



UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO ENGENHARIA DO CONHECIMENTO
CURSO DE PÓS-GRADUAÇÃO EM INTELIGÊNCIA E INOVAÇÃO NO
ENFRENTAMENTO AO CRIME ORGANIZADO

Fábio Henrique Dantas de Carvalho
Fábio Henrique Silva Pinto

**Desenvolvimento de Software de Reconhecimento Facial Face Finder
InsightFace Pro Aplicado à Inteligência Policial: Estudo de Caso na Polícia Militar
do Rio Grande do Norte**

Florianópolis
2026

Fábio Henrique Dantas de Carvalho
Fábio Henrique Silva Pinto

**Desenvolvimento de Software de Reconhecimento Facial Face Finder
InsightFace Pro Aplicado à Inteligência Policial: Estudo de Caso na Polícia Militar
do Rio Grande do Norte**

Trabalho de Conclusão de Curso submetido ao curso de Pós-Graduação em Inteligência e Inovação no Enfrentamento ao Crime Organizado do Centro Tecnológico da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de especialista em Inteligência e Inovação no Enfrentamento ao Crime Organizado.

Orientador(a): Prof. Bruno Vieira

Florianópolis
2026

Carvalho, Fábio Henrique Dantas de Desenvolvimento de Software de Reconhecimento Facial Face Finder InsightFace Pro Aplicado à Inteligência Policial: Estudo de Caso na Polícia Militar do Rio Grande do Norte / Fábio Henrique Dantas de Carvalho, Fábio Henrique Silva Pinto ; orientador, Bruno da Cunha Vieira, 2026. 33 p. Monografia (especialização) - Universidade Federal de Santa Catarina, Centro Tecnológico, Curso de CURSO DE PÓS GRADUAÇÃO EM INTELIGÊNCIA E INOVAÇÃO NO ENFRENTAMENTO AO CRIME ORGANIZADO, Florianópolis, 2026. Inclui referências.

1. Reconhecimento facial.
2. Inteligência policial.

- I. Pinto, Fábio Henrique Silva.
- II. Vieira, Bruno da Cunha.
- III. Universidade Federal de Santa Catarina. CURSO DE PÓS GRADUAÇÃO EM INTELIGÊNCIA E INOVAÇÃO NO ENFRENTAMENTO AO CRIME ORGANIZADO.
- IV. Título.

Fábio Henrique Dantas de Carvalho
Fábio Henrique Silva Pinto

Desenvolvimento de Software de Reconhecimento Facial *Face Finder*
InsightFace Pro Aplicado à Inteligência Policial: Estudo de Caso na Polícia Militar
do Rio Grande do Norte

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do título de Inteligência e Inovação no Enfrentamento ao Crime Organizado e aprovado em sua forma final pelo Curso Pós-Graduação em Inteligência e Inovação no Enfrentamento ao Crime Organizado

Florianópolis, 23 de fevereiro de 2026.

Insira neste espaço

a assinatura

Coordenação do Curso

Banca examinadora

Insira neste espaço

a assinatura

Prof. Bruno da Cunha Vieira, Me.

Orientador

Insira neste espaço

a assinatura

Gmael de Medeiros Guedes,

Florianópolis, [2026].

RESUMO

O avanço das tecnologias de inteligência artificial tem ampliado significativamente o uso de sistemas de reconhecimento facial no contexto da segurança pública, especialmente como ferramenta de apoio às atividades de inteligência policial. Diante do crescimento do volume de imagens provenientes de câmeras de vigilância, dispositivos móveis e bases digitais, métodos tradicionais de identificação manual tornaram-se progressivamente insuficientes em termos de tempo, padronização e escalabilidade. Nesse cenário, este Trabalho de Conclusão de Curso tem como objetivo descrever o desenvolvimento de um software de reconhecimento facial denominado Face Finder InsightFace Pro, concebido para apoiar a identificação de indivíduos no âmbito da inteligência policial, com estudo de caso aplicado à Polícia Militar do Rio Grande do Norte. O trabalho adota uma abordagem aplicada, de natureza tecnológica e caráter descritivo, fundamentada na metodologia Design Science Research, priorizando a apresentação do artefato desenvolvido, sua arquitetura, funcionamento e potencial contributivo. O software foi implementado na linguagem Python, integrando bibliotecas de visão computacional e aprendizado profundo, com utilização de modelos pré-treinados para extração de *embeddings* faciais e comparação por métricas de similaridade. A solução opera de forma local, com interface gráfica intuitiva, permitindo controle institucional dos dados e flexibilidade na definição dos parâmetros de busca. Os resultados esperados indicam potencial para redução do tempo de análise, padronização dos procedimentos de comparação facial e fortalecimento do apoio analítico às atividades de inteligência policial. Ressalta-se que o sistema não substitui o julgamento humano, atuando como ferramenta auxiliar, cujo uso deve observar critérios legais, éticos e institucionais, especialmente no que se refere à proteção de dados pessoais.

Palavras-chave: Reconhecimento facial. Inteligência policial. InsightFace. Design Science Research. Inovação tecnológica.

