FACULDADE SANTA LUZIA - FSL
CURSO DE BACHARELADO EM DIREITO

A INTELIGÊNCIA ARTIFICIAL NO RECONHECIMENTO FACIAL APLICADO À INVESTIGAÇÃO CRIMINAL E SEUS IMPACTOS NA ADMISSIBILIDADE DA PROVA NO PROCESSO PENAL BRASILEIRO

ORIENTANDO(A): JOÃO VICTOR FONSECA SANTOS
ORIENTADOR(A): PROF. ESP. LUÍS CLAUDIO DOS SANTOS RIBEIRO

SANTA INÊS - MA
2025

JOÃO VICTOR FONSECA SANTOS

A INTELIGÊNCIA ARTIFICIAL NO RECONHECIMENTO FACIAL APLICADO À INVESTIGAÇÃO CRIMINAL E SEUS IMPACTOS NA ADMISSIBILIDADE DA PROVA NO PROCESSO PENAL BRASILEIRO

Trabalho de conclusão de curso de graduação da Faculdade Santa Luzia-FLS como pré-requisito para obtenção do grau em Bacharelado em Direito.

Orientador: Prof. Esp. Luís Claudio dos Santos Ribeiro.

.

SANTA INÊS - MA

2025

(19374) FACULDADE SANTA LUZIA – FSL

CREDENCIAMENTO - MEC / PORTARIA MINISTERIAL Nº 1.166 DE 15.09. 2017

JOÃO VICTOR FONSECA SANTOS

A INTELIGÊNCIA ARTIFICIAL NO RECONHECIMENTO FACIAL APLICADO À INVESTIGAÇÃO CRIMINAL E SEUS IMPACTOS NA ADMISSIBILIDADE DA PROVA NO PROCESSO PENAL BRASILEIRO

Data da Defesa: 27 de novembro de 2025

BANCA EXAMINADORA

Orientador
Nome Completo e Titulação

Examinador 1
Nome Completo e Titulação

Examinador 2
Nome Completo e Titulação

Nota: 10,0 (DEZ)

RESUMO

O presente trabalho tem como objeto de estudo a utilização da Inteligência Artificial (IA) no reconhecimento facial para investigação criminal, com foco nos riscos de viés algorítmico e na admissibilidade dessa prova no processo penal brasileiro. O objetivo geral é analisar os desafios jurídicos e técnicos decorrentes da aplicação dessa tecnologia no âmbito penal. Como objetivos específicos, busca-se compreender o funcionamento do reconhecimento facial, identificar os impactos do viés algorítmico sobre a justiça criminal e examinar a compatibilidade dessa prova com os princípios do processo penal. A pesquisa será estruturada em três capítulos: o primeiro tratará do funcionamento da tecnologia e sua aplicação na investigação criminal; o segundo abordará os riscos de viés algorítmico e seus impactos no sistema penal; e o terceiro discutirá os aspectos jurídicos da admissibilidade da prova digital. A metodologia utilizada será qualitativa, com revisão bibliográfica e análise de jurisprudência. Conclui-se que, embora o reconhecimento facial possa ser uma ferramenta útil para investigação criminal, sua implementação sem critérios claros pode comprometer direitos fundamentais e gerar insegurança jurídica.

Palavras-chave: Admissibilidade da prova, Inteligência Artificial, Processo Penal, Reconhecimento facial, Viés algorítmico.

ABSTRACT

This study examines the use of Artificial Intelligence (AI) in facial recognition for criminal investigation, focusing on algorithmic bias risks and the admissibility of such evidence in Brazilian criminal proceedings. The general objective is to analyze the legal and technical challenges arising from the application of this technology in criminal law. The specific objectives are to understand how facial recognition works, identify the impact of algorithmic bias on criminal justice, and assess the compatibility of this evidence with procedural principles. The research is structured into three chapters: the first discusses the technology and its use in criminal investigations; the second addresses algorithmic bias risks and their effects on the legal system; and the third examines the legal aspects of digital evidence admissibility. The methodology is qualitative, based on bibliographic review and case law analysis. The study concludes that although facial recognition can be a valuable investigative tool, its implementation without clear criteria may violate fundamental rights and generate legal uncertainty.

Keywords: Algorithmic bias, Artificial Intelligence, Criminal Procedure, Facial Recognition, Evidence Admissibility.

A INTELIGÊNCIA ARTIFICIAL NO RECONHECIMENTO FACIAL APLICADO À INVESTIGAÇÃO CRIMINAL E SEUS IMPACTOS NA ADMISSIBILIDADE DA PROVA NO PROCESSO PENAL BRASILEIRO

[1] João Victor Fonseca Santos
[2] Luís Claudio dos Santos Ribeiro

INTRODUÇÃO

A Inteligência Artificial (IA) tem se consolidado como uma ferramenta essencial em diferentes campos do conhecimento, especialmente no plano da investigação criminal. Dentre suas aplicações mais notáveis, destaca-se a aplicação de sistemas de reconhecimento facial para identificação e rastreamento de indivíduos suspeitos. Essa inovação, que abrange desde o aprendizado de máquina até sistemas de visão computacional, vem transformando não somente a economia e as comunicações, mas também a maneira como o Estado conduz suas funções de controle e investigação.

Como afirmam Scopel e Puhl (2024), a tecnologia de reconhecimento facial tem assumido papel relevante na investigação criminal contemporânea, ampliando a aptidão do Estado em identificar e supervisionar indivíduos suspeitos. Nesse cenário, analisar criticamente a utilização dessas ferramentas mostra-se imprescindível para compreender seus limites, riscos e possibilidades dentro do Estado Democrático de Direito.

Todavia, a inserção da Inteligência Artificial na persecução penal também levanta questões fundamentais relacionadas aos riscos de viés algorítmico e à admissibilidade da prova gerada por esses sistemas no processo penal brasileiro, revelando desafios e insuficiências que não podem ser desconsiderados, e que podem ocasionar em identificações errôneas e consequentes injustiças. Segundo Scopel e Puhl (2024), embora essa tecnologia ofereça diversas utilidades, seu emprego ainda enfrenta restrições, especialmente devido à necessidade de resguardar direitos fundamentais e garantir maior precisão e transparência nos algoritmos.

---

[1] Concludente do Curso de Direito da Faculdade Santa Luzia – Turma: 2021-1.
[2] Docente da Faculdade Santa Luzia. Mestrando em Contabilidade e Administração pela Fucape. Especialista em Direito Tributário. Especialista em Administração Pública. Especialista em Direito Administrativo e Gestão Pública. Especialista em Contabilidade Pública.

Além dos desafios técnicos e jurídicos mencionados, é essencial considerar o impacto social da utilização da Inteligência Artificial no reconhecimento facial no âmbito da investigação criminal. A introdução dessa tecnologia no sistema de justiça pode reforçar desigualdades existentes, uma vez que algoritmos treinados com bases de dados enviesadas tendem a perpetuar preconceitos estruturais. Lisboa *et al*. (2025) aponta que a falta de transparência nos algoritmos e a ausência de regulamentação adequada perpetuam a opacidade e a irresponsabilidade no aditamento e implementação dessas tecnologias.

Outra questão significativa é a compatibilidade do uso do reconhecimento facial com os direitos fundamentais previstos na Constituição Federal de 1988, especialmente com relação à privacidade e à proteção de dados pessoais. Embora a Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018) estabeleça diretrizes claras para o procedimento de informações sensíveis, incluindo aquelas obtidas através de tecnologias biométricas, conforme Almeida (2020), não é aplicada inteiramente aos casos de tratamento de dados pessoais para fins exclusivamente de segurança pública.

