v7.n5.2026

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

DISCUSSÃO SOBRE RECONHECIMENTO FACIAL EM LARGA ESCALA UTILIZANDO REDES NEURAIS PROFUNDAS NO SISTEMA SADE – PMPR

DISCUSSION ON LARGE-SCALE FACIAL RECOGNITION USING DEEP NEURAL NETWORKS IN THE SADE SYSTEM – PMPR

DISCUSIÓN SOBRE RECONOCIMIENTO FACIAL A GRAN ESCALA UTILIZANDO REDES NEURONALES PROFUNDAS EN EL SISTEMA SADE - PMPR

Raquel Figueiredo Martins[1]

e757704
https://doi.org/10.47820/recima21.v7i5.7704

PUBLICADO: 05/2026

RESUMO

Este artigo apresenta um estudo metodológico e experimental sobre o uso de técnicas de reconhecimento facial baseadas em aprendizado profundo em um cenário hipotético inspirado em sistemas institucionais de segurança pública, com foco na possível integração de um módulo biométrico ao SADE (Sistema de Atendimento e Despacho de Emergências) da Polícia Militar do Estado do Paraná como ferramenta de apoio à decisão. Em contraste com abordagens orientadas à implantação imediata, o estudo busca examinar criticamente a viabilidade técnica, os limites operacionais e as implicações éticas, jurídicas e organizacionais associadas ao emprego dessa tecnologia em contextos sensíveis. Os resultados mostram que o sistema desenvolvido foi capaz de organizar um espaço de *embeddings* faciais com poder discriminativo consistente, indicando que o desempenho nas tarefas de identificação depende diretamente da quantidade e da diversidade de imagens disponíveis por identidade na galeria. Nas avaliações de verificação, observou-se que configurações de segurança mais restritivas reduzem a ocorrência de falsos positivos, mas aumentam as taxas de rejeição de indivíduos genuínos. Esse resultado reforça que métricas agregadas de acurácia, quando consideradas isoladamente, não são suficientes para validar o uso da tecnologia em aplicações policiais. Do ponto de vista metodológico, o estudo contribui ao descrever um pipeline reprodutível para organização dos dados, treinamento do modelo, geração de *embeddings* e avaliação experimental. Com base nos resultados, entende-se que uma eventual integração ao SADE deve ser concebida como um serviço probabilístico de triagem, sempre submetido à supervisão humana, à auditabilidade dos processos, à governança institucional e à proteção dos direitos fundamentais.

PALAVRAS-CHAVE: Reconhecimento facial. Segurança Pública. Sistema SADE.

ABSTRACT

This article presents a methodological and experimental study on the use of deep learning-based facial recognition techniques in a hypothetical scenario inspired by institutional public security systems, focusing on the possible integration of a biometric module into SADE (Emergency Response and Dispatch System) of the Military Police of Paraná as a decision-support tool. In contrast to approaches aimed at immediate deployment, the study critically examines the technical feasibility, operational limitations, and ethical, legal, and organizational implications associated with the use of this technology in sensitive contexts. The results show that the developed system was able to organize a facial embedding space with consistent discriminative power, indicating that performance in identification tasks depends directly on the quantity and

---

[1] Tecnóloga em Inteligência Artificial, Universidade Cruzeiro do Sul, São Paulo-SP, Brasil. Quadro de Praças da Polícia Militar do Estado Paraná, Cornélio Procópio, Paraná, Brasil.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

diversity of images available for each identity in the gallery. In verification evaluations, stricter security settings were found to reduce false positives, but also to increase the rejection rates of genuine individuals. This finding reinforces that aggregated accuracy metrics, when considered in isolation, are insufficient to validate the use of this technology in police applications. From a methodological perspective, the study contributes by describing a reproducible pipeline for data organization, model training, embedding generation, and experimental evaluation. Based on the findings, any potential integration into SADE should be conceived as a probabilistic screening service, always subject to human oversight, process auditability, institutional governance, and the protection of fundamental rights.

KEYWORDS: *Facial recognition. Public security. SADE system.*

RESUMEN
Este artículo presenta un estudio metodológico y experimental sobre el uso de técnicas de reconocimiento facial basadas en aprendizaje profundo en un escenario hipotético inspirado en sistemas institucionales de seguridad pública, con énfasis en la posible integración de un módulo biométrico al SADE (Sistema de Atención y Despacho de Emergencias) de la Policía Militar de Paraná como herramienta de apoyo a la toma de decisiones. A diferencia de los enfoques orientados a la implementación inmediata, el estudio busca examinar críticamente la viabilidad técnica, los límites operativos y las implicaciones éticas, jurídicas y organizacionales asociadas al uso de esta tecnología en contextos sensibles. Los resultados muestran que el sistema desarrollado fue capaz de estructurar un espacio de embeddings faciales con un poder discriminativo consistente, lo que indica que el desempeño en las tareas de identificación depende directamente de la cantidad y diversidad de imágenes disponibles por identidad en la galería. En las evaluaciones de verificación, se observó que configuraciones de seguridad más restrictivas reducen la ocurrencia de falsos positivos, pero aumentan las tasas de rechazo de individuos genuinos. Este resultado refuerza que las métricas agregadas de precisión, cuando se consideran de forma aislada, no son suficientes para validar el uso de esta tecnología en aplicaciones policiales. Desde el punto de vista metodológico, el estudio contribuye al describir un pipeline reproducible para la organización de los datos, el entrenamiento del modelo, la generación de embeddings y la evaluación experimental. Con base en los resultados, se entiende que una eventual integración al SADE debe concebirse como un servicio probabilístico de cribado, siempre sometido a supervisión humana, auditabilidad de los procesos, gobernanza institucional y protección de los derechos fundamentales.

PALABRAS CLAVE*: Reconocimiento facial. Seguridad pública. Sistema SADE.*

INTRODUÇÃO

O reconhecimento facial, definido como a capacidade de identificar ou verificar a identidade de uma pessoa a partir de imagens de seu rosto, é uma das aplicações mais proeminentes da inteligência artificial (Thorat, Nayak e Dandale, 2010). Tecnologias como estas são baseadas em aprendizado profundo e vêm sendo amplamente pesquisadas e aplicadas em diferentes setores, desde autenticação de dispositivos pessoais até segurança em eventos públicos e sistemas de vigilância (Brandner, 2023).

Vale ressaltar que, quando inserido no campo da segurança pública, o debate deixa de ser exclusivamente técnico. A discussão não se limita à melhoria de métricas de acurácia, mas

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

envolve também questões normativas e sociais, especialmente aquelas relacionadas à privacidade, aos direitos fundamentais e à responsabilidade institucional.

Operacionalmente o sistema de reconhecimento biométrico poderá reduzir fases nas etapas investigativas as quais dependem de procedimentos manuais, como a identificação de suspeitos em imagens de câmeras ou registros fotográficos. Entretanto, a aplicação em contextos reais traz à tona preocupações relevantes, sobretudo quanto ao desempenho em ambientes não controlados, à presença de vieses demográficos e à proteção de dados pessoais (Almeida *et al.*, 2021).

Para lidar com a modernização das instituições de segurança do Brasil, em 2018 foi instituída a Política Nacional de Segurança Pública e Defesa Social, Lei nº 13.675, que tem, como um de seus objetivos, "incentivar medidas para modernização de equipamentos, da investigação e da perícia e para a padronização de tecnologia de órgãos e das instituições de segurança pública" (BRASIL, 2018).

Com isso, os sistemas de informação que oferecem suporte à atividade no âmbito da segurança pública vêm sendo modernizados ao longo das últimas décadas. Um exemplo dessa evolução é o Sistema de Atendimento e Despacho de Emergências (SADE), uma infraestrutura tecnológica que articula fluxos de dados e procedimentos em operações da Polícia Militar do Estado do Paraná, desde o registro de ocorrência até a consulta às bases institucionais, integrando assim ferramentas que auxiliam a tomada de decisão do efetivo da Polícia Militar do Paraná em campo. Miranda e Lima (2023) discutem a melhora na eficiência da segurança pública com a implementação do SADE, que com dados de três batalhões da Polícia Militar do Paraná, notaram, além de um ganho significativo no tempo de deslocamento das viaturas policiais até os locais de ocorrências, uma qualidade considerável no atendimento e produção de documentação do registro do ocorrido.

