

RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA: PROPOSTA DE UM APLICATIVO BASEADO EM EMBEDDINGS PARA IDENTIFICAÇÃO DE INDIVÍDUOS EM TEMPO REAL

Fábio Silva Calheiros da Rosa (PM5)

<https://orcid.org/0009-0000-9899-7395>

E-mail: fabio.silval@pm.al.gov.br

DOI-Geral: <http://dx.doi.org/10.47538/RA-2026.V5N1>

DOI-Individual: <http://dx.doi.org/10.47538/RA-2026.V5N1-77>

RESUMO: A modernização da segurança pública exige a adoção de ferramentas que otimizem o tempo de resposta e a precisão nas ações policiais. O presente artigo discute a implementação de uma solução tecnológica móvel para a Polícia Militar de Alagoas (PMAL), visando a identificação instantânea de indivíduos durante abordagens policiais. Atualmente, a verificação de antecedentes criminais depende majoritariamente da consulta via rádio à central de operações, um processo sujeito a congestionamento de rede, ruídos de comunicação e dependência de terceiros. Como alternativa, propõe-se o desenvolvimento de um aplicativo de captura de imagens faciais integrado a um servidor de processamento biométrico baseado em *embeddings* (vetores numéricos). Esta arquitetura centralizada permite que a análise computacional mais crítica seja realizada remotamente, garantindo agilidade e precisão na comparação de faces contra um banco de dados de procurados, sem sobrecarregar os dispositivos móveis dos policiais. O estudo demonstra que essa ferramenta confere maior autonomia ao agente na ponta, reduz o tempo de abordagem e mitiga erros causados por falsidade ideológica, onde suspeitos fornecem dados verbais ou documentos inconsistentes. Conclui-se que a adoção desta tecnologia não apenas agiliza o fluxo operacional, mas também aumenta a segurança da guarnição e a efetividade no cumprimento de mandados de prisão.

PALAVRAS-CHAVE: Segurança Pública. Reconhecimento Facial. Embeddings. Policiamento Inteligente. PMAL.

FACIAL RECOGNITION IN PUBLIC SAFETY: PROPOSAL FOR AN EMBEDDINGS-BASED APPLICATION FOR REAL-TIME INDIVIDUAL IDENTIFICATION

ABSTRACT: The modernization of public safety requires the adoption of tools that optimize response time and precision in police actions. This article discusses the implementation of a mobile technological solution for the Military Police of Alagoas (PMAL), aiming for the instantaneous identification of individuals during police stops. Currently, criminal background checks rely mostly on radio consultations with the operations center, a process subject to network congestion, communication noise, and dependence on third parties. As an alternative, the development of a facial image capture application integrated with a biometric processing server based on embeddings (numerical vectors) is proposed. This centralized architecture allows the most critical computational analysis to be performed remotely, ensuring speed and accuracy in comparing faces against a database of wanted persons without overloading the officers'

mobile devices. The study demonstrates that this tool provides greater autonomy to the agent on the front line, reduces stop-and-search time, and mitigates errors caused by false identity, where suspects provide inconsistent verbal data or documents. It is concluded that the adoption of this technology not only streamlines the operational flow but also increases the safety of the police squad and the effectiveness in executing arrest warrants.

KEYWORDS: Public Safety. Facial Recognition. Embeddings. Smart Policing. PMAL.

INTRODUÇÃO

A segurança pública no Brasil atravessa um momento de profunda transformação, impulsionada pela necessidade de integrar inteligência e tecnologia às rotinas operacionais. No estado de Alagoas, a Polícia Militar (PMAL) tem buscado constantemente a modernização de seus processos para enfrentar uma criminalidade cada vez mais dinâmica e organizada. O conceito de *Intelligence-Led Policing* (Policimento Orientado pela Inteligência) deixa de ser apenas uma tendência teórica para se tornar uma necessidade imperativa na gestão da segurança pública. Neste cenário, a eficiência na ponta da linha — onde o policial interage diretamente com o cidadão e o infrator — torna-se o fiel da balança para o sucesso das operações.