Nesse contexto, Scopel e Puhl (2024) enfatizam que há uma lacuna no ordenamento jurídico brasileiro e propõem uma regulamentação específica a respeito do uso do reconhecimento facial automatizado como prova no processo penal, e que esta regulamentação deve ser regida por uma legislação específica.

O problema que orienta esta pesquisa surge justamente dos desafios técnicos e jurídicos decorrentes do uso do reconhecimento facial em investigações criminais, sobretudo em virtude dos vieses algorítmicos e da ausência de regulamentação específica para sua utilização como prova digital. Assim, questiona-se: como admitir, no processo penal brasileiro, uma prova produzida por sistemas sujeitos a erros estruturais e desigualdades históricas? O reconhecimento facial, ao invés de representar mera inovação tecnológica, expõe a tensão entre eficiência policial e garantia de direitos fundamentais, especialmente quando erros algorítmicos resultam em prisões indevidas e violações do devido processo legal.

A justificativa deste estudo decorre do impacto social e jurídico dos erros documentados no uso do reconhecimento facial. Como demonstram Scopel e Puhl (2024), durante a ampliação do projeto-piloto, no Rio de Janeiro, pelo menos duas pessoas foram erroneamente identificadas como suspeitas, evidenciando que a

tecnologia, quando aplicada sem controle e sem parâmetros técnicos rigorosos, viola liberdades individuais.

Diante desse contexto, o objetivo geral desta pesquisa consiste em analisar o uso de recursos de inteligência artificial no reconhecimento facial aplicado à investigação criminal, bem como examinar seus impactos na admissibilidade da prova digital no processo penal brasileiro. Já os objetivos específicos buscam compreender o funcionamento da Inteligência Artificial e do *machine learning*; examinar o fenômeno do viés algorítmico e seus reflexos no sistema penal; e avaliar os requisitos jurídicos necessários para que a prova digital seja considerada válida e lícita.

A metodologia adotada no presente estudo é qualitativa, bibliográfica e documental, fundamentada em doutrinas jurídicas, estudos interdisciplinares, reportagens jornalísticas e jurisprudência recente. A análise envolve os requisitos legais da prova digital, como a legalidade, o devido processo legal, a cadeia de custódia, a verificação da acurácia dos algorítmos, a transparência algorítmica e o respeito à igualdade material, considerados aspectos essenciais à avaliação da licitude e confiabilidade de elementos probatórios produzidos por sistemas automatizados.

A contribuição acadêmica deste trabalho consiste em oferecer um estudo integrado entre tecnologia, processo penal e direitos fundamentais, propondo critérios de admissibilidade da prova digital compatíveis com as exigências constitucionais.

O trabalho está dividido nas seguintes partes: 1) a introdução, que apresenta a contextualização do tema, o problema a ser abordado, a justificativa, o objetivo geral, a metodologia utilizada e a relevância da contribuição acadêmica; 2) o primeiro capítulo, que expõe os fundamentos técnicos e conceituais da tecnologia, abordando o reconhecimento facial na investigação criminal; 3) o segundo capítulo, que analisa criticamente o viés algorítmico e seus impactos no processo penal, destacando estudos e casos concretos; 4) o terceiro capítulo, que examina os requisitos de admissibilidade da prova digital e discute possibilidades de regulamentação específica para seu uso; e 5) as considerações finais, que sintetizam os principais achados e reforçam a necessidade de critérios claros e regulamentação adequada para o uso legítimo dessa tecnologia no campo penal.

1. O RECONHECIMENTO FACIAL NA INVESTIGAÇÃO CRIMINAL

O reconhecimento facial constitui um método de identificação biométrica no qual um sistema analisa as características do rosto de uma pessoa e, utilizando algoritmos, confronta essas informações com uma imagem digital previamente armazenada, a fim de verificar se há coincidência e confirmar ou não sua identidade (Mena, 2018 apud Scopel e Puhl, 2024).

O uso de sistemas de reconhecimento facial tornou-se cada vez mais significativo no contexto das investigações modernas, ampliando os meios do Estado para identificar e vigiar possíveis suspeitos. Conforme destacam Scopel e Puhl (2024), os órgãos públicos têm utilizado essa tecnologia de forma ampla e para múltiplos propósitos, buscando aprimorar seus mecanismos de controle, inclusive no âmbito das investigações criminais.

Souza e Zanatta (2021) definem que o reconhecimento facial é um processamento computadorizado que detecta rostos, extrai características distintivas dos rostos e compara essas características com as acumuladas em um banco de dados. Almeida (2022) acrescenta que essa tecnologia opera em duas etapas: o reconhecimento do rosto humano e a identificação da pessoa. Já Lisboa *et al*. (2025) aduzem que essa tecnologia possui diversas aplicações, como controle de acesso, segurança, identificação em fotos, desbloqueio de telefones e até mesmo análise de emoções.

Nesse contexto, é mister salientar que o reconhecimento facial é uma das aplicações mais emblemáticas da Inteligência Artificial (IA) no âmbito da segurança pública e da persecução penal. Todavia, a aplicação do reconhecimento facial na investigação criminal brasileira tem suscitado uma sequência de debates éticos, técnicos e jurídico, pois, embora a tecnologia prometa contribuir para a identificação de suspeitos e a elucidação de crimes, ela também pode gerar sérios riscos à integridade dos direitos fundamentais.

Doravante, se aplicadas corretamente, essas ferramentas de reconhecimento facial e inteligência artificial podem otimizar investigações, reduzir custos operacionais e aumentar a eficácia do sistema penal.

1.1. Definição de Inteligência Artificial (IA) e *machine learning*

A Inteligência Artificial consolidou-se como uma das mais significativas

inovações tecnológicas do século XXI, influenciando diversas áreas do conhecimento e da prática social, inclusive o Direito. Em termos gerais, entende-se por Inteligência Artificial a capacidade de sistemas computacionais simularem aspectos da cognição humana, como o raciocínio, o aprendizado e a tomada de decisão autônoma. Tais sistemas são concebidos para executar tarefas específicas e adaptar-se a novas informações, aprendendo com dados previamente analisados.

Coimbra *et al*. (2023) pondera que, apesar de não haver um conceito universalmente aceito, a Inteligência Artificial (IA) é comumente compreendida como a capacidade de máquinas produzirem comportamentos típicos de seres humanos, fundamentada na manipulação de algoritmos.

No campo jurídico, a definição de Inteligência Artificial ganha relevância por seus impactos na produção de provas e na responsabilização penal, principalmente no uso do reconhecimento facial para localizar foragidos, identificar suspeitos ou confirmar identidades em tempo real. Almeida (2022) descreve que “o reconhecimento facial é o resultado do uso de um algoritmo baseado em visão computacional e aprendizado de máquinas, o que demonstra como a Inteligência Artificial é aplicada na prática para resolver problemas complexos de identificação.

De acordo com a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), citada por Civitarese (2024), sistemas de IA são máquinas que, diante de objetivos definidos por humanos, têm a capacidade de realizar previsões, recomendações ou tomar decisões de forma a influenciar o ambiente real ou virtual, operando com níveis variáveis de autonomia. Essa definição enfatiza o papel humano na definição dos fins e o papel autônomo das máquinas na execução dos meios, uma característica central das tecnologias inteligentes.

