Scientia et Ratio
ISSN 2525-8532

O USO DA TECNOLOGIA DE RECONHECIMENTO FACIAL NO COMBATE AO CRIME

THE USE OF FACIAL RECOGNITION TECHNOLOGY IN FIGHTING CRIME

Artigo submetido em 15 de junho de 2026
Artigo aprovado em 16 de junho de 2026
Artigo publicado em 16 de junho de 2026

Scientia et Ratio
Volume 6 – Número 10 – 2026
ISSN 2525-8532

.

Autor:
Bruno Henrique Resende Santos[1]
Israel Andrade Alves[2]

.

Resumo: O presente artigo analisa o uso da tecnologia de reconhecimento facial como instrumento de apoio ao combate ao crime, destacando suas potencialidades, limitações e implicações éticas. A expansão dessa tecnologia em centros urbanos tem fortalecido estratégias de segurança pública, principalmente no monitoramento de espaços, identificação de suspeitos e na agilidade de investigações criminais. No entanto, o uso crescente desses sistemas levanta preocupações quanto à proteção da privacidade, à segurança dos dados e aos riscos de discriminação algorítmica, sobretudo quando operados sem transparência ou regulamentação adequada. O objetivo do é estudo compreender como

essa ferramenta pode contribuir para a prevenção e repressão criminal, ao mesmo tempo em que examina os desafios técnicos e sociais relacionados à sua implementação. São discutidos aspectos como precisão dos algoritmos e de gênero, responsabilidade institucional e limites para o uso estatal da vigilância tecnológica. A análise também compara experiências brasileiras e internacionais, demonstrando avanços, controvérsias e práticas recomendadas. Conclui-se que, embora o reconhecimento facial apresente grande potencial para fortalecer políticas de segurança, sua adoção eficiente e legítima depende de marcos regulatórios claros, supervisão e garantias de respeito aos direitos fundamentais, garantindo equilíbrio entre inovação tecnológica e proteção das liberdades individuais.

Palavras-chave: Reconhecimento Facial. Segurança Pública. Tecnologias de Vigilância. Proteção de Dados. Direitos Fundamentais. Inteligência Artificial.

INTRODUÇÃO

Este artigo aborda o uso da tecnologia de reconhecimento facial no combate ao crime. Nesse contexto, a pergunta-problema que orienta o estudo é: como a tecnologia de reconhecimento facial pode contribuir para o combate ao crime no Brasil, considerando seus potenciais benefícios e os riscos relacionados à privacidade, segurança de dados e possíveis discriminações? O objetivo geral consiste em analisar os efeitos e os desafios dessa tecnologia no campo da segurança pública.

Para isso, estabelecem-se como objetivos específicos identificar suas principais aplicações em políticas de segurança, avaliar os impactos positivos na prevenção, investigação e repressão criminal e examinar riscos e limitações associados à privacidade. A justificativa para a escolha do tema baseia-se na expansão do uso de tecnologias digitais pelos órgãos de segurança pública e na crescente adoção do reconhecimento facial como ferramenta de identificação e monitoramento. Embora apresente potencial para aumentar as ações policiais e auxiliar na elucidação de delitos, essa tecnologia também levanta questões éticas, jurídicas

e sociais que precisam ser discutidas, como a proteção de dados pessoais, o perigo de vigilância excessiva e a possibilidade de discriminações algorítmicas.

Além disso, o debate sobre o reconhecimento facial no combate ao crime ganha ainda mais relevância diante da expansão das cidades inteligentes e do aumento da circulação de imagens em espaços públicos e privados. A relação dessa tecnologia a sistemas de videomonitoramento, bancos de dados governamentais e plataformas de análise, aumenta bastante sua capacidade de atuação, mas também exige regulamentação de mecanismos de controle social.

2. O USO DA TECNOLOGIA DE RECONHECIMENTO FACIAL NO COMBATE AO CRIME: REVISÃO NARRATIVA DA LITERATURA

O presente capítulo desenvolve uma revisão narrativa de literatura sobre o uso da tecnologia de reconhecimento facial no combate ao crime, analisando as contribuições científicas tanto no contexto internacional quanto nacional, análise esta que se fundamenta em vinte artigos científicos selecionados, sendo dez provenientes da literatura internacional e dez da literatura nacional, que abordam diferentes aspectos desta tecnologia emergente na segurança pública.

A tecnologia de reconhecimento facial é uma das mais significativas inovações no campo da segurança pública na atualidade, integrando inteligência artificial, visão computacional e biometria para auxiliar as forças policiais na identificação de suspeitos, localização de pessoas desaparecidas e prevenção de crimes. No entanto, sua implementação suscita debates relacionadas aos direitos fundamentais, privacidade, discriminação algorítmica e eficácia operacional, como se passa a expor nos próximos tópicos.

2.1 LITERATURA INTERNACIONAL

A literatura internacional sobre o uso da tecnologia de reconhecimento facial no combate ao

crime apresenta uma rica diversidade de abordagens metodológicas e enfoques teóricos que se desenvolveram ao longo da última década. Tal análise abrange desde desenvolvimentos tecnológicos específicos até reflexões críticas sobre as implicações éticas, legais e sociais desta tecnologia emergente no contexto da segurança pública global.

De fato, o campo do desenvolvimento tecnológico em reconhecimento facial para aplicações de segurança pública tem sido marcado por avanços significativos em algoritmos e arquiteturas de sistemas. Segundo Amshavalli *et al.* (2025), o desenvolvimento e implementação de tecnologia de reconhecimento facial em departamentos policiais é uma das mais promissoras aplicações da visão computacional na segurança pública contemporânea. Os autores destacam que os sistemas modernos integram várias camadas de processamento de imagem, desde a captura inicial até a identificação final, estruturando canais de processamento confiáveis que operam em tempo real.