No entanto, o SADE ainda não integra nativamente ferramentas baseadas em reconhecimento facial. Essa ausência está relacionada a obstáculos técnicos e institucionais. A confiabilidade diante de imagens degradadas, a robustez a variações de pose, iluminação e a mitigação de vieses são desafios concretos. Além disso, a integração dessa tecnologia exige atenção a aspectos jurídicos e éticos, como proteção de dados pessoais, transparência no uso de algoritmos e garantia de não discriminação.

Experiências internacionais recentes demonstram que a utilização inadequada de sistemas automatizados em segurança pública pode produzir consequências graves. Relatórios do *Center on Privacy & Technology*, da *Georgetown University*, e investigações jornalísticas publicadas pelo *The Washington Post* documentam casos de reconhecimento facial que

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

resultaram em identificações incorretas e prisões injustas (CENTER ON PRIVACY & TECHNOLOGY, 2025; THE WASHINGTON POST, 2025). Em diversos episódios, a saída do sistema foi tratada como evidência conclusiva, sem validação humana adequada ou contextualização investigativa. Esses casos indicam que a avaliação da tecnologia não pode se restringir ao desempenho algorítmico, devendo considerar também seus efeitos institucionais e sociais.

Atualmente, a Secretaria de Estado da Segurança Pública do Paraná, integra os seguintes órgãos como a Polícia Militar do Estado Paraná (PMPR), a Polícia Civil do Estado do Paraná (PCPR), Polícia Científica do Estado do Paraná (PCIPR), Polícia Penal do Estado do Paraná (PPPR) e Corpo de Bombeiros Militar do Estado do Paraná (CBMPR), os quais utilizam-se deste sistema de consulta da Secretaria de Segurança Pública do Paraná (SESP), sistema este que possui acervo de registros e fotografias de indivíduos com mandado de prisão em aberto, pessoas foragidas do sistema prisional e antecedentes criminais, o que possivelmente poderia servir de base de dados para treinamento de algoritmos de Aprendizagem de Máquina no reconhecimento facial dos indivíduos supracitados. Baseado na Lei nº 13.675/2018 a qual abre espaço para o uso de novas tecnologias digitais e sistemas de informação como apoio à segurança, faz-se necessário fomentar a discussão e análise de como esta integração poderia ocorrer.

Embora o reconhecimento facial baseado em aprendizado profundo tenha apresentado avanços significativos nos últimos anos, sua aplicação em contextos de segurança pública ainda envolve limitações técnicas, operacionais, éticas e jurídicas que impedem sua adoção acrítica como ferramenta decisória. No caso do SADE da Polícia Militar do Estado do Paraná, permanece em aberto o problema de como um módulo biométrico dessa natureza poderia ser integrado de maneira tecnicamente viável, institucionalmente governável e juridicamente compatível com a proteção de direitos fundamentais, especialmente em situações de abordagem policial, nas quais erros de identificação podem gerar consequências graves.

O objetivo geral deste artigo é analisar, de forma metodológica e crítica, a possibilidade de integração de um módulo de reconhecimento facial ao SADE como ferramenta de apoio à decisão, considerando simultaneamente sua viabilidade técnica, seus limites operacionais e suas implicações éticas, jurídicas e institucionais. Para isso, propõe-se a construção e avaliação de um pipeline experimental capaz de simular, em cenário hipotético de funcionamento dessa tecnologia em atividades relacionadas à segurança pública.

Como objetivos específicos, o estudo busca: estruturar um pipeline reprodutível para organização dos dados, treinamento do modelo e geração de *embeddings* faciais; avaliar

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

experimentalmente o desempenho do sistema em tarefas de identificação e verificação facial; analisar a relação entre desempenho, quantidade e diversidade de imagens por identidade na galeria; examinar os efeitos de diferentes configurações de segurança sobre a ocorrência de falsos positivos e rejeições indevidas; e discutir, à luz dos resultados obtidos, as condições institucionais, éticas e jurídicas necessárias para uma eventual incorporação dessa tecnologia ao contexto operacional do SADE.

A realização deste estudo justifica-se pela necessidade de produzir evidências técnicas e reflexão crítica sobre o uso de reconhecimento facial em sistemas institucionais de segurança pública, especialmente dentro do contexto da Política Nacional de Segurança Pública e Defesa Social que assim estabelece princípios e objetivos modernizadores na gestão de segurança, contudo ainda carece de análise rigorosa quanto aos seus impactos e limites. Dessa forma, o artigo procura contribuir para o debate sobre o emprego responsável da inteligência artificial na atividade policial, oferecendo subsídios tanto para a pesquisa acadêmica quanto para a formulação de critérios de governança, supervisão humana e proteção de direitos no uso dessa tecnologia.

1. REFERENCIAL TEÓRICO

O reconhecimento facial consolidou-se como um dos eixos centrais da visão computacional contemporânea, especialmente a partir da difusão das redes neurais convolucionais profundas (CNNs). Até o início da década de 2010, predominavam abordagens baseadas em projeções lineares, como *Eigenfaces* e *Fisherfaces*, bem como em descritores manuais, como *Local Binary Patterns*. Embora esses métodos apresentassem desempenho satisfatório em ambientes controlados, revelavam limitações significativas diante de variações de pose, iluminação, oclusão e expressão facial, características inerentes a cenários reais de captura de imagem (KISHORE, 2025).

A incorporação de arquiteturas profundas treinadas em bases de dados de larga escala representou uma inflexão metodológica no campo. O trabalho *DeepFace*, proposto por Taigman *et al.* (2014), demonstrou de forma consistente que redes profundas poderiam alcançar desempenho comparável ao humano em tarefas de verificação facial, utilizando treinamento supervisionado em grandes conjuntos de dados. Em seguida, *FaceNet*, de Schroff *et al.* (2015), consolidou o paradigma baseado em *embeddings* (representações numéricas de baixa dimensionalidade de dados de alta dimensionalidade), ao propor um modelo que aprende representações vetoriais diretamente otimizadas por funções de perda métricas, estruturando o

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

espaço de características de modo a aproximar amostras da mesma identidade e afastar identidades distintas. No mesmo período, *Deep Face Recognition*, de Parkhi, Vedaldi e Zisserman (2015), evidenciou a eficácia de arquiteturas profundas treinadas em bases extensas para tarefas tanto de verificação quanto de identificação. Esses trabalhos estabeleceram as bases do paradigma contemporâneo, no qual representações discriminativas são aprendidas diretamente a partir dos dados brutos, reduzindo a dependência de engenharia manual de atributos.

A ampliação do uso de bases massivas e diversificadas reforçou a importância da variabilidade intraindivíduo para a generalização dos modelos. Conjuntos de dados como o VGGFace2 evidenciaram que variações de idade, pose, iluminação e contexto desempenham papel decisivo na robustez dos sistemas, sobretudo em cenários não controlados (Cao *et al.*, 2018). A partir desse ponto, o avanço do estado da arte passou a concentrar-se não apenas no aprofundamento arquitetural das redes, mas também no desenvolvimento de funções de perda capazes de estruturar geometricamente o espaço de *embeddings* faciais. Entre essas contribuições, destaca-se a *ArcFace*, proposta por Deng *et al.* (2019), que introduz uma margem angular explícita entre classes, promovendo maior separabilidade entre identidades no espaço vetorial. A formulação mostrou-se particularmente eficaz em tarefas de reconhecimento facial em larga escala, tornando-se referência tanto em pesquisas acadêmicas quanto em aplicações industriais.

Quando considerada a natureza institucional das aplicações no setor da segurança pública um falso positivo em reconhecimento facial não constitui um mero erro estatístico; pode desencadear abordagens indevidas, constrangimentos ilegais ou até prisões injustas. Jain, Ross e Prabhakar (2004) advertem que sistemas biométricos com alta acurácia global pode apresentar comportamento insatisfatório quando submetidos a limiares de segurança mais rigorosos, exigidos em contextos forenses e governamentais.