Maranhão *et al*. (2021), por sua vez, aduz que a Inteligência Artificial não se restringe a uma tecnologia isolada, mas envolve um conjunto de métodos capazes de permitir que sistemas computacionais identifiquem padrões e resolvam problemas com base em dados. Nesse contexto, destaca-se o *machine learning* (aprendizado de máquina), um dos ramos centrais da Inteligência Artificial.

O *machine learning* permite que sistemas aprendam e melhorem automaticamente a partir de dados, sem a necessidade de serem explicitamente programados para realizar tarefas específicas. Conforme Civitarese (2024), é um subcampo da inteligência artificial (IA) que se concentra no desenvolvimento de algoritmos e modelos que permitem que os computadores aprendam a partir de

dados e façam previsões ou decisões sem serem explicitamente programados para realizar tarefas específicas.

Para Coimbra *et al*. (2023), o emprego de programas de *machine learning* e sua vertente mais avançada (*deep learning*), conferiu às máquinas uma notável habilidade de evoluir por meio da experiência e de tomar decisões de forma autônoma. Lisboa *et al*. (2025), por sua vez, afirma que o *machine learning* refere-se à capacidade dos sistemas de aprenderem com dados, sem serem explicitamente programados para cada tarefa específica, permitindo que façam previsões ou tomem decisões com base nesse aprendizado. Essa característica torna o *machine learning* especialmente eficaz em contextos como o reconhecimento facial, a análise de padrões criminais e a identificação de suspeitos.

Coimbra *et al*. (2023) observa que o *machine learning*, ao ser aplicado em contextos de segurança pública, tende a espelhar estruturas de poder e desigualdade já existentes, reforçando estereótipos e ampliando a seletividade penal.

> À vista disso, a utilização do reconhecimento facial tem sido divulgada como ferramenta facilitadora e precisa na localização de indivíduos procurados pela polícia, sendo uma solução para o problema de identificação de suspeitos pelo homem. Entretanto, tem havido, com frequência, erros possibilitando prisões indevidas. Isso porque, a precisão dos sistemas de reconhecimento facial não é garantida na totalidade dos casos, pois os algoritmos podem apresentar taxas de erro, especialmente ao identificar indivíduos de grupos étnicos diversos, levando a um risco específico de identificações falsas. (COIMBRA *et al*., 2023)

Lisboa *et al*. (2025) enfatizam que a falta de regulamentação adequada, a opacidade dos algoritmos e os vieses embutidos na tecnologia representam sérias ameaças aos direitos fundamentais e podem perpetuar a discriminação contra grupos já marginalizados. Na visão de Maranhão *et al*. (2021), a opacidade de sistemas de aprendizado de máquina é uma das maiores fontes de atenção e preocupação na atualidade, principalmente em relação ao risco de incorporação de vieses que resultem em construção de perfis ou tomadas de decisão discriminatórias, ou ainda da probabilidade de tomadas de decisão que ignorem valores humanos ou desrespeitem direitos fundamentais e a dignidade humana.

Diante desse cenário, Scopel e Puhl (2024) levantam a dúvida sobre a admissibilidade jurídica das evidências obtidas por reconhecimento facial no processo penal, já que atualmente não existe uma norma específica que regule o uso dessa tecnologia como meio probatório, o que acaba gerando incertezas quanto

à sua validade.

Assim, como destaca Maranhão *et al*. (2021), as perspectivas de implantação da Inteligência Artificial no sistema jurídico brasileiro exige uma reflexão crítica sobre seus limites e possibilidades. A tecnologia deve estar a serviço da justiça e da equidade, e não da reprodução de desigualdades. Dessa forma, o avanço da Inteligência Artificial e do *machine learning* no campo jurídico precisa ser guiado por princípios éticos, normativos e democráticos, assegurando o respeito aos direitos fundamentais e à integridade do Estado Democrático de Direito.

1.2 Uso da tecnologia pelas forças de segurança no Brasil e no mundo

O avanço tecnológico tem transformado significativamente a atuação das forças de segurança pública no Brasil e em diversos países ao redor do mundo. Almeida (2022) observa que a tecnologia de reconhecimento facial está cada vez mais sendo usada como instrumento válido para complementação da atividade policial. Assim como está acontecendo em outras nações em todo o mundo, Ponce (2022) reforça que o Brasil está passando por uma expansão no uso de tecnologias de videomonitoramento e reconhecimento facial para fins de segurança pública.

Em países como China, Estados Unidos e Reino Unido, a incorporação de tecnologias como câmeras de reconhecimento facial, drones, softwares de previsão criminal e sistemas de *big data* tem alterado a lógica tradicional da investigação e da repressão criminal. Maranhão *et al*. (2021) relatam que a China, por exemplo, tem utilizado uma combinação de vigilância por meio de inteligência artificial com uso de enorme quantidade de dados pessoais para monitorar a vida e o comportamento das pessoas em detalhes minuciosos. Todavia, há um amplo debate global centrado na tensão entre segurança pública e liberdade individual, sendo essencial definir os limites éticos e legais do uso dessas ferramentas.

Ocorre que o uso da tecnologia pelas forças de segurança no Brasil e no mundo revela uma tensão estrutural entre eficiência repressiva e respeito aos direitos humanos. Nesse contexto, Ponce (2022) assevera que experiências com câmeras de reconhecimento facial utilizadas para segurança pública levantaram preocupações sobre seus potenciais erros e efeitos discriminatórios. Tal constatação nos convida a fazermos reflexões teóricas sobre como essas tecnologias devem ser enquadradas sob a ótica do direito antidiscriminatório.

Mas apesar dos riscos, é inegável que o uso de tecnologia pelas forças de

segurança pode trazer benefícios significativos à persecução penal, desde que acompanhado de transparência e controle. Como afirmam Lisboa *et al*. (2025), um dos maiores desafios reside na mitigação de vieses e preconceitos, especialmente no tocante à auditoria e à transparência desses sistemas baseados em tecnologia de reconhecimento facial. Afirmam ainda que a busca por uma Inteligência Artificial ética e justa é um desafio urgente e complexo, mas fundamental para construir um futuro digital mais equitativo e seguro para todos.

Assim, a auditoria contínua é condição essencial para compatibilizar inovação tecnológica e proteção de direitos fundamentais. Nessa esteira, é imprescindível refletir sobre os limites da atuação estatal no uso de tecnologias para investigação e repressão, pois se o uso de Inteligência Artificial na segurança pública não for bem regulado, pode prejudicar a observância das garantias processuais, da presunção de inocência e do contraditório.

Com isso, quando um reconhecimento facial automatizado é utilizado para embasar uma prisão em flagrante ou uma denúncia, é fundamental que sua confiabilidade técnica seja demonstrada e que haja possibilidade de contestação por parte da defesa. É dever do Estado, da sociedade e da academia garantir que o uso dessas ferramentas ocorra com responsabilidade, transparência e respeito ao devido processo legal.

1.3 Benefícios e desafios do uso da IA na investigação criminal

O reconhecimento facial pode oferecer vantagens importantes para a investigação criminal, como maior celeridade na identificação de suspeitos, análise automatizada de imagens e economia de recursos. Scopel e Puhl (2024) apontam que, quando determinados requisitos são atendidos, o uso do reconhecimento facial pode se adequar às normas jurídicas e servir como ferramenta legítima para a identificação de pessoas em procedimentos penais.

Dentre os mais importantes benefícios da investigação criminal moderna está o aprimoramento da coleta de provas e a celeridade na apuração dos fatos. Com o advento da tecnologia, a análise de grandes volumes de dados, a rastreabilidade de movimentações financeiras e a identificação de padrões comportamentais tornaram-se mais acessíveis. Isso possibilita identificar padrões de comportamento e conexões entre crimes que seriam imperceptíveis à análise humana.