Atualmente, um dos momentos mais críticos da atividade policial ostensiva é a abordagem e a subsequente identificação de indivíduos em atitude suspeita. O fluxo padrão adotado pela PMAL, assim como na maioria das corporações nacionais, baseia-se na consulta de antecedentes criminais via rádio à Central de Operações (COPOM/CIOPS). Embora funcional historicamente, este modelo apresenta gargalos operacionais severos que comprometem a celeridade da ação policial. Em horários de pico ou durante grandes operações, o congestionamento dos canais de rádio, a interferência na comunicação, a filtragem da informação e a dependência da disponibilidade de operadores na central podem gerar um tempo de espera significativo. Cada minuto aguardando um retorno via rádio representa um período em que a guarnição permanece estática e exposta, reduzindo a capilaridade do patrulhamento e aumentando o risco à segurança da equipe.

Além da questão temporal, o método tradicional de consulta verbal possui vulnerabilidades intrínsecas. A verificação baseia-se majoritariamente em dados alfanuméricos fornecidos pelo próprio abordado (nome, filiação, data de nascimento).

Criminosos contumazes frequentemente decoram dados de terceiros ou apresentam documentos falsificados com alta qualidade, ludibriando a consulta via rádio que, por sua natureza, não dispõe de meios visuais imediatos para confirmação. Sem a biometria, a validação da identidade torna-se subjetiva e suscetível a erros, permitindo que foragidos da justiça sejam liberados por falta de uma verificação mais robusta no local da abordagem.

Neste contexto, a tecnologia de reconhecimento facial móvel surge como uma ferramenta estratégica para mitigar essas vulnerabilidades. A proposta deste artigo é apresentar uma solução baseada em aplicativo para smartphones, capaz de realizar a identificação biométrica de indivíduos em tempo real, descentralizando o acesso à informação. Diferente de sistemas estáticos de videomonitoramento, o foco aqui é empoderar o policial na rua com a capacidade de verificar a identidade de um suspeito através da captura de sua face, comparando-a instantaneamente com um banco de dados de procurados.

A viabilidade técnica desta proposta apoia-se no uso de embeddings — vetores numéricos que representam as características faciais únicas de um indivíduo. Esta abordagem centraliza o processamento pesado em um servidor dedicado, permitindo que a comparação (matching) seja realizada com extrema velocidade e precisão, sem exigir hardware de ponta nos dispositivos móveis dos policiais. Além disso, o uso de algoritmos de compressão de imagem garante que o tráfego de dados permaneça eficiente, adequando-se à realidade de conectividade móvel em diversas regiões do estado de Alagoas. O objetivo deste trabalho, portanto, é demonstrar como essa arquitetura tecnológica pode ser implementada na PMAL, analisando seus benefícios operacionais, a redução do tempo de resposta e o aumento na efetividade do cumprimento de mandados de prisão, consolidando a tecnologia como um vetor de eficiência na segurança pública alagoana.

REFERENCIAL TEÓRICO

A fundamentação deste estudo perpassa três eixos centrais: a evolução do policiamento orientado por inteligência, a arquitetura técnica do reconhecimento facial

via *embeddings* e os aspectos legais que regem o uso de dados biométricos na segurança pública.

TECNOLOGIA E SEGURANÇA PÚBLICA: O PARADIGMA DA INTELIGÊNCIA

A complexidade da criminalidade moderna exige que as instituições de segurança pública transitem de um modelo puramente reativo para um modelo proativo e preditivo. Nesse contexto, o conceito de *Intelligence-Led Policing* (Policimento Orientado pela Inteligência) consolida-se como uma doutrina fundamental. Segundo Ratcliffe (2003), este modelo propõe que a análise de dados e a inteligência criminal devem guiar as operações policiais, otimizando a alocação de recursos e a tomada de decisão.