Simultaneamente às discussões técnicas, intensificou-se o debate ético e jurídico sobre o uso de reconhecimento facial por órgãos de segurança pública. Introna e Wood (2004) argumentam que tecnologias biométricas não são neutras, uma vez que incorporam pressupostos sociais e políticos tanto em sua concepção quanto em sua aplicação. Estudos mais recentes evidenciam a presença de vieses algorítmicos relacionados à raça, gênero e faixa etária, indicando maior suscetibilidade de determinados grupos a erros de identificação. Avaliações independentes conduzidas pelo *National Institute of Standards and Technology* (NIST) corroboram essas preocupações ao demonstrar disparidades estatísticas em sistemas comerciais amplamente utilizados (Grother, Ngan e Hanaoka, 2019).

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Quando se examinam aplicações concretas no policiamento, a literatura internacional apresenta resultados heterogêneos. Alguns estudos relatam ganhos operacionais em tarefas de triagem e investigação preliminar; outros, entretanto, documentam falhas significativas em implantações reais, sobretudo na ausência de protocolos claros de validação humana e auditoria contínua (Garvie, Bedoya e Frankle, 2016). Tais evidências reforçam a compreensão de que o reconhecimento facial, em contextos institucionais, deve ser concebido como ferramenta de apoio à decisão, e não como mecanismo autônomo de imputação de identidade ou responsabilidade.

A literatura recente converge, portanto, para a necessidade de avaliações que ultrapassem métricas tradicionais de acurácia e incorporem análises de risco, viés, robustez e impacto social. A adoção de uma perspectiva multidimensional torna-se indispensável para examinar não apenas o desempenho técnico dos sistemas, mas também as condições sob as quais seu uso pode ser considerado legítimo e proporcional. É nesse ponto de interseção entre desenvolvimento tecnológico e responsabilidade institucional que o presente trabalho se situa, propondo uma investigação experimental em larga escala articulada a uma reflexão crítica sobre os limites e implicações do reconhecimento facial no contexto do policiamento contemporâneo.

2. METODOLOGIA

2.1. Formulação do problema

O problema abordado neste artigo insere-se no contexto do reconhecimento facial biométrico em larga escala, com foco tanto na identificação quanto na verificação facial, em um cenário hipotético inspirado em sistemas institucionais de segurança pública. Diferentemente de aplicações restritas a ambientes controlados, considera-se aqui um cenário de abordagem de suspeitos durante o patrulhamento ostensivo das radiopatrulhas, no qual imagens faciais podem apresentar grande variabilidade de pose, iluminação, qualidade e contexto de captura.

Formalmente, seja $B = \{i_1, i_2, ..., i_N\}$ o conjunto de identidades cadastradas em um banco institucional. Para cada identidade $i_k \in B$, existe um conjunto de imagens de referência (galeria) $G_{ik} = \{x_{k1}, x_{k2}, ..., x_{km}\}$, onde m representa o número de imagens cadastradas para aquela identidade. Dada uma imagem de consulta x_q, o sistema deve produzir uma das seguintes saídas:

• Identificação: determinar se x_q pertence a alguma identidade $i_k \in B$ e, em caso afirmativo, retornar o identificador correspondente;

• Verificação: decidir se duas imagens (x_a, x_b) pertencem ou não à mesma identidade;

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

• Rejeição: indicar que a imagem de consulta não corresponde a nenhuma identidade cadastrada no banco.

Essas decisões são baseadas em uma função de extração de características (*embedding*) definida como:

$$f_\theta : \mathbb{R}^{H \times W \times C} \rightarrow \mathbb{R}^d,$$

em que f_θ representa uma rede neural profunda parametrizada por θ, $H \times W \times C$ são as dimensões da imagem de entrada e $d = 512$ é a dimensionalidade do espaço vetorial aprendido. Os vetores de saída são normalizados pela norma L_2, de modo que:

$$\hat{z} = \frac{f_\theta(x)}{\|f_\theta(x)\|_2},$$

permitindo o uso direto da similaridade cosseno como medida de proximidade entre duas representações:

$$s(\hat{z}_a, \hat{z}_b) = \hat{z}_a^{\top} \hat{z}_b.$$

No caso da identificação, a similaridade entre a imagem de consulta e cada identidade do banco é calculada a partir de representações agregadas da galeria, sendo a decisão final condicionada a um limiar τ. Esse limiar desempenha papel central no controle do compromisso entre falsos positivos e falsos negativos, aspecto particularmente crítico em aplicações de segurança pública.

É importante destacar que, embora o treinamento do modelo seja conduzido em regime *closed-set*, no qual todas as identidades do conjunto de teste estão presentes no treinamento, a avaliação considera explicitamente cenários compatíveis com uso institucional, nos quais a rejeição de consultas e o controle rigoroso de erros são fundamentais. Essa distinção metodológica permite estabilizar o aprendizado do espaço vetorial sem comprometer a análise crítica dos riscos associados ao uso do sistema.

2.2. Metodologia adotada

A metodologia deste trabalho foi estruturada com foco em reprodutibilidade, dentro das limitações computacionais e de armazenamento. O *pipeline* completo compreende as etapas de organização dos dados, treinamento do modelo, geração de *embeddings* e avaliação por protocolos específicos de identificação e verificação.

2.2.1. Base de dados e organização experimental

Foi utilizado o conjunto de dados *VGGFace2*, amplamente empregado na literatura de reconhecimento facial devido à sua elevada variabilidade intraindivíduo e grande número de

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

identidades. Para viabilizar os experimentos em ambiente computacional doméstico e permitir controle rigoroso dos protocolos, adotou-se um subconjunto de 3.000 identidades, com até 30 imagens por identidade, totalizando aproximadamente 90.000 imagens.

A organização do banco de dados foi realizada por meio de arquivos CSV contendo, para cada amostra, o identificador da identidade e o caminho relativo da imagem. A divisão foi realizada de forma estratificada por identidade, garantindo que, para cada indivíduo, um subconjunto fixo de imagens fosse reservado exclusivamente para avaliação, com o objetivo de prevenir o vazamento entre treino e teste.

2.2.2. Arquitetura do modelo

O modelo de reconhecimento facial foi baseado em uma arquitetura de aprendizado profundo composta por três componentes principais:

Rede base (*backbone*) convolucional: foi utilizada a *ResNet-18*, inicializada com pesos pré-treinados no *ImageNet*. Essa escolha reflete um compromisso deliberado entre capacidade representacional e custo computacional, alinhado ao objetivo de estudar cenários realistas de implantação institucional.

Camada de projeção (*embedding*): uma camada linear responsável por mapear as ativações finais do *backbone* para um espaço vetorial de dimensão 512, seguida de normalização *L2*.

Cabeça de classificação (*classification head*) ArcFace: empregada exclusivamente durante o treinamento, introduzindo uma margem angular aditiva entre identidades, de modo a reforçar a separação geométrica no espaço de *embeddings*.

Os algoritmos foram desenvolvidos em *PyTorch*, *framework* escolhido por sua flexibilidade, transparência e ampla adoção na comunidade científica. Na Tabela 1 abaixo, constam os parâmetros da configuração dos experimentos.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Tabela 1. Parâmetros de Configuração do Modelo

Backbone	*ResNet-18*
Embedding	512
Otimizador	*AdamW*
Loss	*ArcFace*
Dimensão	512
Dimensão do Banco de Dados	3000 IDs x 30 Imagens
Épocas	50
Batch size	128
Hardware	RTX 3050 6GB
Framework	*PyTorch*

2.2.3. Treinamento do modelo

O treinamento foi conduzido em regime *closed-set*, utilizando a perda *ArcFace*, com otimização via AdamW e estratégias de regularização adequadas para evitar sobreajuste. O processo foi implementado de modo a controlar o carregamento dos dados, aplicação de aumentos simples (*data augmentation*), atualização dos pesos e salvamento de checkpoints.

A escolha pelo regime *closed-set* foi deliberada, pois esse protocolo de treinamento, em que as identidades presentes no conjunto de treino são as mesmas daquele utilizado durante a fase inicial de avaliação, favorece a aprendizagem estável de um espaço vetorial discriminativo. Essa decisão metodológica está em consonância com a literatura especializada, que observa que a capacidade de lidar com identidades não vistas (*open-set*) é, em geral, tratada principalmente na fase de inferência e de avaliação, sendo um desafio distinto do treinamento *closed-set* (SU *et al.,* 2024).

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

2.2.4. Geração de *embeddings*

Após o treinamento, os *embeddings* faciais foram gerados utilizando exclusivamente o *encoder* do modelo, sem a cabeça ArcFace, garantindo que a avaliação fosse baseada apenas nas representações vetoriais aprendidas.