ABSTRACT

The advancement of artificial intelligence technologies has significantly expanded the use of facial recognition systems in the context of public security, especially as a tool to support police intelligence activities. Faced with the growth in the volume of images coming from surveillance cameras, mobile devices and digital databases, traditional methods of manual identification have become progressively insufficient in terms of time, standardization and scalability. In this scenario, this Final Paper aims to describe the development of a facial recognition software called Face Finder InsightFace Pro, designed to support the identification of individuals in the scope of police intelligence, with a case study applied to the Military Police of Rio Grande do Norte. The work adopts an applied approach, of a technological nature and descriptive character, based on the Design Science Research methodology, prioritizing the presentation of the developed artifact, its architecture, operation and contribution potential. The software was implemented in the Python language, integrating computer vision and deep learning libraries, using pre-trained models for extracting facial embeddings and comparing by similarity metrics. The solution operates locally, with an intuitive graphical interface, allowing institutional control of the data and flexibility in the definition of search parameters. The expected results indicate potential for reducing the analysis time, standardizing facial comparison procedures and strengthening analytical support for police intelligence activities. It should be noted that the system

does not replace human judgment, acting as an auxiliary tool, whose use must observe legal, ethical and institutional criteria, especially with regard to the protection of personal data.

Keywords: Facial recognition. Police intelligence. InsightFace. Design Science Research. Technological innovation.

1 INTRODUÇÃO

A intensificação do uso de tecnologias digitais no âmbito da segurança pública tem provocado transformações profundas nas estratégias de produção, análise e difusão de informações voltadas à prevenção e repressão da criminalidade. Em um cenário marcado pelo crescimento exponencial de dados visuais, especialmente imagens e vídeos oriundos de dispositivos móveis, câmeras de vigilância e redes sociais, os órgãos de inteligência policial passaram a enfrentar o desafio de lidar com grandes volumes de informação de maneira eficiente, célere e confiável. Nesse contexto, a adoção de soluções baseadas em inteligência artificial, em especial aquelas relacionadas ao reconhecimento facial, emerge como alternativa estratégica para a otimização dos processos de identificação de indivíduos e apoio à tomada de decisão operacional (Jain, Ross e Nandakumar, 2011; Zhao et al., 2019).

O reconhecimento facial consiste em um conjunto de técnicas computacionais voltadas à identificação ou verificação de indivíduos a partir de características biométricas extraídas da face humana. Diferentemente de métodos tradicionais de identificação, que dependem fortemente da análise humana e da comparação manual de imagens, os sistemas automatizados baseados em visão computacional e aprendizado profundo permitem extrair padrões faciais complexos, representá-los matematicamente e compará-los em larga escala, reduzindo significativamente o tempo de resposta e o risco de inconsistências subjetivas (Zhao et al., 2019). A face humana constitui uma das formas mais naturais de identificação, o que torna sua modelagem computacional um campo de elevada relevância científica e prática (Turk e Pentland, 1991).

No âmbito da inteligência policial, a identificação rápida e precisa de indivíduos é elemento central para a condução de investigações, análise de vínculos criminais, localização de suspeitos e cruzamento de informações estratégicas. Entretanto, em muitas realidades institucionais brasileiras, ainda prevalecem métodos manuais de

análise de imagens, baseados na observação visual e na comparação empírica entre fotografias, procedimento que demanda elevado esforço humano, tempo prolongado e alto grau de especialização técnica. Tal realidade compromete a eficiência operacional e pode impactar diretamente a capacidade de resposta das forças de segurança (Ratcliffe, 2016).

Diante desse cenário, observa-se a necessidade de desenvolvimento de soluções tecnológicas acessíveis, adaptáveis à realidade local e capazes de apoiar o trabalho dos setores de inteligência sem substituir a análise humana, mas potencializando suas capacidades. O uso de softwares de reconhecimento facial desenvolvidos em ambiente local, com controle institucional e possibilidade de customização, apresenta-se como alternativa viável frente a soluções proprietárias de alto custo ou plataformas externas que levantam preocupações quanto à soberania dos dados e à conformidade legal. Nesse sentido, ressalta-se a importância de modelos tecnológicos que conciliem inovação, transparência e responsabilidade no uso de dados sensíveis (Brakel, 2016; Zuboff, 2019).

O presente Trabalho de Conclusão propõe a descrição e análise do desenvolvimento de um software de reconhecimento facial denominado Face Finder InsightFace Pro, concebido para aplicação no contexto da inteligência policial, com estudo de caso voltado à realidade da Polícia Militar do Rio Grande do Norte. O software foi desenvolvido utilizando a linguagem Python, bibliotecas amplamente consolidadas na área de visão computacional e aprendizado profundo, e um modelo pré-treinado de reconhecimento facial, sendo estruturado de forma modular e orientada à eficiência operacional. Ressalta-se que o artefato tecnológico encontra-se plenamente desenvolvido e em uso pelo discente, não sendo objeto deste trabalho a execução de testes institucionais, validações empíricas ou mensuração estatística de desempenho.