A tecnologia atua, portanto, como um “multiplicador de força”. Na realidade operacional da Polícia Militar de Alagoas (PMAL), onde o efetivo precisa cobrir vastas áreas territoriais, a capacidade de obter informações precisas em tempo real é estratégica. A substituição gradual de processos analógicos — como a consulta de indivíduo via rádio, sujeita a ruídos e delays — por soluções digitais integradas permite que o policial na ponta da linha tenha acesso ao mesmo nível de informação que um analista do serviço de inteligência no quartel. A mobilidade trazida pelos smartphones e aplicativos transforma cada viatura em um nó de rede conectado, capaz de consultar bancos de dados criminais instantaneamente, reduzindo a impunidade decorrente da falta de identificação imediata.

BIOMETRIA FACIAL E A TECNOLOGIA DE EMBEDDINGS

O reconhecimento facial é uma tecnologia biométrica que mapeia características faciais a partir de uma fotografia ou vídeo. No entanto, para a aplicação em dispositivos móveis com limitações de processamento e conectividade, a arquitetura do sistema é determinante. É crucial distinguir dois modos de operação: a *verificação* (1:1), onde se compara uma face com outra específica (como no desbloqueio de um celular), e a *identificação* (1:N), onde uma face é comparada contra um banco de dados com milhares de registros de procurados.

A viabilidade técnica da solução proposta neste artigo reside no uso de embeddings (vetores de características). Esta abordagem, consolidada por trabalhos seminais como o FaceNet (Schroff; Kalenichenko; Philbin, 2015), propõe o mapeamento direto de imagens faciais para um espaço Euclidiano compacto, onde as distâncias correspondem diretamente à similaridade facial. Diferente de sistemas antigos que comparavam imagens pixel a pixel — o que exigiria alto poder computacional e tráfego de dados pesado —, a tecnologia atual utiliza Redes Neurais Convolucionais (CNNs) para converter a imagem da face em uma sequência numérica única (vetor de 128 ou 512 dimensões).

O processo ocorre em três etapas principais:

1. **Deteção e Alinhamento:** O algoritmo localiza a face na imagem e ajusta sua geometria (rotação, escala).

2. **Extração de Características:** A rede neural analisa a face e gera um vetor numérico (o *embedding*) que representa matematicamente as características únicas daquele indivíduo (distância entre os olhos, formato do queixo etc.).

3. **Matching (Comparação):** O sistema compara esse vetor numérico com os vetores armazenados no banco de dados de procurados.

A grande vantagem operacional desta arquitetura para a PMAL é a centralização da inteligência computacional. Ao transferir o processamento pesado (extração de características e cálculo de distância euclidiana) para o servidor, reduz-se a exigência de hardware nos smartphones dos policiais, permitindo o uso de aparelhos intermediários. Além disso, o envio da imagem pode ser otimizado via algoritmos de compressão, garantindo que o tráfego de dados via rede móvel (3G/4G) permaneça eficiente, mesmo em áreas do interior do estado com cobertura oscilante. Dessa forma, o sistema garante que a abordagem policial não seja prejudicada pela latência da rede ou pela falta de capacidade de processamento local.

ASPECTOS LEGAIS, ÉTICOS E A LGPD

A implementação de tecnologias de reconhecimento facial na segurança pública deve observar rigorosamente os preceitos legais, especialmente no que tange à Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018). Embora a LGPD preveja exceções para o tratamento de dados com fins exclusivos de segurança pública e defesa nacional (Art. 4º, III), isso não isenta o Estado da responsabilidade de garantir a integridade, a confidencialidade e a finalidade específica dos dados coletados.

É imperativo que a ferramenta seja desenhada como um sistema de apoio à decisão, e não de decisão autônoma. O aplicativo deve alertar sobre uma possível correspondência (*match*) com um grau de similaridade (ex: 90%), cabendo ao policial realizar a verificação final documental e contextual. Isso mitiga o risco de “viés algorítmico” e falsos positivos, que podem ocorrer devido a fatores como iluminação precária ou similaridade física entre indivíduos. A tecnologia, portanto, não substitui o tirocínio policial, mas o qualifica, oferecendo uma camada adicional de verificação que a visão humana, por si só, não conseguiria processar em larga escala.