A capacidade de análise automatizada de imagens e vídeos é outro benefício

que a Inteligência Artificial proporciona. Ademais, a inteligência artificial tem sido aplicada no cruzamento de dados bancários, registros telefônicos e câmeras de segurança, o que evidencia maior eficiência investigativa.

Outro benefício potencial das tecnologias inteligentes é a economia de recursos humanos e financeiros. Como destacam Maranhão *et al*. (2021), a proliferação de inteligências artificiais significa seu envolvimento ubíquo em diversas relações sociais e econômicas tuteladas pelo Direito. Se aplicadas corretamente, essas ferramentas podem otimizar investigações, reduzir custos operacionais e aumentar a eficácia do sistema penal.

Todavia, ao lado dos benefícios evidentes, surgem inúmeros desafios, éticos, jurídicos e operacionais, que exigem reflexão crítica e rigor metodológico. Almeida (2022) alerta que a incidência de falsos positivos causa danos às pessoas não culpáveis, visto que a identificação errônea de um inocente como uma pessoa que cometeu crime pode acarretar na prisão da pessoa errada e, possivelmente, na condenação de um sujeito que não cometeu nenhum crime. Isso significa que um simples erro algorítmico pode resultar em grave violação de direitos e em injustiças processuais.

O respeito aos direitos fundamentais do investigado, especialmente quanto à privacidade, à ampla defesa e ao contraditório, é outro desafio a ser observado. Nessa esteira, Noble (2022, *apud* Lisboa *et al*., 2025) enfatiza que o reconhecimento facial apresenta desafios significativos, como vieses raciais e de gênero nos algoritmos, problemas de privacidade e falta de consentimento na coleta e uso de dados. Assim, se a coleta de dados por meios tecnológicos não for submetida a rígidos controles legais, pode configurar verdadeiro mecanismo de vigilância estatal indevida. Portanto, a proteção da intimidade, prevista no artigo 5º, inciso X, da Constituição Federal, deve ser baliza inafastável na condução de diligências, inclusive tecnológicas.

Outro desafio relevante é o da cadeia de custódia da prova digital, que exige conhecimento técnico específico e protocolos rigorosos para garantir sua integridade. Segundo Scopel e Puhl (2024), Existem inquietações de ordem ética relacionadas à possibilidade de a tecnologia ser empregada de maneira indevida ou até para finalidades ilícitas. A ausência de preparo dos operadores do direito nesse campo pode comprometer a validade de provas e até gerar nulidades processuais.

Como se percebe, a investigação criminal contemporânea apresenta

inegáveis benefícios relacionados à eficiência, precisão e amplitude probatória, principalmente com o apoio da inteligência artificial. Contudo, seu uso exige cautela, regulamentação e vigilância ética constante, com vistas a estabelecer um equilíbrio entre investigação criminal e direitos fundamentais, constituindo-se em um verdadeiro desafio do processo penal tecnológico.

2. O VIÉS ALGORÍTMICO E SEUS IMPACTOS NO PROCESSO PENAL

2.1 Definição e causas do viés algorítmico

O viés algorítmico consiste na reprodução, pelos sistemas de inteligência artificial, de preconceitos e desigualdades históricas presentes nos dados utilizados para seu treinamento. Pode ser compreendido como uma distorção sistemática nos resultados produzidos por sistemas baseados em inteligência artificial, oriunda, em regra, de imperfeições presentes nos dados de treinamento, na modelagem estatística ou nas decisões humanas que permeiam o processo de construção dos algoritmos.

Conforme Lisboa *et al*. (2025), algoritmos, como qualquer outra ferramenta criada por humanos, refletem e podem perpetuar os vieses e preconceitos de seus criadores. Assim, longe de serem neutros, os algoritmos acabam por espelhar os mesmos estigmas que permeiam o sistema penal humano.

É por isso que Almeida (2022) suscita questionamentos se o reconhecimento facial é uma tecnologia adequada a espaços democráticos diante da iminente possibilidade de violações de direitos fundamentais, como a privacidade e o direito de ir e vir. Complementa, advertindo que a falta de acurácia e a existência de bases de dados de treinamento enviesadas, possuem como consequência a discriminação de grupos que são mais prováveis de serem identificados erroneamente pelo reconhecimento facial. Conforme Ponce (2022), essa discriminação algorítimica decorre do uso de conjuntos de dados que refletem estruturas sociais desiguais, e pode derivar de erros estatísticos, generalizações injustas, bem como de outros resultados tendenciosos que restringem o exercício de direitos.

Tais vieses acabam por refletir, reforçar ou mesmo amplificar discriminações sociais pré-existentes, podendo comprometer a imparcialidade e a equidade na utilização de sistemas baseados em inteligência artificial, especialmente quando aplicadas no campo da investigação criminal. Sobre esse ponto, Scopel e Puhl

(2024) explicam que o reconhecimento facial funciona com base em probabilidades, não oferecendo resultados absolutamente determinados. O sistema apenas aponta níveis de correspondência, mais ou menos prováveis, dependendo da qualidade e da adequação dos dados utilizados em seu treinamento.

Nunes (2021, *apud* Ponce, 2022) relata que 90,5% dos indivíduos presos, após serem detectados por câmeras de monitoramento facial, eram negros. A lista continha vários erros: por exemplo, uma mulher já estava presa e outro foi levado no lugar de um que já havia sido preso há quatro anos. Esse dado evidencia que os erros não são apenas técnicos, mas refletem padrões estruturais de discriminação racial.

Portanto, o viés algorítmico representa um desafio estrutural à justiça penal contemporânea e o seu respectivo combate representa uma condição indispensável para a preservação da legitimidade do processo penal e da confiança no sistema de justiça. Ignorar essas distorções pode implicar na legitimação de decisões injustas, contrariando preceitos constitucionais como a dignidade da pessoa humana, o devido processo legal e a presunção de inocência. O desafio, portanto, reside em compatibilizar a inovação tecnológica com os princípios do Estado Democrático de Direito, assegurando que os algoritmos operem de forma ética, transparente e responsável.

2.2 Estudos e casos concretos de erros no reconhecimento facial

A literatura nacional e internacional tem registrado diversos erros decorrentes do uso de tecnologias de reconhecimento facial, especialmente quando aplicadas à segurança pública. O erro mais recorrente reside no problema dos falsos positivos. Conforme explica Almeida (2022), um falso positivo ocorre quando o sistema reconhece a compatibilidade entre o *template* de uma pessoa capturada em tempo real e um *template* contido no banco de dados, mas a pessoa que passou pela câmera de vigilância não é quem o sistema diz que ela é. Significa atribuir um crime a quem não o praticou. As consequências desse erro no processo penal são severas e podem levar à prisão indevida.

Todavia, além dos falsos positivos, há também a influência dos falsos negativos. Almeida (2022) define os falsos negativos como sendo aqueles que ocorrem quando o sistema de reconhecimento facial falha na correspondência entre um rosto e uma assinatura facial que, de fato, está contida em um banco de dados.

Ou seja, o sistema retornará erroneamente zero resultados em resposta a uma consulta, sendo que existe um resultado válido. Tendo em vista a persecução penal, o prejuízo decorrente da incidência de falsos negativos consiste em não ocorrer a identificação de uma pessoa que cometeu um crime.

Diversos estudos têm demonstrado que sistemas de reconhecimento facial não são infalíveis, sendo particularmente imprecisos na identificação de pessoas negras, mulheres e indivíduos mais jovens, o que gera um risco real de violações de direitos fundamentais.