Diante desse cenário, identificam-se limitações críticas dos métodos manuais de identificação facial em atividades de inteligência policial, particularmente no tempo de processamento, escalabilidade e padronização das análises. A ausência de ferramentas automatizadas de fácil implementação contribui para a sobrecarga dos analistas e para a redução da capacidade de exploração de grandes volumes de dados visuais, realidade que se torna cada vez mais crítica em um ambiente

informacional complexo e dinâmico (Kitchin, 2014), a incapacidade de transformar dados em conhecimento acionável representa um dos principais gargalos das organizações contemporâneas.

O objetivo geral deste trabalho é descrever o desenvolvimento de software de reconhecimento facial para inteligência policial, detalhando fundamentos teóricos, arquitetura, fluxo operacional e contribuições institucionais. Com objetivos específicos de contextualização na segurança pública, princípios tecnológicos, metodologia e análise de resultados/limitações. Sua justificativa assenta em relevância prática (modernização da identificação), acadêmica (integração IA-engenharia-segurança) e social (prevenção criminal ética, conforme (LGPD, 2018), alertando que tecnologias acríticas amplificam vieses e desigualdades, demandando governança e transparência (Mittelstadt et al., 2016).

Nesse contexto, o Face Finder InsightFace Pro foi concebido como um artefato tecnológico voltado ao apoio da inteligência policial, sem a pretensão de substituir o julgamento humano, mas de ampliá-lo por meio da automação de tarefas repetitivas e da padronização dos processos de comparação facial. A solução busca reduzir o tempo despendido na triagem inicial de imagens, permitindo que os analistas concentrem seus esforços em atividades de maior complexidade cognitiva e estratégica. Tal perspectiva está alinhada ao entendimento de Davenport e Kirby (2016), segundo os quais a inteligência artificial, quando bem aplicada, atua como ferramenta de ampliação das capacidades humanas, e não como elemento de substituição total do trabalho analítico.

Ressalta-se que este trabalho adota uma abordagem descritiva e tecnológica, centrada na apresentação do processo de desenvolvimento do software, de sua arquitetura e de seu fluxo de funcionamento, não contemplando testes operacionais oficiais, validações empíricas ou análises estatísticas de desempenho em ambiente institucional real. Essa delimitação metodológica é intencional e coerente com a natureza de um artigo tecnológico, cujo foco reside na concepção do artefato e na explicitação de seus fundamentos técnicos e conceituais no âmbito da Design Science Research (Peppers et al., 2007).

Este trabalho está organizado da seguinte forma:

- Capítulo 1: Introdução
- Capítulo 2: Fundamentação Teórica
- Capítulo 3: Metodologia
- Capítulo 4: Desenvolvimento do software
- Capítulo 5: Resultados esperado e discussão
- Capítulo 6: Conclusão

2 FUNDAMENTAÇÃO TEÓRICA

O avanço das tecnologias digitais nas últimas décadas ampliou significativamente a capacidade de coleta, armazenamento e processamento de dados, transformando imagens em um dos principais insumos informacionais das organizações contemporâneas. A centralidade dos dados na sociedade atual redefine práticas institucionais, exigindo métodos automatizados capazes de transformar grandes volumes de informação em conhecimento acionável. Nesse cenário, a análise manual de imagens torna-se progressivamente insuficiente, sobretudo em contextos que demandam rapidez, precisão e escalabilidade, como ocorre na atividade de inteligência policial (Kitchin, 2014).

O reconhecimento facial insere-se nesse panorama como uma das aplicações da inteligência artificial, por explorar uma característica biométrica amplamente utilizada nos processos naturais de identificação humana. Conforme destacam Jain, Flynn e Ross (2008), a biometria facial apresenta vantagens específicas, como a não invasividade, a possibilidade de aquisição a distância e a compatibilidade com bases de dados já existentes, fatores que explicam sua crescente adoção em diferentes domínios institucionais.

2.1 Reconhecimento Facial e Visão Computacional

O reconhecimento facial pode ser compreendido como um conjunto de técnicas computacionais destinadas a identificar ou verificar indivíduos a partir de imagens ou sequências de vídeo, utilizando características estruturais da face humana. Esse processo envolve, de maneira geral, três etapas fundamentais: a detecção da face na

imagem, a extração de características discriminantes e a comparação dessas características com um conjunto previamente armazenado. De acordo com Zhao et al. (2019), a eficácia de um sistema de reconhecimento facial depende diretamente da robustez dessas etapas e da capacidade do modelo em lidar com variações naturais, como iluminação, pose, expressões faciais e qualidade da imagem.

A visão computacional, enquanto subárea da inteligência artificial, dedica-se ao desenvolvimento de métodos que permitam aos sistemas computacionais interpretar e compreender informações visuais de forma semelhante à percepção humana. Desde os primeiros estudos estruturados na área, como os trabalhos pioneiros de Marr (1982), a visão computacional evoluiu de abordagens baseadas em regras e extração manual de atributos para modelos capazes de aprender representações complexas diretamente dos dados. Essa evolução foi impulsionada, sobretudo, pelo aumento do poder computacional e pela disponibilidade de grandes bases de dados visuais.