METODOLOGIA E PROPOSTA DE SOLUÇÃO

CLASSIFICAÇÃO DA PESQUISA

A presente pesquisa classifica-se como aplicada, de natureza exploratória e propositiva. O objetivo central não é apenas compreender um fenômeno, mas propor uma solução tecnológica concreta para um problema operacional identificado na Polícia Militar de Alagoas (PMAL). O método adotado baseia-se na revisão bibliográfica sobre *Intelligence-Led Policing* e tecnologias de reconhecimento facial, seguida pela modelagem conceitual de um sistema móvel. A proposta busca integrar conceitos teóricos de segurança pública com a arquitetura de sistemas distribuídos, visando a otimização do processo de identificação de indivíduos em campo.

ARQUITETURA DA SOLUÇÃO PROPOSTA

A solução tecnológica proposta consiste em um ecossistema móvel integrado, estruturado em uma arquitetura Cliente-Servidor, composta por três módulos principais:

1. **Módulo Cliente (Aplicativo Móvel):** Desenvolvido para smartphones (Android/iOS), este módulo é a interface do policial na ponta da linha. Sua função primária é a captura da imagem facial e o envio seguro para o servidor, atuando como um terminal de coleta de dados biométricos em campo.

2. **Módulo Servidor (API e Motor de Matching):** Uma API REST segura que recebe as requisições dos dispositivos móveis contendo as imagens capturadas em campo. O servidor hospeda o motor de reconhecimento facial, responsável por processar a imagem recebida, extrair o embedding (vetor de características) e compará-lo instantaneamente com os vetores armazenados no banco de dados de procurados. Este processamento centralizado permite maior robustez computacional, escalabilidade e atualizações constantes dos algoritmos sem necessidade de alterar o aplicativo nos celulares.

3. **Banco de Dados de Vetores:** Diferente de um banco de dados tradicional de imagens, este repositório armazena apenas os *embeddings* (vetores numéricos) gerados a partir das fotos de indivíduos com mandados de prisão em aberto. Isso garante maior segurança (pois a reconstrução da face a partir do vetor é complexa) e extrema velocidade na busca (indexação vetorial).

FLUXO OPERACIONAL DA ABORDAGEM POLICIAL

A implementação desta tecnologia pode alterar significativamente o *modus operandi* da abordagem policial, introduzindo uma etapa de verificação biométrica ágil. O fluxo operacional proposto segue as seguintes etapas:

1. **Abordagem e Suspeita Fundada:** O policial identifica um indivíduo em atitude suspeita e realiza a abordagem padrão de segurança.

2. **Captura da Imagem:** Caso a abordagem leve a um desdobramento de consulta à pessoa, utilizando o aplicativo no smartphone, o policial captura uma fotografia do rosto

do abordado. O sistema orienta o enquadramento correto e verifica a qualidade da imagem (iluminação, foco) para garantir a precisão da análise.

3. **Envio e Processamento no Servidor:** O aplicativo envia a imagem capturada e otimizada para o servidor central via conexão segura (4G/3G/Wi-Fi).

4. **Extração de Características e Matching:** No servidor, o algoritmo de reconhecimento facial processa a imagem recebida, extrai o *embedding* (vetor numérico único) e realiza a comparação imediata com os vetores armazenados no banco de dados de procurados.

5. **Retorno e Decisão:** Em segundos, o servidor devolve a resposta ao aplicativo:

a. **Match Positivo:** O sistema alerta sobre uma possível correspondência, exibindo a foto de cadastro do procurado, nome, mandado de prisão e grau de similaridade (ex: 98%). Cabe ao policial comparar visualmente a foto do sistema com o indivíduo abordado para confirmar a identidade, aliado a outros elementos que confirmem a ocorrência.

b. **Match Negativo:** O sistema informa que não foram encontradas correspondências no banco de dados de procurados.

6. **Ação Policial:** Confirmada a identidade e a vigência do mandado, o policial efetua a prisão e conduz o indivíduo à delegacia, anexando o relatório gerado pelo aplicativo ao Boletim de Ocorrência.