Archana *et al.* (2024) complementam que a integração de análise facial para prevenção aprimorada de crimes através da combinação de videovigilância e algoritmo *FaceNet* evidencia como as redes neurais profundas podem ser aplicadas efetivamente no contexto de segurança urbana, uma vez que a arquitetura *FaceNet*, baseada em *embeddings* faciais (representações matemáticas de rostos humanos usadas em sistemas de reconhecimento facial), oferece precisão superior na identificação de indivíduos suspeitos em ambientes de vigilância complexos, superando limitações tradicionais relacionadas a variações de iluminação e ângulos de captura.

Não destoa desse entendimento as lições de Okemwa *et al.* (2019), embora os autores apontem que o uso de *Redes Neurais Convolucionais* (CNN), combinadas com classificadores *Histogram of Oriented Gradients* (HOG) para melhorar o reconhecimento de expressões faciais, é talvez o mais significativo avanço metodológico em matéria de reconhecimento facial, pois a combinação dessas técnicas resulta em melhor capacidade de detectar nuances comportamentais que podem indicar intenções criminosas, expandindo o potencial

preventivo da tecnologia além da simples identificação de indivíduos.

Já Godwin (2025) aponta que uma abordagem bimodal para detecção e reconhecimento de faces parcialmente ocluídas para controle de crimes na Nigéria, utilizando algoritmos de aprendizado profundo e aprendizado de máquina, se apresenta como uma inovação fundamental para contextos onde criminosos frequentemente utilizam disfarces. Nesse contexto, o estudo emprega *Deep Learning Multi-Task Cascaded Convolutional Neural Networks* para detecção e alinhamento facial, enquanto arquiteturas *VGG16* são utilizadas para aprendizagem de características e classificação. Os resultados obtidos mostram que as *Redes Neurais Convolucionais* produzem nível de confiança de precisão de reconhecimento de 96% para faces ocluídas, comparado aos métodos tradicionais baseados em HOG.

Por sua vez, Shanthi e Manjula (2025), em uma revisão sistemática sobre técnicas *CNN-YOLO* para detecção de faces e armas na prevenção de crimes. Apontam que a integração de múltiplas modalidades de detecção em um único sistema oferece vantagens operacionais significativas. Os autores destacam que os algoritmos YOLO (*You Only Look Once*) quando combinados com redes convolucionais especializadas em reconhecimento facial, por exemplo, criam sistemas híbridos capazes de identificar simultaneamente indivíduos suspeitos e potenciais ameaças, aumentando a eficácia preventiva das operações de segurança.

Dando seguimento, a eficácia do reconhecimento facial no combate ao crime tem produzido resultados que demonstram, a um só tempo, oportunidades e limitações desta tecnologia, o que também é tratado pela literatura internacional. Segundo Johnson (2024), aplicações policiais de reconhecimento facial e controle de crimes violentos em cidades americanas demonstram que a implementação desta tecnologia pode resultar em reduções estatisticamente significativas nas taxas de criminalidade urbana. A partir de um estudo longitudinal, conduzido em várias cidades norte-americanas, o autor aponta que áreas com implementação de sistemas de reconhecimento facial perceberam reduções de até 15% em

crimes violentos, especialmente roubos e agressões, quando comparadas com áreas de controle sem a tecnologia.

Enquanto isso, Badage *et al.* (2025), em um levantamento sobre técnicas de detecção e prevenção de crimes usando abordagens computacionais modernas, indicam que a integração de variadas modalidades de tecnologias, incluindo reconhecimento facial, computação em nuvem e criptografia *end-to-end* (método de proteção de dados em que somente o remetente e o destinatário de uma mensagem conseguem ler seu conteúdo), corroboram para a criação de um ecossistema de segurança mais eficazes. Em outras palavras, os autores concluíram que sistemas híbridos, que combinam análise facial com detecção de padrões comportamentais e análise preditiva, oferecem resultados superiores na prevenção de incidentes criminosos, com taxas de precisão variando entre 85% e 94% dependendo do contexto operacional, se comparados a usos isolados de tecnologias.

Por sua vez, Rey, Blacaflor e Rey (2022), ao refletirem sobre a adotabilidade de reconhecimento facial de código aberto em sistemas automatizados de identificação criminal para aplicação da lei nas Filipinas, demonstram que mesmo países com recursos limitados podem implementar soluções eficazes utilizando tecnologias abertas. Logo, sugerem que sistemas baseados em arquiteturas de código aberto podem alcançar níveis de precisão comparáveis a soluções comerciais proprietárias, com custos operacionais significativamente menores, tornando a tecnologia mais acessível para departamentos policiais com orçamentos restritivos.

Outra questão relevante abordada pela literatura internacional é a dimensão ética e regulamentar do reconhecimento facial na aplicação da lei, tema que tem recebido crescente atenção acadêmica, especialmente no que se refere às implicações para direitos fundamentais e privacidade.

Nesse cenário, Robles *et al.* (2025), ao abordar perspectivas globais sobre a regulamentação

da utilização de tecnologia de reconhecimento facial para prisões na justiça criminal, chamam a atenção para uma significativa variação jurisdicional nas estratégias regulamentares. Em estudo comparativo entre sistemas legais europeus, americanos e asiáticos, demonstram que não existe consenso internacional sobre os padrões apropriados para governança desta tecnologia, criando um ambiente regulamentar fragmentado que pode comprometer tanto a eficácia operacional quanto a proteção de direitos.