Nos primeiros sistemas de reconhecimento facial, predominavam métodos baseados em características geométricas ou estatísticas, como distâncias entre pontos faciais, projeções em subespaços lineares e análise de componentes principais. O modelo conhecido como *Eigenfaces*, proposto por Turk e Pentland (1991), representa um marco nesse período, ao demonstrar que faces poderiam ser representadas como combinações lineares de vetores extraídos de um conjunto de imagens. Embora inovadores para a época, esses métodos apresentavam limitações significativas frente a variações ambientais e condições não controladas.

Com o advento do aprendizado profundo, especialmente das redes neurais convolucionais, o reconhecimento facial passou a operar com representações de alto nível conhecidas como *embeddings* faciais. Esses vetores numéricos condensam informações discriminantes da face em espaços multidimensionais, permitindo comparações eficientes por meio de métricas matemáticas. Segundo Schroff, Kalenichenko e Philbin (2015), a utilização de *embeddings* normalizados e métricas como a similaridade cosseno possibilita alcançar elevados níveis de precisão mesmo em cenários complexos, aproximando o desempenho dos sistemas automatizados à capacidade humana de reconhecimento.

No contexto contemporâneo, os sistemas de reconhecimento facial baseados em *deep learning* demonstram elevada robustez frente a ruídos, variações de iluminação e diferenças de pose, desde que treinados em bases de dados amplas e diversificadas. Contudo, como ressaltam Bowyer, Chang e Flynn (2016), tais sistemas não estão isentos de limitações, especialmente quando aplicados fora dos contextos para os quais foram originalmente treinados, o que reforça a importância de uma compreensão crítica de seus fundamentos e condições de uso.

A incorporação dessas técnicas no ambiente da segurança pública demanda, portanto, uma análise cuidadosa de suas potencialidades e restrições, evitando tanto o entusiasmo acrítico quanto a rejeição baseada em desconhecimento técnico. A compreensão dos fundamentos da visão computacional e do reconhecimento facial constitui, assim, passo essencial para a avaliação do software desenvolvido neste trabalho, permitindo situá-lo de forma adequada no campo científico e institucional.

2.2 Deep Learning Aplicado ao Reconhecimento Facial

O avanço do *deep learning* representou uma ruptura paradigmática no campo do reconhecimento facial, ao substituir abordagens baseadas em extração manual de atributos por modelos capazes de aprender representações discriminantes diretamente a partir dos dados. Diferentemente dos métodos clássicos, nos quais as características faciais eram previamente definidas por especialistas, as redes neurais profundas passaram a identificar padrões complexos de forma autônoma, explorando estruturas hierárquicas que refletem diferentes níveis de abstração visual. Conforme argumentam LeCun, Bengio e Hinton (2015), essa capacidade de aprendizado em múltiplas camadas constitui o principal diferencial das arquiteturas profundas em tarefas de percepção visual.

As redes neurais convolucionais tornaram-se o principal arcabouço técnico para aplicações de reconhecimento facial em função de sua eficiência no processamento de imagens. Essas redes operam por meio de filtros convolucionais que percorrem a imagem de entrada, capturando padrões locais como bordas, texturas e contornos, os quais são progressivamente combinados em representações mais abstratas nas camadas subsequentes. Segundo Goodfellow, Bengio e Courville (2016), essa organização hierárquica permite que o modelo desenvolva invariância a

pequenas variações espaciais, aspecto fundamental para lidar com diferenças de pose, iluminação e expressão facial.

No contexto do reconhecimento facial, o objetivo principal do *deep learning* não é a classificação direta de indivíduos, mas a geração de *embeddings* faciais, isto é, vetores numéricos de alta dimensionalidade que representam de forma compacta as características distintivas de uma face. Esses vetores são projetados em espaços métricos nos quais a distância entre *embeddings* reflete o grau de similaridade entre indivíduos. Conforme demonstrado por Taigman et al. (2014), *embeddings* bem treinados apresentam a propriedade de agrupar faces do mesmo indivíduo em regiões próximas do espaço vetorial, enquanto mantêm faces de indivíduos distintos suficientemente afastadas.

A comparação entre *embeddings* faciais é geralmente realizada por meio de métricas matemáticas, como a distância euclidiana ou a similaridade cosseno, sendo esta última amplamente adotada em sistemas modernos de reconhecimento facial. A similaridade cosseno avalia o ângulo entre dois vetores normalizados, oferecendo maior estabilidade frente a variações de magnitude e ruídos numéricos. De acordo com Schroff, Kalenichenko e Philbin (2015), a normalização dos *embeddings* e o uso dessa métrica contribuem significativamente para a robustez dos sistemas em cenários reais, nos quais a qualidade das imagens pode variar consideravelmente.

Outro aspecto central do *deep learning* aplicado ao reconhecimento facial refere-se ao processo de treinamento dos modelos. Redes profundas exigem grandes volumes de dados rotulados para alcançar níveis elevados de generalização, sendo comum o uso de bases com milhões de imagens de faces capturadas em condições diversas. Conforme apontam Parkhi, Vedaldi e Zisserman (2015), a diversidade dos dados de treinamento é fator determinante para a capacidade do modelo em operar de forma confiável fora de ambientes controlados. Entretanto, o acesso a tais bases de dados e a infraestrutura computacional necessária para o treinamento completo desses modelos constituem barreiras significativas para muitas instituições.