Essa separação explícita entre treinamento e inferência foi essencial para evitar vazamentos de avaliação e assegurar que os resultados obtidos refletissem o comportamento real do sistema em um cenário operacional.

2.2.5. Protocolos de avaliação

A avaliação foi dividida em dois eixos complementares:

- Identificação: mensurada por métricas *Top-1*, *Top-5* e *Top-10*, considerando diferentes tamanhos de galeria (número de imagens por identidade), de modo a analisar o impacto da quantidade de referências no desempenho do sistema.
- Verificação: avaliada por meio de curvas *ROC*, *AUC*, *Equal Error Rate (EER)* e *TARFAR*, utilizando amostragem controlada de pares genuínos e impostores.

Esses protocolos possibilitaram uma análise aprofundada dos *trade-offs* operacionais (ou seja, das relações de compensação inevitáveis entre métricas concorrentes, como redução de falsos positivos e aumento de falsos negativos), especialmente em cenários configurados com critérios de segurança mais rigorosos. Nesses regimes restritivos, pequenas variações no limiar de decisão podem produzir alterações substanciais nas taxas de erro, impactando diretamente o equilíbrio entre sensibilidade e especificidade do sistema.

2.3. Considerações metodológicas finais

A metodologia adotada neste trabalho não tem como objetivo maximizar métricas isoladas de desempenho, mas sim compreender os limites, riscos e implicações práticas de um sistema de reconhecimento facial quando considerado como possível módulo de apoio à decisão em um contexto policial. Ao conectar escolhas técnicas, protocolos experimentais e análise crítica, o estudo busca fornecer subsídios sólidos para discussões futuras sobre a viabilidade, a responsabilidade e a governança do uso de reconhecimento facial em sistemas institucionais.

3. RESULTADOS

Os resultados experimentais apresentados nesta seção têm como objetivo avaliar de forma abrangente o comportamento do sistema de reconhecimento facial desenvolvido,

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

contemplando tanto cenários de identificação quanto de verificação. A análise combina métricas quantitativas consolidadas na literatura com representações gráficas que favorecem uma interpretação mais intuitiva do desempenho do modelo, sempre considerando as implicações práticas e institucionais associadas à aplicação dessa tecnologia em contextos de segurança pública.

Todos os experimentos foram conduzidos exclusivamente no espaço de *embeddings* faciais extraídos pelo *encoder* do modelo previamente treinado, de modo que os resultados reflitam fielmente o comportamento do sistema em fase de inferência. A separação rigorosa entre treinamento e avaliação foi essencial para prevenir vazamentos de informação (*data leakage*) entre os conjuntos de dados e, assim, assegurar a validade metodológica e científica dos resultados apresentados.

3.1. Resultados de identificação facial

A tarefa de identificação foi avaliada por meio das métricas denominadas *Top-1*, *Top-5* e *Top-10*, que indicam se a identidade correta aparece, respectivamente, na primeira posição, entre as cinco primeiras ou entre as dez primeiras posições do ranking de candidatos retornados pelo sistema. Em outras palavras, o *Top-1* mede se o sistema acerta exatamente a primeira sugestão, enquanto o *Top-5* e o *Top-10* verificam se a pessoa correta está entre as principais hipóteses apresentadas. As avaliações foram realizadas considerando diferentes quantidades de imagens por identidade na galeria (conjunto de referência previamente cadastrado). Esse protocolo simula cenários institucionais nos quais uma imagem de consulta deve ser associada à identidade correta dentro de um banco de dados existente.

Os resultados indicam que, com cinco imagens por identidade na galeria, o sistema alcançou aproximadamente 58% de acerto em *Top-1*, isto é, identificou corretamente a pessoa já na primeira posição em mais da metade dos casos. Quando se considera a presença da identidade correta entre as cinco primeiras posições (*Top-5*), a taxa de acerto sobe para cerca de 72%, alcançando aproximadamente 78% quando se analisam as dez primeiras posições (*Top-10*). Esses resultados demonstram que, embora o sistema nem sempre classifique corretamente a identidade como sua primeira escolha, ela tende a aparecer com elevada frequência entre as primeiras posições do ranking, que se configura como uma característica particularmente relevante em aplicações de triagem, nas quais o sistema atua como ferramenta de apoio à decisão humana.

Em contraste, quando a galeria foi reduzida para apenas uma imagem por identidade, observou-se uma queda substancial de desempenho: o *Top-1* foi reduzido para

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

aproximadamente 39%, enquanto o *Top-10* situou-se em torno de 61%. Esse comportamento evidencia de forma clara a dependência do desempenho em relação à representatividade da galeria, corroborando achados amplamente discutidos na literatura de reconhecimento facial, segundo os quais múltiplas amostras por identidade tendem a melhorar a robustez e a estabilidade do processo de identificação (Min, Flynn e Bowyer, 2003).

Tais informações podem ser visualizadas nas Tabelas 2 abaixo.

Tabela 2. Resumo dos principais resultados experimentais

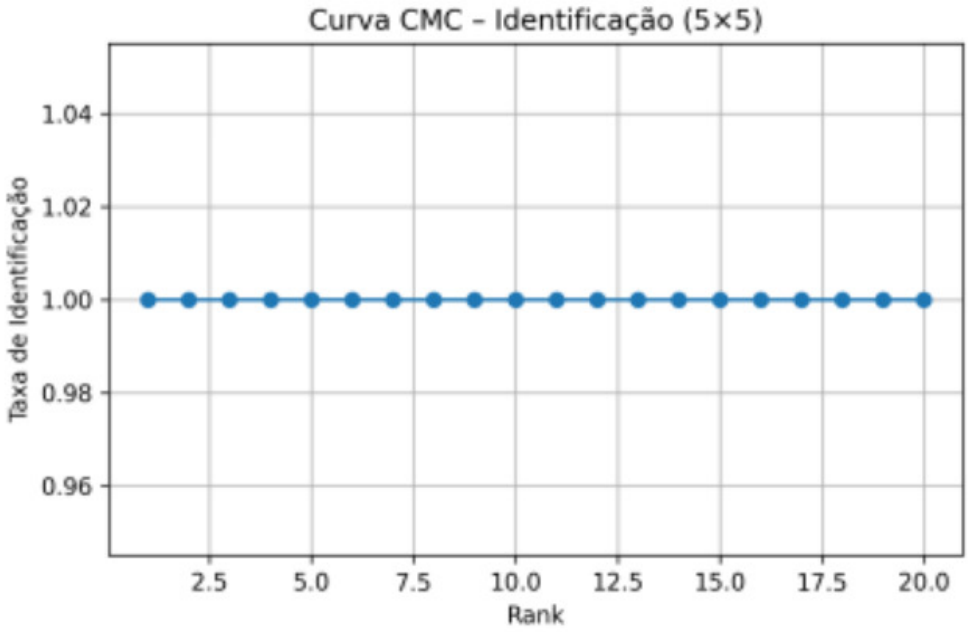
Métrica	Valor
Número de identidades	3000
Dimensão do *embedding*	512
Top-1 (galeria 5 imagens)	0.585
Top-5 (galeria 5 imagens)	0.727
Top-10 (galeria 5 imagens)	0.778
Top-1 (galeria 1 imagem)	0.390
AUC (verificação)	0.941
EER	0.125
TAR @ *FAR* = 10e−2	0.699
TAR @ *FAR* = 10e−3	0.524
TAR @ *FAR* = 10e−4	0.351

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

3.2. Análise da curva *CMC*

A *Curva Cumulative Match Characteristic* (CMC) foi utilizada para analisar de forma mais detalhada o desempenho do sistema no modo de identificação, considerando um protocolo com múltiplas imagens por identidade tanto na galeria quanto na consulta.

Figura 1. Curva CMC para identificação facial no protocolo 5×5



A Figura 1 apresenta a curva CMC referente ao cenário em que foram utilizadas cinco imagens por identidade tanto na galeria quanto no conjunto de consulta, totalizando 3.000 identidades avaliadas. Nessa configuração experimental, a taxa de identificação aproxima-se de 100% já na primeira posição do *ranking*, mantendo-se praticamente constante nas posições seguintes. Em termos práticos, isso indica que, nesse protocolo específico, a identidade correta é recuperada como principal correspondência na quase totalidade das consultas realizadas.

