inteligência artificial e proteção de dados na investigação criminal: limites constitucionais ao combate ao crime organizado. **Revista CNJ**, v. 10, n. 1, p. 191-208, jan./jun. 2026.

LOPES JR., Aury. **Direito processual penal**. 19. ed. São Paulo: SaraivaJur, 2022.

NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE. **Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance**. Washington, DC: The National Academies Press, 2024. Disponível em: <https://doi.org/10.17226/27397>. Acesso em: 28 jul. 2026.

OLIVEIRA, Luciano R.; BEDÊ JR., Américo. Confiança e opacidade: governança de sistemas integrados e IA preditiva no ciclo polícia, MP e Judiciário. **Revista Brasileira de Direito Processual Penal**, v. 12, n. 2, e1400, mai./ago. 2026. Disponível em: <https://doi.org/10.22197/rbdpp.v12i2.1400>. Acesso em: 28 jul. 2026.

OPENAI. **ChatGPT: GPT-5.6 Sol**. [Modelo de linguagem de inteligência artificial generativa]. [S. l.]: OpenAI, 2026. (Utilizado como ferramenta auxiliar de organização e estruturação textual e apoio à sistematização dos materiais previamente selecionados pelo autor, sem utilização como fonte doutrinária, jurisprudencial ou documental.) Disponível em: <https://chatgpt.com/>. Acesso em: 28 jul. 2026.

RAPOSO, Vera Lúcia. When facial recognition does not ‘recognise’: erroneous identifications and resulting liabilities. **AI & Society**, v. 39, p. 1857-1869, 2024. Disponível em: <https://doi.org/10.1007/s00146-023-01634-z>. Acesso em: 28 jul. 2026.

RICHARDSON, Rashida; SCHULTZ, Jason M.; CRAWFORD, Kate. Dirty data, bad predictions: how civil rights violations impact police data, predictive policing systems, and justice. **New York University Law Review Online**, v. 94, p. 15-55, 2019.

UNIÃO EUROPEIA. **Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024**. Regulamento da Inteligência Artificial (AI Act). Jornal Oficial da União Europeia, 12 jul. 2024.

VIEIRA, Andrey Bruno Cavalcante; SANTOS, Hugo Leonardo Rodrigues. Investigação criminal e tecnologias digitais: algumas reflexões sobre o policiamento preditivo e a admissibilidade de provas digitais. **Revista Brasileira de Direito Processual Penal**, v. 11, n. 1, e1072, jan./abr. 2025. Disponível em: <https://doi.org/10.22197/rbdpp.v11i1.1072>. Acesso em: 28 jul. 2026