Em razão dessas limitações, a utilização de modelos pré-treinados tornou-se prática recorrente em aplicações de reconhecimento facial, especialmente em contextos institucionais que demandam soluções rápidas e eficientes. Modelos pré-

treinados concentram o conhecimento adquirido em grandes bases de dados e podem ser reutilizados como componentes de sistemas específicos, reduzindo custos de desenvolvimento e riscos técnicos. Segundo Pan e Yang (2010), essa estratégia de reaproveitamento do conhecimento, conhecida como transferência de aprendizado, permite acelerar a implementação de soluções sem comprometer significativamente o desempenho.

No entanto, a adoção de modelos pré-treinados não elimina a necessidade de compreensão crítica de seus limites e implicações. Como destacam Buolamwini e Gebru (2018), sistemas de reconhecimento facial podem apresentar vieses relacionados à distribuição dos dados de treinamento, impactando de forma desigual diferentes grupos populacionais. Tal constatação reforça a importância de avaliar cuidadosamente o contexto de aplicação e de adotar medidas institucionais que mitiguem riscos associados ao uso indiscriminado dessas tecnologias.

Dessa forma, o *deep learning* aplicado ao reconhecimento facial deve ser compreendido não apenas como um avanço técnico, mas como um campo que exige articulação entre eficiência computacional, responsabilidade social e adequação institucional. Essa perspectiva orienta a análise do software desenvolvido neste trabalho, cuja arquitetura se apoia em modelos pré-treinados consolidados, mas cujo uso é delimitado por critérios operacionais e legais compatíveis com a atividade de inteligência policial.

2.3 Reconhecimento Facial na Segurança Pública

A incorporação do reconhecimento facial no campo da segurança pública deve ser compreendida como parte de um processo mais amplo de transformação das práticas de inteligência e investigação criminal, impulsionado pela digitalização das relações sociais e pela ampliação dos registros visuais disponíveis. A proliferação de câmeras de vigilância, dispositivos móveis e plataformas digitais resultou em um aumento expressivo do volume de imagens potencialmente relevantes para a atividade policial, tornando inviável a análise exclusivamente manual desses dados. A vigilância contemporânea opera em ambientes saturados de informação visual, exigindo ferramentas capazes de lidar com essa complexidade de forma sistemática (Lyon, 2003).

Nesse contexto, o reconhecimento facial emerge como tecnologia de apoio à identificação de indivíduos, permitindo a realização de buscas automatizadas em grandes bases de imagens e a geração de indícios que podem subsidiar investigações. Diferentemente de abordagens determinísticas, esses sistemas operam de maneira probabilística, fornecendo graus de similaridade que devem ser interpretados por analistas capacitados, em consonância com outros elementos informacionais disponíveis. Ratcliffe (2016) ressalta que a inteligência policial eficaz não se baseia em evidências isoladas, mas na integração de múltiplas fontes de dados, o que reforça o papel do reconhecimento facial como ferramenta auxiliar e não como mecanismo decisório autônomo.

Experiências internacionais demonstram que o uso do reconhecimento facial em ambientes policiais pode contribuir para a localização de pessoas desaparecidas, identificação de suspeitos e análise de vínculos criminais, desde que inserido em protocolos claros e supervisionados. Estudos analisados por Introna e Wood (2004) indicam que a eficácia desses sistemas depende menos da tecnologia em si e mais da forma como ela é integrada às rotinas organizacionais, aos fluxos decisórios e às práticas de responsabilização institucional. A ausência de diretrizes claras tende a ampliar riscos de uso indevido e a comprometer a legitimidade das ações policiais.

A literatura especializada aponta que soluções tecnológicas desenvolvidas internamente ou adaptadas às realidades institucionais específicas tendem a apresentar maior aderência operacional e maior controle sobre os fluxos de dados sensíveis. Diferentemente de plataformas comerciais fechadas, softwares concebidos em ambiente local permitem ajustes finos nos parâmetros de funcionamento, definição clara de responsabilidades e maior alinhamento com protocolos institucionais já consolidados. Segundo Hevner et al. (2004), artefatos tecnológicos desenvolvidos sob uma lógica orientada ao problema organizacional tendem a gerar maior valor prático quando fundamentados em uma base teórica consistente e em uma metodologia adequada de pesquisa aplicada.

No cenário brasileiro, o debate sobre o uso do reconhecimento facial na segurança pública intensificou-se nos últimos anos, especialmente diante de iniciativas pontuais adotadas por órgãos estaduais e municipais. Embora tais experiências revelem potencial tecnológico, também evidenciam desafios

significativos relacionados à governança dos dados, à transparência dos processos e à capacitação dos operadores. Conforme analisa Silva (2020), a adoção acrítica de tecnologias de vigilância pode reproduzir desigualdades estruturais e ampliar práticas discriminatórias, caso não sejam acompanhadas de salvaguardas normativas e institucionais adequadas.