Um desses estudos foi apresentado pelo National Institute of Standards and Technology (NIST), agência governamental estadunidense sobre inovação e competitividade tecnológica. O NIST analisou dezenas de algoritimos de reconhecimento facial usados por 99 desenvolvedores e encontrou uma variedade de taxas de precisão entre eles, com taxas mais altas de falsos positivos em rostos asiáticos e afro-americanos em relação aos de causasianos (Eaton, 2020 *apud* Souza e Zanatta, 2021).

Entre outras descobertas, este estudo demonstrou que os falsos positivos são entre 2 e 5 vezes maiores em mulheres que em homens, variando de acordo com o algoritmo, país de origem e idade (Nist, 2019 *apud* Almeida, 2022). Esse resultado revela que algoritmos de reconhecimento facial têm variações na acurácia, dependendo do grupo demográfico de um sujeito.

Ainda no campo internacional, um relatório produzido pelo Big Brother Watch – BBW, em 2018, indica que, no Reino Unido, 95% de correspondências feitas por reconhecimento facial resultaram em identificação incorreta de pessoas inocentes. Ou seja, do total de pessoas reconhecidas pelo sistema como um *template* contido no conjunto de dados, 95% eram falsos positivos (Almeida, 2022).

No Brasil, os efeitos desses erros já se materializaram em casos concretos amplamente divulgados pela imprensa, que passaremos a discriminar resumidamente, extraídos das literaturas pesquisada e de fontes jornalísticas.

O primeiro caso de relevância refere-se aos falsos positivos que ensejaram em duas prisões equivocadas no Rio de Janeiro, em 2019, ocorridas após a integração da tecnologia de reconhecimento facial nas políticas de segurança pública, tendo início durante o Carnaval daquele ano com a instalação de 34 câmeras. Durante a ampliação do projeto-piloto, pelo menos duas pessoas foram erroneamente identificadas como suspeitas, caracterizando falsos positivos (Scopel

e Puhl, 2024). Esse caso demonstra que o sistema, ao operar em ambiente real e com grande fluxo de pessoas, tende a gerar alertas imprecisos que resultam em abordagens ilegais e em violações à liberdade individual.

O segundo caso de relevância ocorreu na Bahia, em face de prisões indevidas por mandados já revogados. Conforme reportagem divulgada por Alencar (2023), no portal g1 Bahia, Um homem negro acabou sendo preso ao chegar ao Parque de Exposições da capital com sua esposa e seu filho, onde pretendiam aproveitar o evento. Vigilante de profissão, ele foi detido e permaneceu 26 dias encarcerado, acusado injustamente de um roubo. O delito que motivou a prisão havia sido praticado em 2012 por outra pessoa. O verdadeiro autor do crime foi capturado em flagrante e forneceu às autoridades o nome e as digitais do vigilante. Esse indivíduo foi liberado em 2013 e posteriormente condenado a cinco anos e quatro meses de prisão. Ainda que não tenha havido erro de identificação facial, houve erro no cruzamento de dados, evidenciando que a tecnologia depende de bases atualizadas e confiáveis, o que não ocorreu.

Outros casos de erros decorrentes do uso de tecnologias de reconhecimento facial é demonstrado no quadro abaixo:

Quadro 1: Exemplos de falsos positivos em reconhecimento facial (fontes jornalísticas)

Data	Local	Vítima	Resumo	Fonte
10/07/2019	Copacabana, RJ	Mulher (moradora)	Sistema de reconhecimento facial da PM identificou erroneamente a mulher como foragida; ela foi detida, levada à 12ª DP e liberada depois da checagem de documentos.	G1 Rio
28/09/2020 (audiência)	Niterói, RJ	Danillo Félix	Foi preso com base em reconhecimento fotográfico (fotos antigas do Facebook), mas absolvido após audiência, porque a vítima não o reconheceu presencialmente.	O Dia
02/01/2024	Copacabana, RJ	Silvio Gabriel Juarez (argentino)	Preso após alerta do sistema de videomonitoramento com reconhecimento facial; na audiência de custódia constatou-se que seu mandado já havia sido revogado –detenção ilegal.	Brasil de Fato
13/04/2024 (jogo)	Estádio Lourival Batista, Aracaju, SE	João Antônio (personal trainer)	Identificado por reconhecimento facial via drone, foi retirado da arquibancada por policiais durante partida de futebol; depois se descobriu que era um erro e ele foi liberado.	Carta Capital

(continua)

10/10/2024 (sentença)	Recife, PR	Homem absolvido por erro em reconhecimento por foto	Decisão anulou sentença após constatação de falhas graves no reconhecimento do réu, que foi baseado em uma foto 3x4 tirada 9 anos antes do crime.	CNN Brasil

Fonte: Elaborado pelo autor.

Como se vê, os erros documentados não apenas prejudicam indivíduos injustamente identificados, mas também comprometem a credibilidade do sistema de justiça criminal, repercutindo negativamente tanto na legitimidade das instituições quanto na confiança social. Assim, é imprescindível a criação de normas que obriguem a realização de auditorias periódicas, a publicação dos critérios técnicos utilizados, o direito à explicação em casos de decisões automatizadas e a responsabilização de agentes públicos e empresas envolvidas em casos de erro ou abuso.

3. A ADMISSIBILIDADE DA PROVA DIGITAL NO PROCESSO PENAL BRASILEIRO

3.1 A prova digital e seus requisitos de admissibilidade

A transformação digital do sistema de justiça trouxe novas formas de produção e utilização de provas, entre elas as derivadas de sistemas algorítmicos e inteligência artificial. A *digital evidence* ou prova digital tem se tornado uma das principais formas de obtenção de elementos probatórios no processo penal contemporâneo, sobretudo diante da crescente informatização da sociedade e da intensificação do uso de tecnologias digitais.

A prova digital se caracteriza por qualquer elemento probatório extraído de dispositivos ou sistemas eletrônicos, como registros em redes sociais, conversas em aplicativos de mensagens, e-mails, dados de geolocalização, arquivos armazenados em nuvem, entre outros.

Ao estabelecer os princípios da presunção de inocência e do in dubio pro reo, a Constituição exige que a condenação penal só ocorra quando a culpa estiver comprovada para além de qualquer dúvida razoável (Lopes Jr., 2019, *apud* Scopel e Puhl, 2024). Para fundamentar uma decisão condenatória, o juiz pode recorrer às chamadas provas atípicas,aquelas que não estão expressamente previstas no Código de Processo Penal ,como ocorre com o uso do reconhecimento facial. Assim,

em tese, o ordenamento jurídico brasileiro admite a utilização de provas digitais, desde que observadas as garantias processuais e técnicas.

Com a ampliação do espaço virtual como ambiente de práticas humanas, lícitas ou ilícitas, o Direito Penal e o Direito Processual Penal precisaram, então, adaptar suas ferramentas de persecução para lidar com dados eletrônicos e rastros digitais. Nesse sentido, o reconhecimento facial automatizado tem sido empregado como elemento de prova em diversas investigações e ações penais, mas sua admissibilidade ainda é tema de controvérsia.

Essa controvérsia ocorre porque a utilização de tais provas no processo penal exige rigor técnico e jurídico quanto à sua admissibilidade, sob pena de violação de direitos e garantias fundamentais, para serem consideradas válidas judicialmente. Assim, qualquer tecnologia que produza evidências digitais, como é o caso do reconhecimento facial, deve submeter-se a esses requisitos de licitude, ainda que apresente avanços técnicos relevantes.