Esse desempenho sugere que, quando múltiplas imagens representativas estão disponíveis para cada identidade, as representações aprendidas pelo modelo se organizam de maneira estável no espaço de *embeddings*. A presença de diferentes amostras por classe tende a reduzir os efeitos da variabilidade intra-classe, decorrente de alterações de pose, iluminação ou expressão facial, e a aumentar a proximidade entre vetores pertencentes à mesma identidade,

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

ao mesmo tempo em que preserva distâncias adequadas em relação às demais. O resultado é uma separação mais consistente entre identidades distintas no espaço vetorial normalizado.

Cabe ressaltar, entretanto, que essa configuração corresponde a uma condição favorável de avaliação. Em contextos operacionais nos quais o cadastro facial se limita a poucas imagens ou apresenta menor diversidade amostral, o desempenho observado pode não se repetir na mesma proporção, o que exige análise cuidadosa e contextualizada dos resultados.

3.3. Impacto do tamanho da galeria

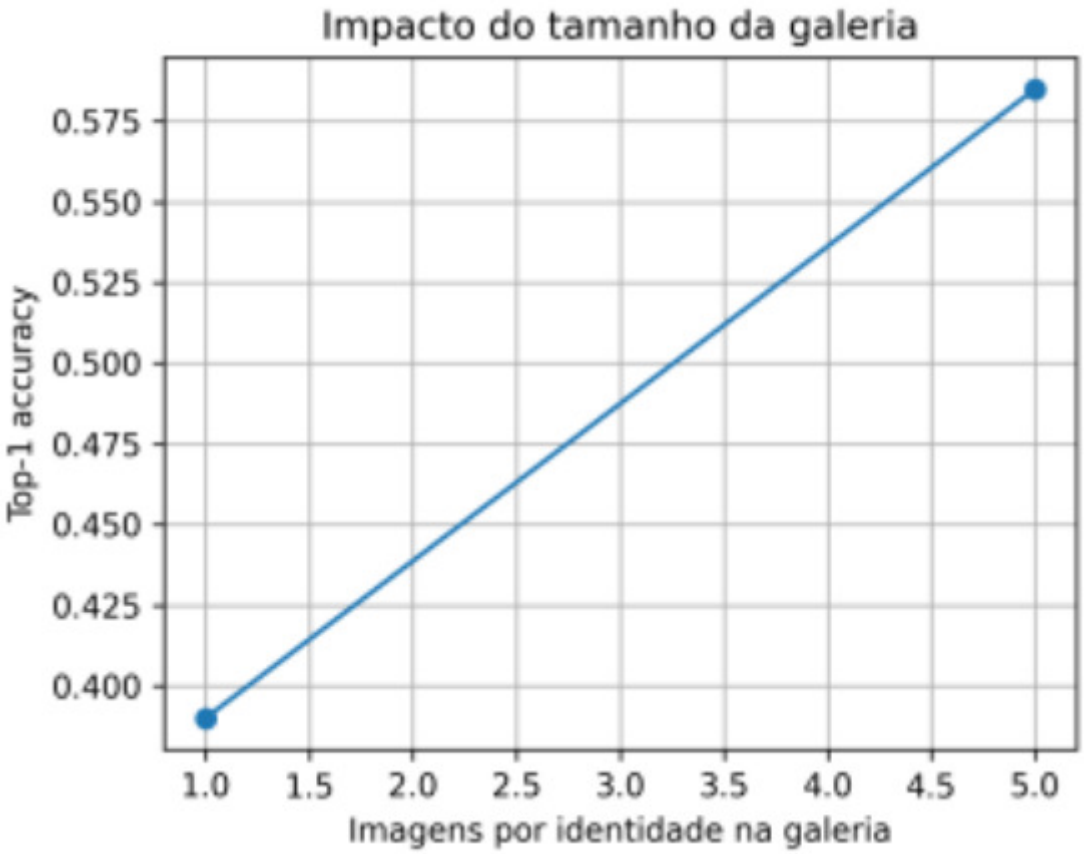
Para investigar de forma mais realista o efeito da representatividade do banco de dados, foi analisado o impacto do número de imagens por identidade na galeria sobre a acurácia *Top-1*.

A Figura 2 evidencia uma progressão consistente do desempenho à medida que aumenta o número de imagens disponíveis por identidade na galeria. Quando apenas uma imagem por identidade é utilizada, a acurácia *Top-1* situa-se em torno de 39%. Ao ampliar esse número para cinco imagens por identidade, o desempenho eleva-se para aproximadamente 58%. Esse padrão confirma empiricamente uma característica amplamente reconhecida em sistemas de reconhecimento facial baseados em *embeddings*: quanto maior a diversidade das amostras de referência, maior a probabilidade de que ao menos uma delas apresente elevada similaridade com a imagem de consulta no espaço vetorial.

Sob a perspectiva institucional, o resultado evidencia uma relação de compensação entre custo de armazenamento, esforço de coleta de dados e desempenho do sistema. Em contextos policiais, nos quais as bases de dados podem conter registros incompletos ou imagens desatualizadas, essa limitação deve ser considerada de maneira explícita. Ignorar esse fator pode conduzir a decisões fundamentadas em expectativas excessivamente otimistas quanto à confiabilidade do reconhecimento automático.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Figura 2. Impacto do número de imagens por identidade na galeria sobre a acurácia *Top 1*



3.4. Resultados de verificação facial

A tarefa de verificação facial foi avaliada por meio da análise da curva *ROC*, da área sob a curva (*AUC*), da taxa de erro no ponto de igualdade entre falso aceite e falso rejeite (*Equal Error Rate EER*) e de métricas do tipo *TAR* em níveis específicos de *FAR*, considerando uma amostragem controlada de pares genuínos e impostores. Esse protocolo é particularmente pertinente em aplicações de segurança, nas quais a redução de falsos positivos constitui requisito central para a confiabilidade operacional do sistema.

Os resultados indicam uma *AUC* de aproximadamente 0,94, o que sugere boa capacidade de discriminação global entre pares genuínos e pares impostores. O *Equal Error Rate* observado foi da ordem de 0,125, indicando que, no ponto em que as taxas de falso aceite e falso rejeite se igualam, ainda persiste uma proporção não desprezível de erros. Em ambientes institucionais, especialmente aqueles vinculados à segurança pública, esse nível de erro

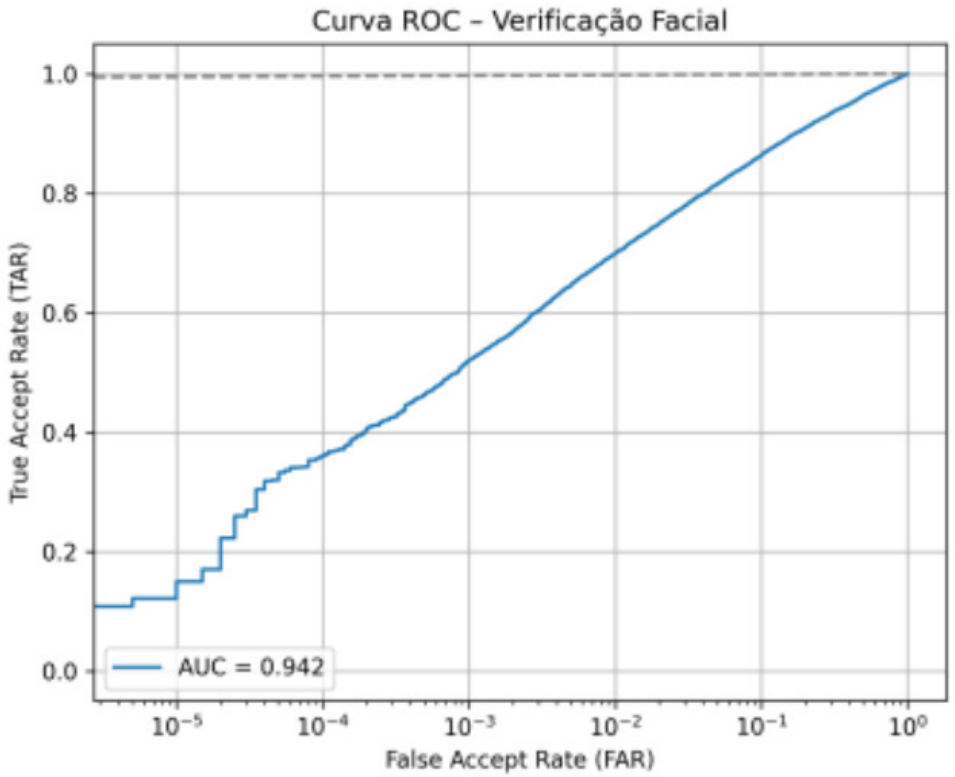
Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

demanda análise criteriosa, uma vez que decisões automatizadas podem produzir impactos relevantes quando associadas a identificações incorretas.