A atividade de inteligência policial, em particular, demanda soluções tecnológicas que privilegiem a precisão, a rastreabilidade das análises e o controle sobre as informações sensíveis manipuladas. O reconhecimento facial, quando utilizado como ferramenta de triagem e apoio analítico, pode contribuir para a racionalização do trabalho dos analistas, reduzindo o tempo dedicado a tarefas repetitivas e ampliando a capacidade de exploração de bases de dados visuais. Segundo Ackoff (1989), a eficiência organizacional está diretamente associada à capacidade de transformar dados em informação relevante, processo no qual a automação desempenha papel central.

Entretanto, o uso dessa tecnologia em contextos policiais também levanta preocupações relacionadas à proteção de direitos fundamentais, à presunção de inocência e à privacidade dos cidadãos. Autores como Zuboff (2019) e Brakel (2016) alertam que sistemas de reconhecimento facial podem ser incorporados a lógicas de vigilância excessiva se não forem limitados por princípios claros de necessidade, proporcionalidade e finalidade. Tais preocupações são particularmente relevantes em países com histórico de desigualdade social e seletividade penal, exigindo cautela redobrada na implementação dessas soluções.

Nesse sentido, a literatura aponta para a necessidade de modelos de uso do reconhecimento facial que priorizem o controle institucional, a transparência dos procedimentos e a possibilidade de auditoria dos sistemas empregados. Conforme argumentam Mittelstadt et al. (2016), a responsabilização no uso de sistemas baseados em inteligência artificial depende da clareza quanto aos papéis humanos envolvidos, aos critérios adotados e às limitações técnicas das ferramentas utilizadas. A adoção de softwares desenvolvidos ou adaptados internamente pode contribuir para esse controle, ao permitir maior compreensão do funcionamento do sistema e maior alinhamento com normativas locais.

Assim, o reconhecimento facial na segurança pública deve ser compreendido como tecnologia de apoio estratégico à inteligência policial, cujo valor reside na capacidade de ampliar a eficiência analítica sem comprometer princípios legais e éticos. Essa perspectiva orienta a proposta apresentada neste trabalho, que descreve o desenvolvimento de um software concebido para operar como instrumento auxiliar, integrado às práticas existentes e sujeito à interpretação crítica dos profissionais responsáveis pela análise final das informações.

2.4 Aspectos Éticos, Legais e Proteção de Dados Pessoais

A utilização de sistemas de reconhecimento facial no contexto da inteligência policial impõe a necessidade de uma reflexão aprofundada acerca de seus desdobramentos éticos e legais, especialmente diante do caráter sensível dos dados biométricos envolvidos. A face humana, enquanto identificador biométrico, possui elevada capacidade de individualização, o que confere aos sistemas que a utilizam um potencial significativo de impacto sobre direitos fundamentais como a privacidade, a dignidade da pessoa humana e a presunção de inocência. Conforme destaca Floridi et al. (2018), tecnologias baseadas em inteligência artificial não são neutras, devendo ser analisadas à luz dos valores sociais e jurídicos que orientam sua aplicação.

No campo ético, um dos principais desafios associados ao reconhecimento facial refere-se ao risco de ampliação de práticas de vigilância desproporcionais, sobretudo quando a tecnologia é empregada sem critérios claros de finalidade e necessidade. Autores como Lyon (2018) argumentam que a normalização de mecanismos de vigilância automatizada pode alterar de forma profunda a relação entre o Estado e os cidadãos, produzindo efeitos de autocensura e erosão da confiança institucional. Nesse sentido, a adoção de sistemas de reconhecimento facial deve ser acompanhada de diretrizes que limitem seu uso a contextos específicos e devidamente justificados.

Outro aspecto ético relevante diz respeito à possibilidade de vieses algorítmicos, fenômeno amplamente discutido na literatura contemporânea. Estudos conduzidos por Buolamwini e Gebru (2018) demonstraram que sistemas de reconhecimento facial podem apresentar desempenhos desiguais entre diferentes grupos populacionais, em função da composição dos conjuntos de dados utilizados

em seu treinamento. Tal constatação reforça a necessidade de cautela na interpretação dos resultados gerados por esses sistemas, bem como a importância de que decisões críticas não sejam fundamentadas exclusivamente em outputs automatizados.

Do ponto de vista jurídico, o uso de dados biométricos no Brasil encontra-se submetido às disposições da Lei Geral de Proteção de Dados Pessoais, que classifica tais informações como dados pessoais sensíveis. O tratamento desse tipo de dado exige observância rigorosa de princípios como finalidade, adequação, necessidade, transparência e segurança, sendo imprescindível a existência de base legal específica para sua coleta e utilização (LGPD,2018). No contexto da segurança pública, embora a legislação preveja exceções, essas não afastam a obrigação de adoção de medidas de governança e proteção adequadas.

A atividade de inteligência policial, por sua natureza, opera em uma zona de tensão entre a necessidade de eficácia investigativa e a preservação de garantias individuais. Nesse cenário, o reconhecimento facial deve ser compreendido como ferramenta auxiliar, cujo uso precisa estar integrado a protocolos institucionais claros e submetido à supervisão humana qualificada. Conforme observa Barroso (2020), o desafio contemporâneo do Estado reside em equilibrar inovação tecnológica e proteção de direitos, evitando tanto a paralisia normativa quanto o uso irrestrito de tecnologias potencialmente invasivas.