Por sua vez, Kotsoglou *et al.* (2020), em reflexão sobre o "longo braço do algoritmo" e o reconhecimento facial automatizado como evidência e gatilho para intervenção policial, levantam questões relevantes sobre a natureza probabilística dos resultados algorítmicos e sua adequação como base para ações policiais. Os autores argumentam que embora o reconhecimento facial automatizado possa aparecer objetivo e suficiente, isso é contraditório devido à natureza probabilística dos resultados, ao fato de que fabricantes de tecnologia AFR podem definir valores padrão de *threshold* (valor de referência que define um limite entre duas condições) para taxas de falso alarme arbitrariamente, e ao fato de que o usuário final pode alterar esses valores conforme sua preferência, evidenciando a complexidade dos sistemas de reconhecimento facial e a possibilidade de intervenção humana nos resultados.

Por conseguinte, o estudo destaca que o fato de que o olho humano é usado para garantir que uma intervenção seja justificada, foi considerado pelo tribunal como uma salvaguarda importante. Contudo, Kotsoglou *et al.* (2020) questionam a validade desta salvaguarda em circunstâncias onde um oficial em campo é apresentado com uma descoberta do AFR e solicitado a agir baseado nela, especialmente quando decisões sobre os valores incorporados na ferramenta são feitas em outros locais. Ou seja, ao mesmo tempo que a supervisão humana se apresenta benéfica, também pode corroborar para enviesamentos.

Ainda segundo Kotsoglou *et al.* (2020), no contexto de evidências em procedimentos criminais, os meios pelos quais a identificação ocorreu devem ser divulgados à defesa para que o direito o acusado tenha direito a um julgamento justo. E que devem ser

disponibilizadas também informações sobre *matches* desconsiderados e taxas de erro e incertezas do próprio sistema. Para os autores, apenas assim defesa teria a capacidade de efetivamente interrogar o sistema através da testemunha especialista, da mesma forma como interrogariam uma testemunha ocular.

Também se encontra, na literatura internacional, debate sobre o desenvolvimento metodológico no campo do reconhecimento facial para segurança pública, questão que tem sido caracterizada pela crescente sofisticação das abordagens técnicas. Para Badage *et al.* (2025), técnicas como detecção facial usando *MTCNN (Multi-task Cascaded Convolutional Neural Networks*), criptografia *end-to-end* via Protocolo *Signal*, e modelos híbridos *CNN-SVM* para classificação de incidentes têm sido exploradas extensivamente. Os pesquisadores destacam que arquiteturas baseadas em MTCNN oferecem vantagens particulares em cenários de vigilância onde faces podem aparecer em múltiplas orientações e condições de iluminação variáveis.

Ainda segundo Badage *et al.* (2025), a integração de quatro módulos funcionais principais – *Engine de Criptografia End-to-End* (E3), Módulo de Reconhecimento Facial (FRM), Unidade de Classificação Híbrida (HCU), e Camada de Integração Multi-Modal (MMIL) – cria sistemas capazes de operação segura e precisa em tempo real através de ambientes diversos. O módulo E3 implementa o Protocolo Signal com atualizações de chave *Double Ratchet, Curve25519* para troca de chaves, AES-256 para criptografia, e HMAC-SHA256 para integridade de mensagens, garantindo sigilo avançado, confidencialidade de mensagens e resistência a adulteração.

Já Godwin (2025), ao realizar uma comparação entre abordagens de aprendizado profundo e aprendizado de máquina tradicional para detecção de faces parcialmente ocluídas, aponta para a superioridade clara dos métodos baseados em redes neurais profundas. O estudo utilizou *datasets* obtidos de *Disguised Faces in the Wild* junto com dados primários de imagens faciais africanas (ocluídas e não-ocluídas) compreendendo padrões diversos de

oclusão e os resultados mostraram que, enquanto métodos CNN alcançaram 96% de precisão para faces ocluídas, abordagens tradicionais baseadas em HOG com *Support Vector Machine* apresentaram performance significativamente inferior.

Apesar dos avanços, a literatura internacional também identifica limitações significativas e alguns relevantes obstáculos na implementação de sistemas de reconhecimento facial para segurança pública. Para Kotsoglou *et al.* (2020), existem preocupações relevantes sobre a natureza probabilística dos resultados algorítmicos e como estes devem ser interpretados no contexto de tomada de decisões policiais. Os autores argumentam que o reconhecimento facial automatizado pode criar riscos de que descobertas científicas ou algorítmicas usurpem o papel do tomador de decisão legítimo, necessitando o desenvolvimento de mecanismos regulatórios e de transparência para proteger a posição do humano com prerrogativa de tomada de decisão.

Por sua vez, Badage *et al.* (2025) apontam para desafios que ainda persistem, apesar dos avanços inclusive acadêmicos, dentre os quais destacam a latência no processamento de grandes volumes de dados, exposição de metadados, interoperabilidade entre jurisdições, e falta de consciência pública. O estudo por eles apresentado identifica que sistemas de criptografia complexos introduzem latência, especialmente durante transferências de arquivos grandes, enquanto manter sincronização de chaves através de múltiplos dispositivos se mostra difícil. E concluem que características de colaboração em tempo real são prejudicadas devido à segmentação de dados e verificações de segurança.

Não destoa desse entendimento as lições de Archana *et al.* (2024), os quais destacam limitações operacionais como a dependência de condições ambientais adequadas, necessidade de bases de dados extensas para treinamento, e requisitos computacionais significativos para processamento em tempo real. Os pesquisadores observam que performance do sistema pode declinar significativamente em cenários de baixa iluminação ou faces parcialmente obstruídas, limitando a aplicabilidade em certas condições

operacionais.

Em meio a esse cenário de obstáculos relevantes, a literatura internacional também aponta para variações significativas nas abordagens regionais para implementação de tecnologia de reconhecimento facial na segurança pública. Rey, Brancaflor e Rey (2022) observam que o contexto filipino demonstra como países em desenvolvimento podem adaptar tecnologias de reconhecimento facial utilizando soluções de código aberto, superando limitações orçamentárias tradicionais. Para os autores, implementações baseadas em arquiteturas abertas podem alcançar eficácia comparável a sistemas proprietários, oferecendo alternativas viáveis para departamentos com recursos limitados.