3.5. Análise da curva *ROC*

A Figura 3 apresenta a curva *ROC* obtida no experimento de verificação, com a *False Accept Rate* (*FAR*) representada em escala logarítmica. Observa-se que, mesmo em regimes de segurança mais rigorosos, como aqueles em que a *FAR* se situa na ordem de 10^{-3} ou 10^{-4}, o sistema preserva valores expressivos de *True Accept Rate* (*TAR*). Esse comportamento é desejável em aplicações sensíveis, como controle de acesso e apoio à investigação criminal, nas quais se busca conciliar elevada capacidade discriminativa com restrições operacionais estritas.

Figura 3. Curva ROC da tarefa de verificação facial.



À medida que o limiar de decisão se torna mais conservador, contudo, verifica-se redução gradual da *TAR*, evidenciando a tensão inerente entre segurança e usabilidade. Em contextos policiais, nos quais falsos positivos podem produzir consequências relevantes, a

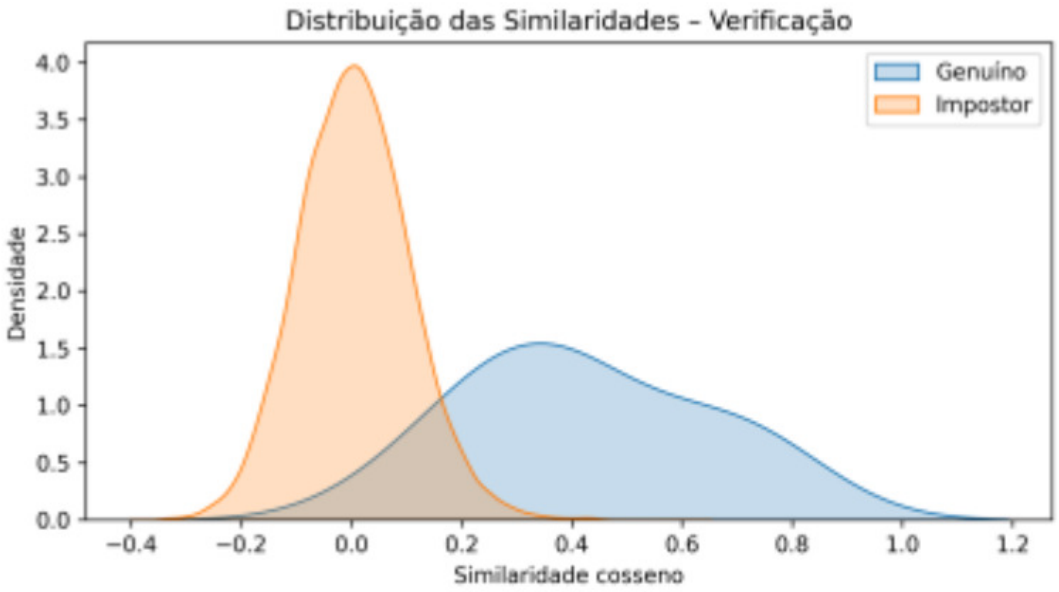
Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

definição do limiar tende a priorizar níveis muito baixos de *FAR*. Essa escolha, embora reduza o risco de aceitações indevidas, implica maior probabilidade de rejeição de indivíduos genuínos, o que reforça a necessidade de critérios técnicos bem fundamentados na configuração do sistema.

3.6. Distribuição das similaridades e interpretação geométrica

A Figura 4 apresenta a distribuição das similaridades de cosseno calculadas para pares genuínos e pares impostores. Nota-se que os pares genuínos se concentram em valores mais elevados de similaridade, com média aproximada de 0,38, ao passo que os pares impostores permanecem majoritariamente próximos de zero. Ainda que exista uma faixa de sobreposição entre as duas distribuições, a diferença global entre elas é suficiente para explicar o desempenho observado na curva *ROC* e nas métricas baseadas na relação entre taxa de aceitação verdadeira e taxa de aceitação falsa.

Figura 4. Distribuição das similaridades cosseno para pares genuínos e impostores



O gráfico também permite uma leitura geométrica do comportamento do modelo, ao evidenciar o efeito da função de perda *ArcFace* na organização do espaço de *embeddings*. Ao impor margens angulares entre identidades distintas, essa função favorece maior coesão entre vetores da mesma classe e maior afastamento entre classes diferentes. A região de

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

sobreposição observada reflete, por sua vez, a complexidade do conjunto de dados empregado, marcado por ampla variação de pose, iluminação, idade e expressão facial, fatores que naturalmente introduzem dispersão nas representações aprendidas.

3.7. Implicações dos resultados

Quando interpretados à luz de um cenário hipotético inspirado em sistemas institucionais, os resultados sugerem que o reconhecimento facial pode assumir papel relevante como ferramenta de apoio às abordagens policiais, mas não como mecanismo autônomo de identificação. A recorrente presença da identidade correta entre as primeiras posições do ranking indica utilidade em etapas de triagem e investigação preliminar, contribuindo para reduzir o universo de busca e orientar a análise humana de forma mais eficiente.

Em contrapartida, os valores observados de *Equal Error Rate* e o comportamento da taxa de aceitação verdadeira em regimes de baixa taxa de aceitação falsa evidenciam limitações que não podem ser negligenciadas. A utilização do sistema como instrumento decisório exclusivo implicaria riscos operacionais expressivos.

Falsos positivos e falsos negativos não se limitam a indicadores estatísticos de desempenho. Em contextos institucionais, especialmente na segurança pública, tais erros podem gerar consequências concretas, como abordagens indevidas, constrangimentos, restrições de liberdade e falhas na proteção de direitos fundamentais, além de comprometer a confiança social e a legitimidade das ações estatais (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, 2019).

3.8. Síntese geral dos resultados

De modo geral, os experimentos indicam que o sistema apresenta alto desempenho em tarefas de identificação quando múltiplas imagens por identidade estão disponíveis na galeria. Em cenários com número reduzido de amostras por identidade, o desempenho diminui, aproximando-se de condições mais realistas de operação. Na tarefa de verificação facial, observa-se adequado poder discriminativo, conforme evidenciado pela curva *ROC* e pelas distribuições de similaridade. Ainda persistem, contudo, limitações em regimes de segurança mais rigorosos, especialmente aqueles compatíveis com aplicações institucionais sensíveis.

Os achados estão em consonância com a literatura contemporânea em reconhecimento facial e corroboram a consistência do pipeline experimental adotado. Para além da apresentação de métricas, os resultados oferecem base empírica para discutir aspectos de escalabilidade,

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

robustez e risco operacional, estabelecendo conexão direta entre a avaliação técnica do sistema e as reflexões éticas, jurídicas e institucionais desenvolvidas nas seções seguintes.

4. DISCUSSÕES

A incorporação de sistemas de reconhecimento facial no âmbito da segurança pública ultrapassa a dimensão estritamente técnica e requer exame atento de suas implicações éticas, jurídicas e institucionais. Os resultados experimentais apresentados demonstram que, ainda que o sistema alcance boa capacidade de separação entre identidades, persistem taxas de erro relevantes, sobretudo quando se adotam limiares mais conservadores. Em contextos policiais, tais erros não se traduzem em meras variações estatísticas, mas podem repercutir diretamente sobre direitos fundamentais, como liberdade individual, dignidade da pessoa humana e presunção de inocência.