A transparência dos processos e a rastreabilidade das análises realizadas constituem elementos centrais para a legitimidade do uso do reconhecimento facial em ambientes policiais. Sistemas que permitem a documentação das etapas de processamento, a explicitação dos critérios adotados e a revisão dos resultados contribuem para a responsabilização institucional e para a mitigação de abusos. Segundo Mittelstadt et al. (2016), a *accountability* em sistemas baseados em inteligência artificial depende diretamente da capacidade de compreender e explicar seus funcionamentos, ainda que de forma simplificada.

Nesse sentido, a opção por desenvolver soluções tecnológicas de reconhecimento facial em ambiente local e sob controle institucional pode representar vantagem significativa em relação a plataformas externas ou proprietárias. O domínio

sobre a arquitetura do sistema, seus parâmetros de funcionamento e seus fluxos de dados favorece a adequação às exigências legais e éticas, além de possibilitar ajustes conforme orientações normativas futuras. Essa perspectiva está alinhada ao entendimento de Hevner et al. (2004), segundo o qual artefatos tecnológicos devem ser concebidos considerando não apenas sua eficiência técnica, mas também seu impacto organizacional e social.

Dessa forma, os aspectos éticos e legais não constituem elementos acessórios, mas dimensões centrais na análise de sistemas de reconhecimento facial aplicados à inteligência policial. A compreensão desses fatores é fundamental para contextualizar o software descrito neste trabalho, delimitando seu uso como instrumento de apoio analítico, orientado por princípios de responsabilidade, proporcionalidade e respeito aos direitos fundamentais, e preparando o terreno para a apresentação da metodologia e do desenvolvimento técnico do artefato nos capítulos subsequentes.

2.5 Framework InsightFace

O avanço dos sistemas de reconhecimento facial baseados em *deep learning* impulsionou o surgimento de *frameworks* especializados capazes de integrar, de forma eficiente, modelos de detecção, alinhamento e extração de características faciais. Entre essas soluções, o InsightFace destaca-se como um dos *frameworks* de código aberto mais difundidos na literatura científica e em aplicações práticas, em razão de sua robustez, desempenho e aderência a padrões contemporâneos de pesquisa em visão computacional. Segundo Deng et al. (2019), o InsightFace foi concebido com o objetivo de fornecer um ambiente unificado para experimentação e implantação de modelos de reconhecimento facial em larga escala.

O InsightFace estrutura-se a partir de modelos de aprendizado profundo previamente treinados em grandes bases de dados faciais, permitindo a extração de *embeddings* altamente discriminantes mesmo em condições adversas de captura de imagem. Esses modelos incorporam arquiteturas modernas de redes neurais convolucionais, combinadas com funções de perda específicas para maximizar a separabilidade entre indivíduos no espaço vetorial. Conforme demonstrado por Wang et al. (2018), a utilização de funções de perda angulares contribui para aumentar a margem entre classes, resultando em representações mais estáveis e precisas.

Um dos diferenciais do InsightFace reside na integração entre detecção facial e reconhecimento propriamente dito, reduzindo erros acumulados ao longo do pipeline de processamento. A etapa de detecção identifica a presença e a localização da face na imagem, enquanto o alinhamento ajusta a posição dos principais pontos faciais, garantindo que a extração de características ocorra de maneira consistente. De acordo com Li et al. (2015), o alinhamento adequado da face exerce influência direta sobre a qualidade dos *embeddings* gerados, impactando o desempenho global do sistema.

Além disso, o InsightFace foi projetado para operar de forma eficiente em ambientes com recursos computacionais limitados, característica particularmente relevante para aplicações institucionais que não dispõem de infraestrutura de alto desempenho. A possibilidade de execução em unidades centrais de processamento, aliada à flexibilidade de configuração dos parâmetros de detecção e extração, amplia o espectro de uso do framework em contextos reais. Segundo Howard et al. (2017), a eficiência computacional constitui fator crítico para a adoção de soluções de visão computacional fora de ambientes laboratoriais.

No contexto deste trabalho, a escolha do InsightFace fundamenta-se em sua maturidade técnica, ampla validação na literatura e facilidade de integração com bibliotecas consolidadas da linguagem Python. O *framework* permite a geração de *embeddings* faciais de alta dimensionalidade, os quais podem ser armazenados, normalizados e comparados de maneira eficiente, viabilizando operações de busca em bases de dados extensas. Essa característica é especialmente relevante para a inteligência policial, onde o volume de imagens analisadas tende a crescer continuamente.

Outro aspecto relevante refere-se à modularidade do InsightFace, que possibilita a substituição ou atualização de componentes específicos do sistema sem a necessidade de reestruturação completa do software. Tal flexibilidade favorece a manutenção evolutiva do artefato tecnológico, permitindo sua adaptação a novos requisitos operacionais ou a avanços futuros na área de reconhecimento facial. Conforme argumentam Bass, Clements e Kazman (2012), arquiteturas modulares contribuem significativamente para a sustentabilidade de sistemas complexos ao longo do tempo.