A prova digital, diferentemente da prova material tradicional, decorre do tratamento e armazenamento de informações eletrônicas, o que exige requisitos específicos, dentre os quais destacam-se: a legalidade, o devido processo legal, a cadeia de custódia, a verificação da acurácia dos algorítmos, a transparência algorítmica e o respeito à igualdade material.

O primeiro requisito de admissibilidade da prova digital é a legalidade, que decorre do art. 5º, LVI, da Constituição Federal: *"são inadmissíveis, no processo, as provas obtidas por meios ilícitos"*. Ao vedar o uso de provas obtidas por meios ilícitos, a Constituição impede que qualquer elemento produzido de forma ilegal seja aproveitado no processo, abrangendo tanto as provas ilícitas quanto as ilegítimas, independentemente de a violação ocorrer em normas de direito material ou processual. (Capez, 2024 *apud* Scopel e Puhl, 2024). Assim, provas digitais obtidas sem autorização judicial, sem fundamento legal ou mediante violação da privacidade devem ser desentranhadas do processo penal.

Outro requisito é o respeito ao devido processo legal, o qual impõe que todas as formas de obtenção de evidências digitais como mensagens, metadados, registros de IP, vídeos, dados de geolocalização, reconhecimento facial etc, sejam obtidos com observância estrita da lei. Badaró (2021, *apud* Scopel e Puhl, 2024) ressaltam que, quando se trata de provas digitais, é indispensável observar técnicas próprias da informática que assegurem sua autenticidade e preservação. Isso

envolve cuidados específicos em todas as etapas, desde a coleta e documentação até o armazenamento, exame e apresentação desses dados, seguindo padrões reconhecidos no Brasil e no exterior. Nesse sentido, destacam que tecnologias automatizadas só podem ser utilizadas quando houver regras claras e passíveis de verificação.

A cadeia de custódia é outro elemento essencial à admissibilidade da prova digital, funcionando como garantia de integridade, autenticidade e confiabilidade do material apresentado no processo. No geral, a cadeia de custódia é considerada como sendo o conjunto de procedimentos documentados que descreve cada etapa pela qual passa a prova, desde a identificação, coleta, armazenamento e transporte, até sua análise pericial e apresentação em juízo. Dessa forma, Scopel e Puhl (2024) destacam que a apresentação de provas digitais no processo penal deve ocorrer mediante perícia especializada, acompanhada do registro integral da cadeia de custódia, a fim de garantir sua confiabilidade. Nesse sentido, a cadeia de custódia constitui elemento fundamental do devido processo legal, pois impede interferências indevidas, adulterações ou inserções não controladas na evidência.

A verificação da acurácia dos algorítmos, ou seja, a porcentagem de vezes em que o reconhecimento facial falha, é requisito essencial para a admissibilidade da prova digital. Conforme Buolamwini e Gebru (2018, *apud* Almeida, 2022), algumas características da imagem podem atrapalhar no bom funcionamento do reconhecimento facial, tais como a iluminação, o enquadramento do rosto, a expressão facial, a qualidade de imagem e o envelhecimento facial. A falta de acurácia pode gerar impactos discriminatórios, especialmente contra grupos raciais vulneráveis. Portanto, somente um algoritmo com acurácia comprovada, auditável e compatível com as garantias fundamentais, poderá produzir prova digital apta a ingressar validamente no processo penal.

A transparência algorítmica constitui outro requisito de admissibilidade da prova digital no processo penal, pois permite avaliar se a tecnologia respeitou padrões éticos e técnicos. Lisboa *et al*. (2025) aduz que a falta de transparência nos algoritmos e a ausência de regulamentação adequada perpetuam a opacidade e a irresponsabilidade no desenvolvimento e implementação da tecnologia de reconhecimento facial. Isso significa que provas produzidas por algoritmos opacos, cujos critérios internos são desconhecidos, violam o contraditório e não podem ser amplamente aceitas.

Por fim, temos o requisito do respeito à igualdade material, com vistas a proteger o acusado contra métodos probatórios que produzam efeitos sistematicamente desiguais, discriminatórios ou desproporcionais, advindo de vieses algorítmicos raciais. Conforme Coimbra *et al*. (2023), a discriminação algorítmica racial é, em essência, uma expressão do racismo estrutural presente na instrumentalização de diversas tecnologias que influenciam a tomada de decisões. Isso pode ser impactante na confiança da prova digital, uma vez que é exigido para a sua admissibilidade, não apenas ausência de discriminação direta, mas que o método probatório não produza impactos desiguais por sua própria lógica de funcionamento. Portanto, qualquer tecnologia utilizada para fins probatórios precisa demonstrar neutralidade algorítmica, ou ao menos que foram adotadas medidas técnicas para minimizar vieses.

Outro aspecto relevante é o papel do contraditório na produção e utilização da prova digital. Nesse diapasão, a parte acusada deve ter acesso ao conteúdo e às condições de produção da prova, podendo contestar sua autenticidade, integridade e relevância. Isso implica, por exemplo, a possibilidade de requerer perícia técnica independente ou impugnar a metodologia utilizada pela autoridade policial na obtenção dos dados.

Em suma, quando os parâmetros de admissibilidade da *digital evidence* (ou prova digital) não são atendidos, esta não pode ingressar validamente no processo, sob pena de comprometer a avaliação judicial e a previsibilidade das decisões, reforçando, assim, a necessidade de normatização para garantir segurança jurídica.

3.2 Possibilidades de regulação e melhorias na admissibilidade

Segundo Scopel e Puhl (2024), o emprego do reconhecimento facial automatizado como prova no processo penal demanda uma norma própria que estabeleça seus critérios de uso, algo que ainda não está previsto na legislação brasileira.. A esse respeito, Lisboa et al. (2025) aduzem que essa lacuna regulatória, aliada à opacidade dos sistemas de Inteligência Artificial, levanta preocupações sobre o potencial de discriminação e violação de direitos fundamentais.

Como se observa, a regulamentação do uso do reconhecimento facial no processo penal é uma necessidade evidente no cenário jurídico brasileiro. Para Fernandes e Resende (2023 *apud* Scopel e Puhl, 2024), A normatização precisa atender a dois propósitos: assegurar a proteção dos direitos e garantias

fundamentais da população e, ao mesmo tempo, possibilitar o uso automatizado de dados pessoais para tornar a persecução penal mais eficiente. Essa necessidade se torna ainda mais relevante diante dos desafios que marcam a sociedade na atual era de riscos globais.

Atualmente, o ordenamento jurídico brasileiro conta com normas gerais sobre provas no Código de Processo Penal, mas estas não se adequam às particularidades das evidências digitais, isto é, não contemplam as especificidades das tecnologias emergentes. Ao contrário das provas tradicionais, as provas digitais podem ser facilmente alteradas, apagadas ou replicadas. Além disso, demandam cadeia de custódia especializada (com *logs*, registros *hash* e rastreabilidade), envolvem softwares e sistemas cujos métodos internos podem ser opacos (*black box*), e dependem de verificação de integridade, autenticidade, confiabilidade e acurácia algorítmica.

Como o legislador ainda não se manifestou sobre o tema, cabe ao operador do direito recorrer às provas tradicionais e aos procedimentos já previstos no ordenamento para enfrentar as especificidades envolvidas na coleta de informações digitais (Badaró, 2021 *apud* Scopel e Puhl, 2024), bem como aplicar dispositivos legais análogos para permitir a sua admissibilidade, como é o caso da Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018).