Sob o ponto de vista ético, a literatura especializada destaca que sistemas de reconhecimento facial operam com base em probabilidades e, portanto, não devem ser compreendidos como instrumentos de determinação inequívoca da verdade (Raposo, 2024). Estudos têm evidenciado que o risco de falsos positivos não se distribui de maneira homogênea entre diferentes grupos populacionais, podendo afetar de forma desproporcional indivíduos historicamente vulnerabilizados. Buolamwini e Gebru (2018) demonstram, por exemplo, disparidades significativas de desempenho em sistemas comerciais de análise facial, o que reforça a necessidade de que tais tecnologias sejam empregadas, quando muito, como instrumentos auxiliares, sempre subordinados à avaliação humana e a outros elementos probatórios. A adoção acrítica de decisões automatizadas, especialmente em ambientes coercitivos, pode contribuir para a reprodução e amplificação de vieses sociais preexistentes sob a aparência de neutralidade técnica.

No plano jurídico, o uso institucional do reconhecimento facial demanda cautela reforçada, sobretudo porque envolve o tratamento de imagens e fotografias de pessoas, isto é, informações de natureza sensível no contexto da identificação biométrica. No Brasil, a Lei Geral de Proteção de Dados qualifica dados biométricos como dados pessoais sensíveis, impondo exigências rigorosas quanto à sua coleta, tratamento e armazenamento (BRASIL, 2020). Contudo, é importante ressaltar que, embora em seu artigo quarto, a Lei determina que ela “[...] não se aplica ao tratamento de dados pessoais: [...] III - realizado para fins exclusivos de: a) segurança pública; [...]”, essa situação não autoriza concluir que tais práticas ocorram em um espaço normativo vazio.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Ao contrário, o § 1º do mesmo dispositivo prevê que esse tratamento seja disciplinado por legislação específica, com observância do devido processo legal e de medidas proporcionais e estritamente necessárias à tutela do interesse público. Assim, no cenário hipotético discutido neste artigo, em que a própria administração pública empregaria tais ferramentas, entende-se que caberia ao próprio Estado estruturar a regulação aplicável, bem como instituir mecanismos de governança, segurança da informação e proteção contra acessos indevidos, vazamentos ou compartilhamentos com terceiros não autorizados. Em suma, a utilização estatal de sistemas dessa natureza não dispensa o dever de proteção; ao contrário, exige salvaguardas jurídicas, institucionais e técnicas ainda mais rigorosas.

Ademais, o atendimento a requisitos como finalidade legítima, necessidade, adequação, proporcionalidade e transparência não decorre automaticamente da viabilidade técnica do sistema, mas demanda fundamentação específica e controles institucionais efetivos, conforme analisam Doneda *et al.* (2019). Além disso, decisões administrativas ou judiciais baseadas exclusivamente em sistemas automatizados suscitam questionamentos quanto à observância de garantias constitucionais, sobretudo quando inexistem mecanismos claros de contestação, auditoria e revisão humana.

Sob a perspectiva organizacional, os resultados deste estudo indicam que a eventual integração do reconhecimento facial em sistemas institucionais não pode ser tratada como simples atualização tecnológica. Trata-se de processo que envolve governança, definição precisa de responsabilidades, capacitação dos agentes e monitoramento contínuo de desempenho. Relatórios internacionais apontam que experiências problemáticas de uso dessa tecnologia decorrem, muitas vezes, menos de limitações algorítmicas e mais da ausência de protocolos claros, critérios de supervisão e avaliação sistemática de impactos sociais, como discutido por Garvie, Frankle e Bedoya (2016).

Em conjunto, os achados experimentais reforçam que, embora o reconhecimento facial apresente potencial técnico significativo, suas limitações impedem que seja legitimamente empregado como instrumento decisório autônomo em contextos sensíveis. O uso responsável dessa tecnologia deve restringir-se a funções de apoio e triagem, inserido em estrutura institucional que assegure supervisão humana qualificada do policial militar em campo, mecanismos de responsabilização e primazia da proteção de direitos fundamentais.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

5. CONSIDERAÇÕES FINAIS

Este artigo apresentou um estudo metodológico e experimental sobre o uso de técnicas de reconhecimento facial baseadas em aprendizado profundo em um cenário hipotético inspirado em sistemas institucionais de segurança pública, com ênfase na possibilidade de integração como módulo de apoio à decisão no SADE. Diferentemente de abordagens voltadas à implantação imediata ou à busca por desempenho de estado da arte, o objetivo central consistiu em examinar criticamente os limites, riscos e potencialidades dessa tecnologia quando incorporada a um fluxo decisório humano e institucional.

Sob o ponto de vista técnico, os experimentos indicaram que o experimento desenvolvido foi capaz de estruturar um espaço de *embeddings* faciais com capacidade discriminativa consistente nos protocolos avaliados, exibindo separação entre identidades e desempenho compatível com a arquitetura adotada. As análises de identificação evidenciaram a dependência direta do desempenho em relação à quantidade e à diversidade de imagens por identidade na galeria. Já as avaliações de verificação demonstraram que configurações mais restritivas de segurança, típicas de contextos policiais (baixa tolerância a falsos positivos), implicam aumento nas taxas de rejeição de indivíduos genuínos. Esses resultados reforçam que métricas agregadas de acurácia, consideradas isoladamente, são insuficientes para julgar a adequação de sistemas biométricos em ambientes sensíveis.

No contexto de uma possível implementação de um módulo de reconhecimento facial ao SADE, os resultados indicam que a implementação deve ser entendida como a implantação de um serviço de triagem probabilística, na qual a saída do sistema é uma lista ranqueada de hipóteses, e não uma confirmação automática de identidade. Além disso, é recomendável que seja adotado um fluxo assistido, incluindo uma validação mínima de qualidade, a geração do *embedding*, a consulta à galeria institucional e o retorno de candidatos com seus escores, juntamente com uma indicação de faixa de decisão.

Deste modo, se o sistema retornar um valor abaixo do limiar, o resultado deve ser tratado como não suficiente. Na zona intermediária, deve ser classificado como incerto. Acima do limiar, deve ser apresentado como indicação mais forte, sem caracterizar confirmação. Em todos os casos, a etapa final precisa ser obrigatoriamente supervisionada por um operador humano, com corroboração por outras evidências, para evitar que a ferramenta seja usada como decisão automatizada.

A dependência do desempenho em relação à composição da galeria também mostra que a integração ao SADE precisa incluir políticas explícitas de curadoria e atualização do acervo

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

institucional do banco de dados de imagens. Isso envolve diversidade temporal, controle de duplicatas, critérios mínimos de qualidade e rastreabilidade da origem.

Do ponto de vista metodológico, o estudo contribui ao detalhar um pipeline que contempla organização dos dados, treinamento do modelo, geração de *embeddings* e procedimentos de avaliação, com atenção à separação entre treinamento e inferência. Entretanto, para que a integração ao SADE seja institucionalmente controlável, recomenda-se que o módulo seja acompanhado por uma política de auditabilidade: cada consulta deve gerar registros completos (caso, *timestamp*, origem/contexto da imagem, versão do modelo e do pré-processamento, parâmetros de limiar, lista Top-K retornada e decisão humana subsequente), possibilitando responsabilização e auditorias técnicas e organizacionais.

No plano ético, jurídico e organizacional, a análise conduzida indica que o reconhecimento facial, ainda que tecnicamente viável, não deve ser compreendido como instrumento neutro ou decisório autônomo no âmbito policial. As taxas de erro observadas, especialmente em cenários de baixa tolerância a falsos positivos, revelam que a adoção indiscriminada dessa tecnologia pode comprometer a proteção de direitos fundamentais. Eventual integração a sistemas institucionais deve, portanto, estar condicionada a critérios de proporcionalidade, supervisão humana efetiva, transparência e mecanismos claros de governança, de modo a evitar que uma ferramenta de apoio seja convertida em fonte de decisões automatizadas inadequadas.

Entre as limitações do estudo destacam-se o uso de subconjunto controlado de identidades, a avaliação restrita a imagens estáticas e a ausência de experimentação completa em cenário *open-set* com rejeição explícita de indivíduos desconhecidos em larga escala. Também não foram realizadas análises específicas de viés demográfico, aspecto particularmente relevante para aplicações reais e que demanda investigação própria.