Já Robles *et al.* (2025), em uma visão mais global sobre a regulamentação, destacam a exigência de abordagens diversificadas entre diferentes sistemas jurídicos. Eles enfatizam que jurisdições europeias tendem a priorizar proteção de privacidade e direitos fundamentais, enquanto contextos asiáticos frequentemente enfatizam eficácia operacional e segurança pública. Sistemas norte-americanos apresentam abordagem intermediária, buscando equilibrar preocupações de segurança com proteções constitucionais.

Enquanto isso, Godwin (2025), sugere que o cenário nigeriano ilustra desafios específicos enfrentados por países africanos, incluindo limitações infraestruturais, diversidade étnica nas bases de dados de treinamento, e necessidade de adaptação tecnológica para padrões locais de criminalidade. Para o autor, soluções tecnológicas devem ser adaptadas para contextos culturais e operacionais específicos para alcançar eficácia máxima.

Portanto, não há como negar que a literatura internacional evidencia um campo em rápida evolução, caracterizado por avanços tecnológicos significativos acompanhados de crescente sofisticação nas considerações éticas e regulamentares. Os estudos examinados demonstram que enquanto a tecnologia de reconhecimento facial oferece capacidades substanciais para melhoria da segurança pública, sua implementação requer a considerações de vários fatores,

incluindo precisão técnica, proteção de direitos fundamentais, governança apropriada e adaptação a contextos locais específicos, até mesmo porque inexiste regulamentação geral.

2.2 LITERATURA NACIONAL

A literatura nacional sobre o uso da tecnologia de reconhecimento facial no combate ao crime reflete as singularidades do contexto brasileiro, caracterizado por profundas desigualdades sociais, racismo estrutural e um marco regulatório em desenvolvimento. A produção acadêmica brasileira, concentrada entre 2022 e 2025, período selecionado para análise da literatura, aponta preocupações específicas com questões de discriminação algorítmica, violação de direitos fundamentais e a necessidade de regulamentação adequada para esta tecnologia emergente na segurança pública nacional.

De fato, o panorama brasileiro de implementação de tecnologias de reconhecimento facial na segurança pública tem sido marcado por experiências regionais diversificadas, com destaque para os estados da Bahia, Ceará e São Paulo. Segundo Barretto (2024), a relação entre redes de radiocomunicação LTE e prisões por reconhecimento facial no contexto da Secretaria de Segurança Pública da Bahia demonstra como a modernização da infraestrutura de comunicação potencializou significativamente os resultados operacionais na identificação e prisão de foragidos da justiça. Para o referido autor, houve um aumento de 616% nas prisões por reconhecimento facial no período analisado entre 2019 e 2023, além de 71,76% de crescimento nas prisões em eventos carnavalescos após a ativação da rede LTE.

Por sua vez, Silva e Xavier (2025), em análise ao Projeto “Identifica Ceará”, apontam tratar-se de uma das mais ambiciosas políticas públicas de segurança pública de prevenção e combate ao crime no Brasil. Os autores chamam a atenção para o fato de que o sistema em comento integra tecnologias de reconhecimento facial em uma estratégia mais ampla de segurança urbana, destacando que a implementação sistemática desta tecnologia no estado cearense resultou em melhorias mensuráveis nos indicadores de segurança pública,

particularmente na identificação de foragidos e na prevenção de crimes em espaços públicos monitorados.

Já Melo e Serra (2022), ao abordar propostas tecnológicas nas capitais brasileiras, destaca um fenômeno de dispersão da implementação de sistemas de reconhecimento facial, caracterizado pela ausência de coordenação nacional e pela prevalência de soluções fragmentadas desenvolvidas em âmbito municipal e estadual. O estudo em comento sugere que pelo menos quinze capitais brasileiras implementaram ou estavam em processo de implementação de sistemas de reconhecimento facial entre 2019 e 2022, cada uma adotando abordagens tecnológicas e regulamentares distintas.

Nesse contexto, Vieira e Herdman (2024) defendem que a utilização de tecnologias de reconhecimento facial como facilitadores da segurança pública é uma evolução natural dos métodos de identificação criminal no contexto brasileiro. E destacam que estas tecnologias, quando adequadamente implementadas e regulamentadas, podem contribuir significativamente para a melhoria da eficiência investigativa e preventiva das forças policiais, particularmente em contextos urbanos com alta densidade populacional e complexidade criminal.

Porém, a dimensão racial da implementação de tecnologias de reconhecimento facial se apresenta como uma das principais preocupações da literatura nacional brasileira. Conforme Neris (2025), o reconhecimento facial e racismo algorítmico representam desafios centrais na segurança pública brasileira, evidenciando como algoritmos de reconhecimento facial podem perpetuar e amplificar desigualdades raciais preexistentes na sociedade brasileira. O autor demonstra que sistemas de reconhecimento facial apresentam taxas de erro significativamente mais altas para pessoas negras, resultando em identificações equivocadas que contribuem para o encarceramento desproporcional da população afrodescendente.

Semelhantes são as lições de Costa e Kremer (2022), para os quais a inteligência artificial e

discriminação representam desafios estruturais para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial. Para os autores, estas tecnologias afetam desproporcionalmente direitos fundamentais de grupos marginalizados, particularmente pessoas negras e transexuais, criando um ambiente de vigilância opressiva que intensifica contextos de vulnerabilidade social preexistentes.

Já Fagundes e Fernandes (2024), em análise específica do reconhecimento facial pela segurança pública do Estado da Bahia, afirma que a tecnologia opera como instrumento de uma necropolítica. Para os autores, o que seria uma solução para a segurança pública acabou apresentando-se como uma verdadeira ameaça, operando racismo, classicismo, xenofobia e preconceito de gênero como principais resultados dessa investida tecnológica. O estudo demonstra como a má utilização dessas tecnologias pode intensificar políticas de extermínio e vilanização de corpos negros e pobres no território baiano.