REQUISITOS DE SEGURANÇA, AUDITORIA E INTEGRAÇÃO

Para garantir a integridade do processo e a conformidade com a legislação vigente (LGPD), a solução deve implementar rigorosos protocolos de segurança:

- **Criptografia Ponta-a-Ponta:** Toda a comunicação entre o aplicativo e o servidor deve ser criptografada (TLS/SSL), impedindo a interceptação de dados sensíveis.
- **Autenticação e Controle de Acesso:** O acesso ao aplicativo deve ser restrito a policiais em serviço, mediante login individual e senha (ou biometria do próprio policial).

- **Trilha de Auditoria (Logs):** O sistema deve registrar automaticamente todas as consultas realizadas: quem pesquisou (ID do policial), quando (data/hora), onde (geolocalização GPS) e qual foi o resultado. Isso inibe o uso indevido da ferramenta para fins pessoais ou não autorizados.
- **Integração com Sistemas Legados:** A solução deve prever APIs de integração com os sistemas de gestão de ocorrências da PMAL e com o Banco Nacional de Mandados de Prisão (BNMP) do CNJ, garantindo que a base de dados de procurados esteja sempre atualizada em tempo real.

RESULTADOS ESPERADOS E DISCUSSÃO

A implementação da solução de reconhecimento facial móvel proposta neste estudo tem o potencial de gerar impactos profundos e imediatos na rotina operacional da Polícia Militar de Alagoas. A análise dos resultados esperados baseia-se na comparação direta entre o fluxo atual (analógico/via rádio) e o fluxo proposto (digital/biométrico).

REDUÇÃO DRÁSTICA DO TEMPO DE RESPOSTA

O indicador mais tangível de sucesso é a redução do tempo médio de identificação de indivíduos procurados. Atualmente, uma consulta via rádio ao COPOM/CIOPS pode levar alguns minutos, dependendo do tráfego de voz e da disponibilidade de operadores. Em grandes eventos ou em situações críticas, esse tempo pode ser ainda maior, gerando filas de espera na rede de rádio.

Com a solução proposta, estima-se que o ciclo completo — da captura da foto ao retorno do servidor — ocorra em menos de 30 segundos, mesmo considerando a latência de redes móveis 3G/4G. Essa agilidade transforma a dinâmica da abordagem: o que antes era um “gargalo” que prendia a guarnição no local, passa a ser um procedimento instantâneo. Isso libera a viatura mais rapidamente para o patrulhamento preventivo, aumentando a ostensividade da polícia nas ruas.

AUTONOMIA E DESCONGESTIONAMENTO DO COPOM

Ao descentralizar a consulta para a ponta da linha (o smartphone do policial), a solução retira uma carga significativa de trabalho dos operadores do COPOM. O rádio, que é um recurso crítico e finito, fica liberado para comunicações de emergência e coordenação tática, sua verdadeira finalidade.

Essa autonomia empodera o policial. Ele não precisa mais “pedir permissão” ou aguardar na fila para saber quem está abordando. A informação chega diretamente à sua mão, permitindo uma tomada de decisão baseada em dados (Intelligence-Led Policing) e não apenas na intuição ou na disponibilidade de terceiros.

MITIGAÇÃO DA FALSIDADE IDEOLÓGICA

Um dos maiores desafios da abordagem policial é a identificação de indivíduos que mentem o nome ou apresentam documentos falsos. O método tradicional de consulta textual (nome/mãe/nascimento) é vulnerável a essas fraudes. Se o suspeito fornecer o nome de um irmão sem passagens (“laranja”), o sistema via rádio retornará “nada consta”, e o indivíduo será liberado indevidamente.

A biometria facial elimina essa vulnerabilidade. O rosto é uma chave única que não pode ser esquecida, trocada ou falsificada facilmente em uma abordagem de rua. Ao comparar a face diretamente com o banco de mandados, o sistema ignora o nome fornecido verbalmente e foca na identidade biológica. Espera-se, portanto, um aumento significativo no cumprimento de mandados de prisão de foragidos que hoje circulem livremente usando identidades falsas.