Como desdobramentos possíveis, destacam-se a ampliação progressiva do número de identidades avaliadas, aproximando-se de escalas compatíveis com bases institucionais reais; a exploração de arquiteturas mais robustas ou especializadas; a incorporação de estratégias de mineração de amostras difíceis e de métodos eficientes de indexação para busca em grandes bases; a avaliação sistemática em cenários *open-set* com mecanismos formais de rejeição; e estudos aprofundados sobre vieses algorítmicos e seus impactos diferenciados entre grupos demográficos.

Em síntese, a presente pesquisa busca contribuir para um debate mais qualificado sobre o uso de reconhecimento facial no aperfeiçoamento da segurança pública. Ao situar essa tecnologia como ferramenta probabilística de apoio, e não como solução definitiva, reforça-se a

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

necessidade de que decisões institucionais relacionadas à inteligência artificial sejam pautadas por cautela, responsabilidade e compromisso efetivo com a proteção de direitos fundamentais do ser humano.

REFERÊNCIAS

ALMEIDA, Lucas A.; SILVA, Renata M.; COSTA, Henrique P. Reconhecimento facial, segurança pública e direitos fundamentais: desafios éticos e jurídicos. *Revista de Ciências Criminais Contemporâneas*, São Paulo, v. 8, n. 2, p. 45–63, 2021.

BRANDNER, Tobias. Facial recognition technologies: opportunities, risks and ethical implications. *AI & Society*, London, v. 38, n. 1, p. 125–138, 2023. DOI: 10.1007/s00146-022-01465-9.

BRASIL. Lei nº 13.675, de 11 de junho de 2018. Institui o Sistema Único de Segurança Pública (Susp) e cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13675.htm. Acesso em: 1 mar. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 1 mar. 2026.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: intersectional accuracy disparities in commercial gender classification. In: *CONFERENCE ON FAIRNESS, ACCOUNTABILITY AND TRANSPARENCY*, 2018, New York. *Proceedings [...]* New York: PMLR, 2018. p. 77–91.

CAO, Qiong; SHEN, Li; XIE, Weidi; PARKHI, Omkar M.; ZISSERMAN, Andrew. VGGFace2: a dataset for recognising faces across pose and age. In: *IEEE INTERNATIONAL CONFERENCE ON AUTOMATIC FACE & GESTURE RECOGNITION*, 2018, Xi'an, China. *Proceedings [...]* [S. l.]: IEEE, 2018. p. 67–74.

CENTER ON PRIVACY & TECHNOLOGY. *Garbage in, garbage out: face recognition on flawed data*. Washington, DC: Georgetown University Law Center, 2019. Disponível em: https://www.law.georgetown.edu/privacy-technology-center/publications/garbage-in-garbage-out-face-recognition-on-flawed-data/. Acesso em: 29 jan. 2026.

CRAWFORD, Kate. *Atlas of AI: power, politics, and the planetary costs of artificial intelligence*. New Haven: Yale University Press, 2021.

DENG, Jiankang; GUO, Jia; XUE, Niannan; ZAFEIRIOU, Stefanos. ArcFace: additive angular margin loss for deep face recognition. In: *IEEE/CVF CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION*, 2019, Long Beach, CA. *Proceedings [...]* [S. l.]: IEEE, 2019. p. 4690–4699.

DONEDA, Danilo et al. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *Facial recognition technology: fundamental rights considerations in the context of law enforcement*. Luxembourg: Publications Office of the European Union, 2019. Disponível em: https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law. Acesso em: 17 fev. 2026.

GARVIE, Clare; BEDOYA, Alvaro; FRANKLE, Jonathan. *The perpetual line-up: unregulated police face recognition in America*. Washington, DC: Georgetown Law Center on Privacy & Technology, 2016.

GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. *Face recognition vendor test (FRVT): demographic effects*. Gaithersburg, MD: National Institute of Standards and Technology, 2019. DOI: 10.6028/NIST.IR.8280.
INTRONA, Lucas D.; WOOD, David. Picturing algorithmic surveillance: the politics of facial recognition systems. *Surveillance & Society*, London, v. 2, n. 2/3, p. 177–198, 2004. DOI: 10.24908/ss.v2i2/3.3373.

JAIN, Anil K.; ROSS, Arun; PRABHAKAR, Salil. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, New York, v. 14, n. 1, p. 4–20, 2004. DOI: 10.1109/TCSVT.2003.818349.

KISHORE, Saritha et al. Evaluation of Deep Learning Methods in Face Recognition: datasets, metrics, and results. *International Journal on Science and Technology (IJSAT)*, v. 16, n. 4, out./dez. 2025. DOI: 10.71097/IJSAT.v16.i4.9087.

MIN, J.; FLYNN, P.; BOWYER, K. W. Using multiple gallery and probe images per person to improve performance of face recognition. In: *IEEE COMPUTER SOCIETY CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION WORKSHOPS*, 2003, Washington, DC. *Proceedings [...]* Washington, DC: IEEE, 2003. p. 25. DOI: 10.1109/CVPRW.2003.10033.

MIRANDA, João Vitor Arnas de; LIMA, Luis Henrique de. O uso de tecnologias como forma de melhorar a eficiência na segurança pública: um quadro comparativo na PMPR pré e pós implementação do sistema de atendimento e despacho de emergências (SADE). *Revista Científica de Alto Impacto*, v. 27, n. 127, out. 2023. DOI: 10.5281/zenodo.8433291.

PARKHI, Omkar M.; VEDALDI, Andrea; ZISSERMAN, Andrew. Deep face recognition. In: *BRITISH MACHINE VISION CONFERENCE*, 2015, Swansea, UK. *Proceedings [...]* Durham: BMVA Press, 2015. p. 41.1–41.12. DOI: 10.5244/C.29.41.

RAPOSO, Vera Lúcia. When facial recognition does not 'recognise': erroneous identifications and resulting liabilities. *AI & Society*, v. 39, p. 1857–1869, 2024. DOI: 10.1007/s00146-023-01634-z.

SANTOS, Thiago Federovicz Mendes dos. A implantação do sistema de atendimento e despacho de emergências via mobile no 10º batalhão da Polícia Militar do Paraná. *Brazilian Journal of Development*, Curitiba, v. 9, n. 3, p. 11214–11241, 2023. DOI: 10.34117/bjdv9n3-153.

SCHEIRER, Walter J.; JAIN, Lalit P.; BOULT, Terrance E. Probability models for open set recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, New York, v. 36, n. 11, p. 2317–2324, 2014. DOI: 10.1109/TPAMI.2014.2321392.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

SCHROFF, Florian; KALENICHENKO, Dmitry; PHILBIN, James. FaceNet: a unified embedding for face recognition and clustering. In: *IEEE CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION*, 2015, Boston, MA. *Proceedings [...]* [S. l.]: IEEE, 2015. p. 815–823. DOI: 10.1109/CVPR.2015.7298682.

SU, Yiyang; KIM, Minchul; LIU, Feng; JAIN, Anil; LIU, Xiaoming. Open-Set Biometrics: Beyond Good Closed-Set Models. *arXiv*, [cs.CV], 2024. Disponível em: https://arxiv.org/abs/2407.16133. Acesso em: 17 fev. 2026.

TAIGMAN, Yaniv; YANG, Ming; RANZATO, Marc'Aurelio; WOLF, Lior. DeepFace: closing the gap to human-level performance in face verification. In: *IEEE CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION*, 2014, Columbus, OH. *Proceedings [...]* [S. l.]: IEEE, 2014. p. 1701–1708.

THORAT, S. B.; NAYAK, S. K.; DANDALE, Jyoti P. Facial recognition technology: an analysis with scope in India. *International Journal of Computer Science and Information Security*, v. 8, n. 1, 2010. Disponível em: https://arxiv.org/abs/1005.4263. Acesso em: 17 fev. 2026.

WANG, Xukang; WU, Ying Cheng; ZHOU, Mengjie; FU, Hongpeng. Beyond surveillance: privacy, ethics, and regulations in face recognition technology. *Frontiers in Big Data*, Lausanne, v. 7, art. 1337465, 2024. DOI: 10.3389/fdata.2024.1337465.

WASHINGTON POST. Arrested by AI: police ignore standards after facial recognition matches. Washington, DC, 2025. Disponível em: https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/. Acesso em: 29 jan. 2026.

Digitally signed by RECIMA21 REVISTA CIENTIFICA MULTIDISCIPLINAR LTDA:40166538000195.
Timestamp: 2026-05-03 19:01:45 -03.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.