Pereira (2025) aborda a questão destacando a dispersão da tecnologia de reconhecimento facial no âmbito da segurança pública brasileira e os sintomas da mescla do urbanismo militar à retórica de guerra preventiva. A autora identifica que a implementação desta tecnologia no Brasil ocorre dentro de uma lógica militarizada de segurança pública que privilegia abordagens repressivas sobre estratégias preventivas e sociais, resultando em um ambiente de vigilância permanente que afeta desproporcionalmente populações vulneráveis.

Há, também, uma preocupação na literatura nacional quanto ao desenvolvimento do marco regulatório nacional para tecnologias de reconhecimento facial, pois o que se vislumbra até hoje são tentativas fragmentadas de regulamentação e ausência de legislação específica em âmbito federal. De acordo com Pontes e Silva (2023), o impacto da tecnologia de reconhecimento facial na eficiência da prova pericial e na garantia dos direitos individuais evidencia conflitos significativos entre eficácia investigativa e proteção de direitos fundamentais. Para os autores, as tecnologias podem tanto aprimorar a qualidade da prova pericial quanto criar riscos substanciais para direitos individuais, particularmente direitos à

privacidade e à não-discriminação.

Macri Júnior, Macri e Frontini (2023), ao tecerem considerações acerca do uso de tecnologias de reconhecimento facial como instrumento de segurança pública, indicam a urgência de regulamentação baseada em princípios de proporcionalidade e necessidade. Defendem a suspensão do uso dos algoritmos de reconhecimento até que sejam supridas deficiências técnicas e regulatórias, argumentando que a ideia de uma moratória enfrenta resistência de um contexto político-criminal caracterizado por crescentes demandas por segurança via expansão dos meios repressivos.

Ainda segundo Macri Júnior, Macri e Frontini (2023), o funcionamento das tecnologias de reconhecimento facial pode resultar em violações significativas de direitos fundamentais, especialmente quando aplicadas no contexto da segurança pública sem salvaguardas adequadas. Desta feita, apontam riscos relacionados à precisão dos algoritmos, potencial para discriminação sistêmica e ausência de transparência nos processos de tomada de decisão algorítmica.

Semelhantes são as lições de Vieira e Herdman (2024), os quais destacam que regulamentação do uso de tecnologias de reconhecimento facial deve pautar-se no equilíbrio entre avanços tecnológicos no direito penal e proteção de direitos constitucionalmente garantidos. E chamam a atenção para a importância do artigo 226 do Código de Processo Penal para estabelecer procedimentos corretos de reconhecimento de pessoas, enquanto analisam o conflito entre o direito à segurança previsto no artigo 5º, inciso XXXIII da Constituição Federal, e direitos à privacidade e intimidade protegidos pelo artigo 5º, inciso X da mesma carta constitucional.

Dando seguimento, a literatura também foca na eficácia operacional das tecnologias de reconhecimento facial. Contudo, não há consenso, pois percebeu-se resultados contraditórios que demonstram, a um só tempo, um cenário de oportunidade e também de relevantes

limitações. Exemplificando, Barretto (2024) aponta que a integração entre tecnologias de videomonitoramento inteligente e redes de banda larga privativas fortalece substancialmente as ações de segurança pública, contribuindo para a captura de criminosos e redução da impunidade. De fato, o autor documenta resultados operacionais expressivos, incluindo milhares de prisões realizadas através de sistemas de reconhecimento facial na Bahia, demonstrando o potencial desta tecnologia para melhorar a eficiência investigativa policial.

Silva e Xavier (2025), considerando o Projeto "Identifica Ceará", como já dito alhures, demonstra como políticas públicas coordenadas podem maximizar os benefícios operacionais de tecnologias de reconhecimento facial, ressaltando que a implementação sistemática e coordenada desta tecnologia, quando combinada com treinamento adequado de pessoal e protocolos operacionais claros, pode resultar em melhorias substanciais na capacidade de identificação de suspeitos e prevenção de crimes em espaços públicos.

Vieira e Herdman (2024) acrescentam que o reconhecimento facial é indubitavelmente um grande avanço em questões de segurança pública, desde que usados de forma equilibrada, oferecendo benefícios substanciais para penalização e reconhecimento correto de indivíduos envolvidos em atividades criminosas. Tais tecnologias, na visão dos autores, podem fornecer formas de prova eficazes que garantam proteção da sociedade, particularmente em contextos de alta criminalidade urbana.

No entanto, conforme Fagundes e Fernandes (2024), os resultados da implementação de sistemas de reconhecimento facial têm sido mais quantitativos que qualitativos, com foco excessivo em números de prisões sem consideração adequada para qualidade das identificações e impactos sociais desproporcionais. Defendem que a ênfase em métricas quantitativas obscurece problemas fundamentais relacionados à precisão dos sistemas e seus efeitos discriminatórios sobre populações vulneráveis.

Exatamente por isso, o que se percebe é a documentação crescente da resistência social e críticas acadêmicas à implementação indiscriminada de tecnologias de reconhecimento facial na segurança pública brasileira. Segundo Melo e Serra (2022), as propostas de gestores públicos municipais apontam claramente um conflito entre demandas por segurança e preocupações com direitos fundamentais, resultando em debates públicos intensos sobre a apropriação social dessas tecnologias. Para os autores, movimentos de resistência civil organizados, incluindo campanhas como “Tire Meu Rosto da Sua Mira”, que advogam pelo banimento total do uso de tecnologias de reconhecimento facial na segurança pública, são um claro exemplo dessa resistência social.