Embora a LGPD não defina critérios processuais sobre validade, integridade, contraditório ou cadeia de custódia, nem disciplina algoritmos, acurácia ou confiabilidade probatória, e nem tampouco estabelece requisitos para perícias ou reconhecimento facial, porém essa norma impõe limites ao tratamento de dados biométricos, considerados sensíveis, e exige o consentimento ou a existência de fundamento legal claro para sua coleta e uso.

A informação facial é um dado personalíssimo e singular a cada pessoa, como as digitais dos dedos, a íris do olho e o DNA. De acordo com a LGPD, um dado biométrico, quando vinculado a uma pessoa natural, é um dado sensível (art. 5º, II). Com isso, a legislação destaca o tratamento de dados pessoais sensíveis, já que, caso esses sejam conhecidos e submetidos a tratamento, podem se prestar a uma potencial utilização discriminatória ou lesiva e que apresentariam maiores riscos potenciais do que outros tipos de informação (Almeida, 2022). Portanto, a harmonização entre o processo penal e a LGPD se mostra essencial para proteger a privacidade dos indivíduos e evitar abusos investigativos.

De forma análoga, a regra do art. 3º do Código de Processo Civil (CPC) permite que as normas do CPC, subsidiariamente, sejam aplicadas na admissibilidade de provas digitais, reconhecendo que fotos, vídeos, áudios e outras representações tenham força probatória.

> Código de Processo Civil:
> [...]
> Art. 369. As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz.
> [...]
> Art. 422. Qualquer reprodução mecânica, como a fotográfica, a cinematográfica, a fonográfica ou de outra espécie, tem aptidão para fazer prova dos fatos ou das coisas representadas, se a sua conformidade com o documento original não for impugnada por aquele contra quem foi produzida.
> § 1º As fotografias digitais e as extraídas da rede mundial de computadores fazem prova das imagens que reproduzem, devendo, se impugnadas, ser apresentada a respectiva autenticação eletrônica ou, não sendo possível, realizada perícia.
> § 2º Se se tratar de fotografia publicada em jornal ou revista, será exigido um exemplar original do periódico, caso impugnada a veracidade pela outra parte.

Outras legislações espassas também contribuem para fundamentar, de forma subsidiária, a admissibilidade da prova digital, como a Lei nº 13.964/2019 – Pacote Anticrime (arts. 158-A a 158-F, que tratam da cadeia de custódia); a Lei nº 12.965/2014 – Marco Civil da Internet (arts. 10, 13 a 15, que estabelece regras para a validade da prova digital); a Lei nº 12.737/2012 – Lei Carolina Dieckmann (que tipifica crimes informáticos); a Lei nº 9.296/1996 – Lei de Intercepções Telefônicas (é aplicada analogicamente a interceptações telemáticas e dados digitais, com jurisprudência pacífica do STJ e STF); e a Lei nº 12.850/2013 (há entendimento de que suas previsões abrangem dados digitais, metadados e registros telemáticos, inclusive extração de dados de celulares).

Mesmo com essas prováveis possibilidades de admissibilidade das provas digitais no curso do processo penal, com base nas leis apresentadas, mesmo de forma subsidiária, torna-se urgente uma regulamentação específica que estabeleça diretrizes claras para o uso da Inteligência Artifical na tecnologia de reconhecimento facial. Tal regulamentação deve observar os princípios constitucionais do devido processo legal, da ampla defesa, da dignidade da pessoa humana e da igualdade, além de incorporar exigências técnicas mínimas de precisão, transparência e responsabilidade.

Atualmente, alguns projetos de lei tramitam nas duas Casas do Congresso Nacional, como é o caso do Projeto de Lei n° 2.338/2023, de autoria do Senador Rodrigo Pacheco (PSD/MG); do Projeto de Lei nº 1.515/2022, de autoria do Deputado Federal Coronel Armando (PL/SC); e do Projeto de Lei nº 4.939/2020, de autoria do Deputado Federal Hugo Leal (PSD/RJ). O quadro a seguir resume as prerrogativas de cada projeto:

Quadro 2: Iniciativas de projetos de lei que abordam admissibilidade de provas digitais

Projeto de Lei	Ementa
PL 2.338/ 2023	Define diretrizes gerais, válidas em todo o país, para orientar a criação, a aplicação e o uso responsável de sistemas de inteligência artificial no Brasil, visando resguardar direitos fundamentais e assegurar que essas tecnologias sejam seguras, confiáveis e voltadas ao bem da pessoa humana, ao fortalecimento do regime democrático e ao avanço científico e tecnológico.
PL 1.515/2022	Regula o uso de dados pessoais por autoridades competentes quando destinado exclusivamente à segurança do Estado, à defesa nacional, à proteção da segurança pública e às atividades de investigação e repressão de delitos, conforme estabelecido no inciso III do artigo 4º da Lei nº 13.709, de 14 de agosto de 2018.
PL 4.939/2020	Estabelece princípios e diretrizes na aplicabilidade do Direito da Tecnologia da Informação, bem como normas de obtenção e admissibilidade de provas digitais na investigação e no processo, definindo crimes e penas.

Fonte: Elaborado pelo autor.

Como se vê, a evolução tecnológica trouxe formas de obtenção de evidências que o ordenamento jurídico brasileiro não estava preparado para receber. Essa defasagem gera insegurança jurídica e evidencia a necessidade de um marco regulatório específico. Apenas com esse arcabouço normativo robusto e direcionado, será possível garantir que a tecnologia atue como aliada da justiça, e não como instrumento de arbitrariedade ou discriminação.

CONSIDERAÇÕES FINAIS

A análise empreendida ao longo deste trabalho permitiu compreender que o reconhecimento facial aplicado à investigação criminal constitui importante avanço tecnológico, mas cujo uso demanda cautela redobrada. A admissibilidade dessa prova no processo penal requer critérios objetivos e regulamentação específica para evitar injustiças e garantir maior segurança jurídica.

Ao longo do estudo, constatou-se que a Inteligência Artificial representa um marco tecnológico capaz de otimizar a eficiência das forças de segurança, ampliando a capacidade de identificação de suspeitos e a celeridade nas investigações. Contudo, também se evidenciou que essa inovação traz consigo

importantes desafios éticos, técnicos e jurídicos.

No contexto internacional e nacional, o estudo revelou expansão do uso dessas tecnologias por órgãos de segurança pública, o que evidencia a busca por soluções mais eficazes no combate à criminalidade. Porém, essa expansão ocorreu de maneira não uniforme e, por vezes, sem regulamentação adequada, gerando preocupações sobre transparência, controle e responsabilidade na adoção de sistemas de vigilância automatizada.

O exame dos fundamentos técnicos da Inteligência Artificial e do *machine learning* demonstrou que esses sistemas funcionam a partir do processamento de grandes quantidades de dados e da identificação de padrões matemáticos, o que explica tanto sua precisão quanto sua suscetibilidade a erros. Assim, o entendimento de como esses algoritmos operam é indispensável para avaliar se os resultados produzidos por eles possuem confiabilidade suficiente para servir como meio de prova no processo penal.

Os efeitos do viés algorítmico revelaram-se um dos pontos mais críticos do trabalho. Essa constatação demonstra que a aparente neutralidade tecnológica não elimina riscos de discriminação, sobretudo contra grupos vulneráveis, o que impõe ao Estado o dever de avaliar criticamente essas ferramentas antes de utilizá-las como fundamento probatório.