SEGURANÇA DA GUARNIÇÃO

Há uma máxima na atividade policial: “tempo parado é tempo exposto”. Quanto mais tempo uma guarnição permanece estática em via pública aguardando o retorno de uma consulta via rádio, maior é o risco que está correndo, não podendo ser descartadas situações como tentativa de resgate do abordado ou hostilidade popular. Ao reduzir o tempo de verificação de minutos para segundos, a tecnologia contribui diretamente para

a segurança física dos policiais, permitindo que a abordagem seja concluída de forma célere e técnica.

VIABILIDADE ECONÔMICA E ESCALABILIDADE

Diferente de soluções que exigem a compra de *hardwares* proprietários caros (como óculos inteligentes ou câmeras corporais com processamento local), a arquitetura proposta utiliza os smartphones já existentes ou modelos intermediários de mercado. O processamento pesado fica no servidor (nuvem ou data center da PMAL), o que barateia o custo por ponta. Isso torna o projeto altamente escalável: para incluir os policiais no sistema, basta instalar o aplicativo e conceder acesso, sem necessidade de adquirir novos equipamentos de alta performance.

CONCLUSÃO

A modernização da segurança pública no estado de Alagoas passa, inevitavelmente, pela integração de inteligência e tecnologia às rotinas operacionais da Polícia Militar. O presente estudo demonstrou que a adoção de uma solução móvel de reconhecimento facial, baseada na arquitetura cliente-servidor e no uso de *embeddings*, não é apenas tecnicamente viável, mas estrategicamente imperativa para o enfrentamento da criminalidade moderna.

Ficou evidente que o modelo tradicional de verificação de antecedentes — dependente da comunicação via rádio e da identificação verbal — apresenta gargalos operacionais severos. A lentidão na resposta do COPOM, a vulnerabilidade a dados falsos fornecidos por suspeitos e a exposição prolongada das guarnições durante as abordagens são problemas que podem ser mitigados com a tecnologia proposta. Ao descentralizar o acesso à informação, transformando o smartphone do policial em uma ferramenta de biometria avançada, a instituição ganha em celeridade e precisão.

A análise técnica revelou que a centralização do processamento pesado em servidores dedicados permite superar as limitações de hardware dos dispositivos móveis e a instabilidade das redes de dados em áreas remotas. O uso de algoritmos de compressão

de imagem e a comparação vetorial no *backend* garantem que a resposta chegue à ponta da linha em segundos, conferindo autonomia decisória ao agente de segurança.

Conclui-se, portanto, que a implementação desta ferramenta representa um salto qualitativo para a PMAL. Mais do que agilizar o fluxo de trabalho, ela potencializa a capacidade de *Intelligence-Led Policing*, permitindo que cada abordagem seja guiada por dados concretos e não apenas pela intuição. Para trabalhos futuros, sugere-se a expansão do banco de dados para incluir não apenas mandados de prisão, mas também registros de pessoas desaparecidas e integração com bases civis de identificação, consolidando um ecossistema de segurança pública verdadeiramente integrado e eficiente a serviço da sociedade alagoana.

REFERÊNCIAS

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 16 fev. 2026.

RATCLIFFE, Jerry H. **Intelligence-led policing.** Canberra: Australian Institute of Criminology, 2003. (Trends & issues in crime and criminal justice, n. 248). Disponível em: <https://www.aic.gov.au/publications/tandi/tandi248>. Acesso em: 16 fev. 2026.

SCHROFF, Florian; KALENICHENKO, Dmitry; PHILBIN, James. **FaceNet: A Unified Embedding for Face Recognition and Clustering.** In: IEEE CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION (CVPR), 2015, Boston. *Proceedings...* Boston: IEEE, 2015. p. 815-823.

Submissão: outubro de 2025. Aceite: novembro de 2025. Publicação: fevereiro de 2026.