Nesse contexto, Costa e Kremer (2022) chamam a atenção para o fato de que os argumentos pelo banimento de tecnologias discriminatórias ganham força no debate acadêmico e social brasileiro, especialmente em cenários de vulnerabilidade que afetam desproporcionalmente pessoas negras e transexuais. Para os mencionados autores, não são poucos os casos que demonstram aspectos críticos da implementação de tecnologias de reconhecimento facial, argumentando pela necessidade de moratórias ou banimentos em contextos onde a discriminação algorítmica se mostra persistente.

Pereira (2025) apresenta argumentos um pouco diversos, destacando que a retórica de guerra preventiva que caracteriza a implementação de tecnologias de reconhecimento facial no Brasil é reflexo de uma militarização crescente da segurança pública que privilegia soluções tecnológicas sobre abordagens sociais integradas. Para a citada autora, tal estratégia resulta em políticas de segurança que intensificam desigualdades sociais existentes, particularmente afetando populações urbanas marginalizadas.

Neris (2025) complementa que a resistência acadêmica e social às tecnologias de reconhecimento facial no Brasil também se articula em torno de preocupações fundamentais com justiça racial e direitos humanos, o que tem levado organizações da sociedade civil, acadêmicos e ativistas a desenvolver estratégias coordenadas para contestar a

implementação acrítica dessas tecnologias, propondo alternativas que priorizem abordagens de segurança pública baseadas em direitos humanos e justiça social.

Outra questão apontada pela literatura nacional é a diversidade regional na implementação de tecnologias de reconhecimento facial reflete as heterogeneidades do federalismo brasileiro e as diferentes capacidades institucionais dos estados e municípios. Conforme Barretto (2024), a experiência baiana ilustra como Estados com maior capacidade de investimento em infraestrutura tecnológica podem implementar sistemas mais sofisticados, resultando em maior eficácia operacional, mas também em riscos ampliados para direitos fundamentais. De fato, a Bahia investiu milhões de reais na implementação de sistemas integrados que combinam reconhecimento facial com redes de comunicação avançadas.

Já Silva e Xavier (2025) observam o modelo cearense de implementação e enfatizam que a coordenação entre diferentes agências de segurança pública e integração com políticas urbanas mais amplas são fundamentais para o sucesso de programas de reconhecimento facial. E ressaltam que o “Identifica Ceará” é talvez a experiência mais bem-sucedida no que tange as novas tecnologias, pois busca equilibrar eficácia operacional com considerações de direitos humanos, embora ainda enfrente desafios significativos relacionados à transparência e responsabilização.

Melo e Serra (2022), ao comparar algumas capitais brasileiras, apontam padrões heterogêneos de implementação que refletem diferentes prioridades políticas, capacidades técnicas e níveis de resistência social. Apontam que cidades como São Paulo, Rio de Janeiro e Recife desenvolveram abordagens distintas, cada uma enfrentando desafios específicos relacionados à aceitação pública e eficácia operacional, o que apresenta benefícios, mas também evidencia o problema da inexistência de normativas gerais.

Pereira (2025) complementa que as diferenças regionais na implementação de tecnologias de reconhecimento facial também refletem diferentes tradições de policiamento e culturas

institucionais das forças de segurança pública. Logo, Estados com históricos de maior militarização policial tendem a implementar estas tecnologias dentro de ferramentas mais repressivas, enquanto contextos com tradições de policiamento comunitário podem desenvolver abordagens mais participativas.

Ainda, tem-se que a literatura nacional também identifica limitações técnicas significativas que afetam a eficácia e confiabilidade de sistemas de reconhecimento facial no contexto brasileiro. Segundo Pontes e Silva (2023), questões relacionadas à qualidade de bases de dados, calibração de algoritmos para diversidade étnica brasileira e integração com sistemas legados representam desafios técnicos substanciais. Para os autores, muitos sistemas implementados no Brasil utilizam algoritmos desenvolvidos para populações com características étnicas diferentes, resultando em taxas de erro mais altas para a população brasileira.

Macri Júnior, Macri e Frontini (2023) apontam deficiências técnicas como limitações de infraestrutura de conectividade, qualidade inadequada de imagens de vigilância e falta de padronização entre diferentes sistemas implementados por agências distintas, enquanto Neris (2025) destaca as limitações técnicas dos algoritmos de reconhecimento facial são amplificadas no contexto brasileiro devido à diversidade étnica da população e características específicas de iluminação e condições ambientais prevalentes no país.

Por sua vez, Vieira e Herdman (2024) observam a existência de desafios operacionais, dentre os quais incluem necessidade de treinamento especializado para operadores, manutenção adequada de equipamentos e desenvolvimento de protocolos claros para interpretação de resultados algorítmicos. Em outras palavras, na visão dos autores, a eficácia de sistemas de reconhecimento facial depende de fatores humanos e organizacionais que frequentemente recebem atenção inadequada durante processos de implementação.

Por último, mas não menos importante, a literatura nacional se alinha em torno da

necessidade de desenvolvimento de marcos regulatórios específicos e implementação de salvaguardas sólidas e bem fundamentadas para tecnologias de reconhecimento facial na segurança pública brasileira. Macri Júnior, Macri e Frontini (2023) apontam que propostas para regulamentação adequada incluem estabelecimento de princípios de proporcionalidade e necessidade, desenvolvimento de mecanismos de transparência algorítmica e criação de instâncias de supervisão independente, ou seja, a regulamentação deve equilibrar potencialidades de segurança pública com proteção rigorosa de direitos fundamentais.

Costa e Kremer (2022) destacam a necessidade de se priorizar proteção de grupos vulneráveis através de desenvolvimento de tecnologias mais inclusivas, implementação de auditorias regulares de viés algorítmico e criação de mecanismos de recurso para indivíduos afetados por identificações equivocadas. Para tanto, propõem que futuras políticas públicas devem incorporar princípios de justiça racial e equidade social como elementos centrais de design e implementação.