Quanto à admissibilidade da prova digital, concluiu-se que o processo penal brasileiro exige critérios rígidos de legalidade, integridade, autenticidade e confiabilidade para qualquer elemento probatório. A prova derivada de sistemas de reconhecimento facial, por sua natureza técnica complexa, demanda requisitos ainda mais rigorosos, especialmente no que se refere à cadeia de custódia e à verificação da acurácia dos sistemas utilizados. É dever do Estado garantir que o emprego da Inteligência Artificial em segurança pública não se torne um instrumento de violação de liberdades individuais, mas sim um meio legítimo e equilibrado de promoção da justiça e da segurança coletiva.

Diante dessa realidade, conclui-se que o futuro do uso da Inteligência Artificial no âmbito penal dependerá diretamente da capacidade do legislador, do Judiciário e das instituições de segurança pública em estabelecer limites, responsabilidades e salvaguardas que garantam um equilíbrio entre inovação tecnológica e o Estado Democrático de Direito, sem comprometer os valores essenciais que sustentam o sistema jurídico e a proteção da dignidade humana.

REFERÊNCIAS

ALENCAR, Itana. Com mais de mil prisões na BA, sistema de reconhecimento facial é criticado por 'racismo algorítmico'; inocente ficou preso por 26 dias. G1 Bahia, 1 set. 2023. Disponível em: <https://g1.globo.com/ba/bahia/noticia/2023/09/ 01/com-mais-de-mil-prisoes-na-ba-sistema-de-reconhecimento-facial-e-criticado-por-racismo-algoritmico-inocente-ficou-preso-por-26-dias.ghtml>. Acesso em: 10 out. 2025.

ALMEIDA, Eduarda Costa. Os grandes irmãos: o uso de tecnologias de reconhecimento facial para persecução penal. Revista Brasileira de Segurança Pública, São Paulo, v. 16, n. 2, p. 264-283, 2022. DOI: https://doi.org/ 10.31060/rbsp.2022.v16.n2.1377. Acesso em: 18 set. 2025.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 1.515/2022. 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. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2182274&filename=PL%201515/2022>. Acesso em: 16 out. 2025. Texto Original.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 4.939/2020. Dispõe sobre as diretrizes do direito da Tecnologia da Informação e as normas de obtenção e admissibilidade de provas digitais na investigação e no processo, além de outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1936366&filename=PL%204939/2020>. Acesso em: 16 out. 2025. Texto Original.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm> Acesso em: 20 set. 2025.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 22 set. 2025.

BRASIL. Lei nº 12.850, de 02 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em: <https://www.planalto.gov.br/CCivil_03/_Ato2011-2014/2013/Lei/L12850.htm>. Acesso em: 22 set. 2025.

BRASIL. Lei nº 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 22 set. 2025.

BRASIL. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil.

Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105 .htm>. Acesso em: 22 set. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 22 set. 2025.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Disponível em: <https://www.planalto.gov.br/ccivil_ 03/_ato2019-2022/2019/lei/l13964.htm>. Acesso em: 22 set. 2025.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: <https://www.planalto.gov.br/ ccivil_03/leis/l9296.htm>. Acesso em: 22 set. 2025.

BRASIL. Senado Federal. Projeto de Lei nº 2.338/2023. Dispõe sobre o uso da Inteligência Artificial. Disponível em: <https://www25.senado.leg.br/web/atividade/ materias/-/materia/157233> . Acesso em: 16 out. 2025. Texto Original.

BRASIL DE FATO, 6 out. 2023. Argentino preso por reconhecimento facial é solto após erro em sistema de mandado de prisão. Disponível em: <https://odia. ig.com.br/rio-de-janeiro/2024/01/6769179-argentino-preso-por-reconhecimentofacial-e-solto-apos-erro-em-sistema-de-mandado-de-prisao.html>. Acesso em: 12 out. 2025.

CARTA CAPITAL, 19 abr. 2023. Erros em série expõem fragilidade do reconhecimento facial como ferramenta de combate ao crime. Disponível em: <https://www.cartacapital.com.br/tecnologia/erros-em-serie-expoem-fragilidade-dore conhecimento-facial-como-ferramenta-de-combate-ao-crime>. Acesso em: 12 out. 2025.

CIVITARESE, Cristiano Hauck. Inteligência artificial no sistema jurídico brasileiro: fato ou ficção? Revista Processus de Estudos de Gestão, Jurídicos e Financeiros, Brasília, ano 15, v. 15, n. 49, 2024. Disponível em: <https://periodicos.processus. com.br/index.php/egjf/article/view/1234>. Acesso em: 17 set. 2025.

CNN BRASIL, 20 dez. 2024. Condenado após reconhecimento por foto antiga é absolvido pelo STJ. Disponível em: <https://www.cnnbrasil.com.br/nacional/ nordeste/pe/condenado-apos-reconhecimento-por-foto-antiga-e-absolvido-pelo-stj/>. Acesso em: 12 out. 2025.

COIMBRA, Jéssica Pérola Melo et al. Interseções entre racismo algorítmico, reconhecimento facial e segurança pública no Brasil. Revista Jurídica do CESUPA, Belém, v. 4, n. 2, p. 136-160, 2023. Disponível em: <https://periodicos.cesupa.br/ index.php/RJCESUPA/pt_BR/article/view/225>.Acesso em: 20 set. 2025.

G1 RIO, 11 jul. 2019. Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano. Disponível em: <https://g1.globo.com/rj/rio-dejaneiro/noticia/201 9/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detidaporen gano.ghtml>. Acesso em: 12 out. 2025.

LISBOA, M. et al. Desvendando vieses em IA: um estudo sobre reconhecimento facial e futuros feministas. Temáticas, Campinas, v. 33, n. 65, 23 jun. 2025. DOI: 10.20396/tematicas.v33i65.19932. Disponível em: <https://econtents.sbu.unicamp.br/inpec/index.php/tematicas/article/view/19932>. Acesso em: 18 set. 2025.

MARANHÃO, Juliano Souza de Albuquerque et al. Inteligência artificial aplicada ao direito e o direito da inteligência artificial. Suprema – Revista de Estudos Constitucionais, Brasília, v. 1, n. 1, p. 154-180, 2021. DOI: https://doi.org/10.53798/suprema.2021.v1.n1.a20. Acesso em: 14 set. 2025.

O DIA, 4 jan. 2024. RJ: Jovem negro acusado por reconhecimento facial é inocentado pela terceira vez. Disponível em: <https://www.brasildefato.com.br/2023/10/06/rj-jovem-negro-acusado-por-reconhecimento-facial-e-inocentado-pela-terceira-vez>. Acesso em: 12 out. 2025.

PONCE, Paula Pedigoni. Direct and indirect discrimination applied to algorithmic systems: reflections to Brazil. Computer Law & Security Review, v. 48, 2023. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0267364922001091?via%3Dihub>. Acesso em: 18 set. 2025.

SCOPEL, Bruna Gonçalves; PUHL, Eduardo. A tecnologia de reconhecimento facial e sua utilização como prova no processo penal. Academia de Direito, [S.l.], v. 6, p. 3678–3700, 12 dez. 2024. DOI: https://doi.org/10.24302/ acaddir.v6.5587. Acesso em: 18 set. 2025.

SOUZA, Michel R. O.; ZANATTA, Rafael A. F. The Problem of Automated Facial Recognition Technologies in Brazil. Latin American Human Rights Studies, Goiânia, v. 1, p. 1-22, 30 jun. 2021. Disponível em: <https://revistas.ufg.br/lahrs/article/view/69423/36801>. Acesso em: 15 set. 2025.