Pontes e Silva (2023) enfatizam que o desenvolvimento de capacidades técnicas nacionais, incluindo pesquisa e desenvolvimento de algoritmos calibrados para a população brasileira e criação de infraestruturas de dados que respeitem privacidade e direitos fundamentais. Logo, sugerem que o Brasil deve investir em desenvolvimento tecnológico autônomo para reduzir dependência de soluções estrangeiras que podem não ser adequadas para o contexto nacional.

Pereira (2025) destaca algumas transformações necessárias, como abordagens militarizadas de segurança pública para modelos baseados em direitos humanos e participação comunitária. Portanto, aponta que as tecnologias de reconhecimento facial podem ser ferramentas úteis para segurança pública apenas quando implementadas dentro de frameworks democráticos que priorizem transparência, responsabilização e proteção de direitos fundamentais.

Resta claro que a literatura nacional aponta para um consenso sobre a necessidade de implementação responsável de tecnologias de reconhecimento facial que considere especificidades do contexto brasileiro. Segundo Barretto (2024), políticas públicas orientadas à inovação tecnológica devem considerar a convergência entre comunicação segura e inteligência artificial como vetor estratégico, mas sempre dentro de contextos que protejam direitos fundamentais e promovam transparência operacional.

Enquanto isso, Silva e Xavier (2025) apontam experiências de sucesso, como a cearense, chamando a atenção para estratégias que coordenam questões técnicas, legais e sociais desde as fases iniciais de planejamento, reforçando o que Vieira e Herdman (2024), preconizam, que é o uso equilibrado de tecnologias de reconhecimento facial, considerando competências técnicas e éticas entre operadores, criação de sistemas de supervisão adequados e estabelecimento de protocolos claros para situações de identificação duvidosa.

Destarte, a literatura nacional brasileira sobre reconhecimento facial na segurança pública evidência um campo em desenvolvimento caracterizado por alguns conflitos entre as demandas por segurança pública e a proteção de direitos fundamentais. Isso se deve ao fato de que, enquanto estas tecnologias oferecem vantagens, principalmente para melhoria da eficácia policial, sua implementação enfrenta obstáculos e desafios, a exemplo do racismo estrutural, das desigualdades sociais e da ausência de marcos regulatórios adequados.

CONCLUSÃO

A literatura internacional e nacional sobre o uso da tecnologia de reconhecimento facial no combate ao crime converge em reconhecer os avanços tecnológicos da ferramenta e seu potencial para aprimorar a segurança pública, ao mesmo tempo em que ressaltam alguns obstáculos éticos, sociais e regulatórios que precisam ser enfrentados. Conforme demonstrado pelos estudos internacionais selecionados, o reconhecimento facial tem se mostrado eficaz para a identificação rápida de suspeitos e a prevenção de crimes, com

destaque para o desenvolvimento de algoritmos avançados baseados em aprendizado profundo, que otimizam a precisão e a capacidade operacional dos sistemas em contextos variados. Contudo, não ignoram os riscos de vieses raciais incorporados nos algoritmos e a necessidade premente de regulamentação clara que equilibre a eficácia com a proteção dos direitos humanos e liberdades fundamentais.

Por sua vez, a literatura brasileira aprofunda essa discussão, contextualizando as especificidades locais, como o racismo estrutural, a desigualdade social e o ambiente político-institucional fragmentado. Em sua maioria apontam que, apesar dos ganhos operacionais observados em Estados como Bahia, Ceará e São Paulo, aqui citados ilustrativamente, a ausência de uma regulamentação federal e a presença de vieses algorítmicos têm provocado sérios impactos sociais, sobretudo sobre grupos vulneráveis, como a população negra e pessoas trans, levando a reconhecer que o uso da tecnologia na segurança pública precisa ser mediado por princípios éticos, jurídicos e sociais claros que minimizem riscos de discriminação e garantam amplos mecanismos de revisão e supervisão.

REFERENCIAL BIBLIOGRÁFICO

a. Referencial internacional padrão ABNT

1. AMSHAVALLI, M. *et al.* Development and Implementation of Face Recognition Technology in The Police Department. **International Research Journal of Advanced Engineering and Management** (IRJAEM), v. 3, n. 05, 2025. Disponível em: https://goldncloudpublications.com/index.php/irjaem/article/view/1024. Acesso em: 2 out. 2025.
2. ARCHANA, M. *et al.* Leveraging Facial Analytics for Enhanced Crime Prevention: Integrating Video Surveillance and FaceNet Algorithm. In: **International Conference on Pervasive Computing and Social Networking** (**ICPCSN**), n. 4, p. 503-509, 2024. Disponível em: https://ieeexplore.ieee.org/document/10607383. Acesso em: 2 out. 2025.

3. BADAGE, A. *et al.* A Survey on Crime Detection and Prevention Techniques using Modern Computational Approaches. International **Journal for Research in Applied Science & Engineering Technology** (IJRASET), v. 13, n. IX, 2025. Disponível em: https://www.ijraset.com/best-journal/a-survey-on-crime-detection-and-prevention-techniques-using-modern-computational-approaches. Acesso em: 2 out. 2025.
4. GODWIN, O. A Bimodal Approach for Partially Occluded Face Detection and Recognition for Crime Control in Nigeria Using Deep Learning and Machine Learning Algorithms**. Must Journal of Research and Development** (MJRD), v. 6, n. 2, 2025. Disponível em: https://mjrd.must.ac.tz/index.php/mjrd/article/view/233. Acesso em: 2 out. 2025.
5. JOHNSON, T. L. Police facial recognition applications and violent crime control in U.S. cities. **Cities**, v. 155, 2024. Disponível em: https://www.sciencedirect.com/science/article/pii/S0264275124006863. Acesso em: 2 out. 2025.
6. KOTSOGLOU, K. N. *et al.* The long arm of the algorithm? Automated Facial Recognition as evidence and trigger for police intervention. **Forensic Science International: Synergy**, v. 2, p. 86–89, 2020. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC7219190/. Acesso em: 2 out. 2025.
7. OKEMWA, J. G. *et al.* Using CNN and HOG Classifier to Improve Facial Expression Recognition. **International Journal for Research in Applied Science & Engineering Technology** (IJRASET), v. 7, n. VI, 2019. Disponível em: https://www.ijraset.com/fileserve.php?FID=23995. Acesso em: 2 out. 2025.
8. REY, W.; BLANCAFLOR, E.; REY, K. W. J. D. Adoptability of Open-Source Face Recognition (FR) on Automated Criminal Identification System for Law Enforcement in the Philippines: A Systematic Review. IEEE **Conference Publication**. Disponível em: https://ieeexplore.ieee.org/document/10071202. Acesso em: 2 out. 2025.
9. ROBLES, P. *et al.* Global perspectives on regulating facial recognition technology utilization for criminal justice arrests. **Global Public Policy and Governance**, v. 5, p. 186–204, 2025. Disponível em:

https://link.springer.com/article/10.1007/s43508-025-00117-9. Acesso em: 02 out. 2025.

10. SHANTHI, P.; MANJULA, V. A systematic review on CNN-YOLO techniques for face and weapon detection in crime prevention. Discover Computing, v. 28, art. 204, 2025. Disponível em: https://link.springer.com/article/10.1007/s10791-025-09715-x. Acesso em: 2 out. 2025.

- Referencial nacional padrão ABNT
- BARRETTO, Ubiraci Alves Muniz. Redes de radiocomunicação LTE e as prisões por reconhecimento facial: Um estudo de caso da Secretaria de Segurança Pública da Bahia. **Revista do Instituto Brasileiro de Segurança Pública (RIBSP**), v. 7, n. 19, p. 67-80, 2024. Disponível em: https://revista.ibsp.org.br/index.php/RIBSP/article/view/232. Acesso em: 2 out. 2025.
- COSTA, Ramon Silva; KREMER, Bianca. Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial. **Revista Brasileira de Direitos Fundamentais & Justiça,** v. 16, n. 1, 2022. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/1316. Acesso em: 2 out. 2025.
- FAGUNDES, Bárbara D.'angeles Alves; FERNANDES, Patrick Wendell Teixeira. Os "novos olhos" da segurança pública da Bahia: ruídos de uma necropolítica nos programas de reconhecimento facial. **Direito & TI**, v. 1, n. 18, p. 39-58, 2024. Disponível em: https://direitoeti.com.br/direitoeti/article/view/160. Acesso em: 2 out. 2025.
- MACRI JÚNIOR, José Roberto; MACRI, Bianka Jaquetti; FRONTINI, Helena. Considerações acerca do uso de tecnologias de reconhecimento facial como instrumento de segurança pública. **Revista Científica Integrada**, v. 6, n. 1, 2023. Disponível em: https://revistas.unaerp.br/rci/article/view/3102. Acesso em: 2 out. 2025.
- MELO, Paulo Victor; SERRA, Paulo. Tecnologia de reconhecimento facial e segurança pública nas capitais brasileiras: apontamentos e problematizações. **Comunicação e Sociedade**, n. 42, p. 205-220, 2022. Disponível em: https://journals.openedition.org/cs/8111. Acesso em: 2 out. 2025.

- NERIS, Roberto Cezar Marcelino. Reconhecimento facial e racismo algorítmico: os desafios na segurança pública brasileira – Inteligência artificial aplicada: soluções para um mundo automatizado. **Científica Digital**, p. 125-144, 2025. Disponível em: https://downloads.editoracientifica.com.br/articles/250519437.pdf. Acesso em: 2 out. 2025.
- PEREIRA, Letícia Pádua. Dispersão da tecnologia de reconhecimento facial no âmbito da segurança pública brasileira: sintomas da mescla do urbanismo militar à retórica de guerra preventiva. **Res Severa Verum Gaudium**, v. 10, n. 1, p. 65-91, 2025. Disponível em: https://seer.ufrgs.br/resseveraverumgaudium/article/view/145963. Acesso em: 2 out. 2025.
- PONTES, Marco Aurelio Muniz de; SILVA, Diogo Severino Ramos da. O impacto da tecnologia de reconhecimento facial na eficiência da prova pericial e na garantia dos direitos individuais. **Derecho y Cambio Social**, v. 20, n. 71, 2023. Disponível em: https://derechoycambiosocial.org/index.php/revista/article/view/2835. Acesso em: 2 out. 2025.
- SILVA, Lucas Lucena da; XAVIER, Antônio Roberto. O Projeto "Identifica Ceará" como política pública de segurança pública de prevenção e combate ao crime. **Revista Políticas Públicas & Cidades,** v. 14, n. 4, p. e2001-e2001, 2025. Disponível em: https://journalppc.com/RPPC/article/view/2001. Acesso em: 2 out. 2025.
- VIEIRA, Marcio de Souza; HERDMAN, Eleandro. A utilização de tecnologias de reconhecimento facial como facilitadores da segurança pública. **Caderno Pedagógico**, v. 21, n. 10, p. e9721-e9721, 2024. Disponível em: https://ojs.studiespublicacoes.com.br/ojs/index.php/cadped/article/view/9721. Acesso em: 2 out. 2025.

---

[1] Graduando em Direito pela Faculdade Serra do Carmo – FASEC. Email: **brunoresende26@icloud.com.**

[2] Professor da Faculdade de Direito Serra do Carmo – FASEC. Mestre em Direitos Humanos e Prestação Jurisdicional pela UFT/ESMAT. Pós graduado em Direito Público pela PUC Minas. Delegado de Polícia Civil do Estado do Tocantins. Email: prof.israelalves@fasec.edu.br