Apesar de suas vantagens, o uso do InsightFace não elimina a necessidade de uma compreensão crítica de suas limitações e pressupostos. O desempenho do *framework* depende da qualidade dos dados de entrada, das condições de captura das imagens e da adequação dos parâmetros adotados. Ademais, como todo sistema baseado em aprendizado profundo, o InsightFace herda características dos conjuntos de dados utilizados em seu treinamento, o que exige cautela quanto à generalização dos resultados em contextos específicos. Essa preocupação é amplamente discutida por Mehrabi et al. (2021), ao analisarem os riscos associados a vieses algorítmicos em sistemas de inteligência artificial.

Assim, a adoção do InsightFace no desenvolvimento do software descrito neste trabalho fundamenta-se em uma escolha técnica consistente, alinhada às exigências de eficiência, robustez e adaptabilidade da inteligência policial, sem desconsiderar a necessidade de uso responsável e contextualizado da tecnologia. A compreensão de seu funcionamento e de suas implicações constitui elemento essencial para a análise do artefato apresentado, preparando o terreno para a descrição da arquitetura e do fluxo operacional do sistema desenvolvido.

3 METODOLOGIA

A metodologia adotada neste Trabalho de Conclusão de Curso fundamenta-se em uma abordagem aplicada, de natureza tecnológica e caráter descritivo, com foco na apresentação e análise do desenvolvimento de um artefato computacional voltado à inteligência policial. O estudo não tem como objetivo a validação empírica do software em ambiente institucional real, mas a descrição sistemática de seu processo de concepção, arquitetura e funcionamento, conforme as diretrizes de pesquisas orientadas à solução de problemas práticos. Segundo Gil (2019), pesquisas aplicadas buscam gerar conhecimentos direcionados à resolução de demandas concretas, mantendo rigor científico sem a exigência de experimentação controlada.

Do ponto de vista dos procedimentos técnicos, o trabalho enquadra-se como um artigo tecnológico, modalidade que privilegia a apresentação de soluções inovadoras desenvolvidas a partir de conhecimentos científicos consolidados. Essa tipologia é adequada quando o foco reside no artefato produzido e em sua contribuição prática, e não na mensuração estatística de resultados. A metodologia adotada busca

garantir coerência entre o problema identificado, a solução proposta e a descrição técnica apresentada (Dresch, Lacerda e Antunes Júnior, 2015; Wazlawick, 2021).

Como estratégia metodológica central, este trabalho adota os pressupostos da *Design Science Research*, abordagem amplamente utilizada em pesquisas na área de sistemas de informação e engenharia de software. A *Design Science Research* parte da identificação de um problema relevante em um contexto organizacional e propõe o desenvolvimento de um artefato capaz de contribuir para sua solução. Segundo Hevner et al. (2004), essa abordagem enfatiza a utilidade, a inovação e a fundamentação teórica do artefato, elementos que orientam a estrutura deste estudo.

A aplicação da *Design Science Research* neste trabalho ocorreu de forma adaptada, considerando a natureza descritiva do artigo tecnológico. A primeira etapa consistiu na identificação do problema operacional enfrentado por setores de inteligência policial, relacionado à lentidão e à limitação dos métodos manuais de identificação facial em grandes volumes de imagens. Essa etapa baseou-se na observação prática do contexto de uso e na análise da literatura sobre inteligência policial e reconhecimento facial.

A segunda etapa envolveu a definição dos objetivos da solução, estabelecendo-se que o artefato deveria automatizar a detecção e comparação de faces, operar de forma local, permitir controle institucional sobre os dados e apresentar interface acessível ao usuário final. Esses objetivos orientaram as decisões técnicas relacionadas à escolha das linguagens, bibliotecas e modelos de reconhecimento facial empregados no desenvolvimento do software.

Na terceira etapa, realizou-se o desenvolvimento do artefato tecnológico, denominado Face Finder InsightFace Pro. Essa fase contemplou a implementação da arquitetura modular do sistema, a integração do *framework* de reconhecimento facial, a construção da interface gráfica e a definição do fluxo operacional do software. Ressalta-se que o desenvolvimento técnico foi realizado previamente à elaboração deste trabalho, sendo o código de responsabilidade exclusiva do discente.

A quarta etapa consistiu na organização e comunicação do conhecimento produzido, por meio da descrição detalhada do software, de sua arquitetura e de seu

funcionamento, bem como da discussão dos resultados esperados e das limitações identificadas. Conforme afirmam Peffers et al. (2007), a comunicação clara do artefato e de seu contexto de aplicação é elemento essencial da *Design Science Research*, permitindo que outros pesquisadores e profissionais compreendam sua utilidade e possibilidades de adaptação.

Como delimitação metodológica, destaca-se que este trabalho não contempla testes comparativos, métricas de desempenho, validação estatística ou aplicação oficial do software em operações policiais. Tais etapas são compreendidas como possibilidades futuras de pesquisa e desenvolvimento, não constituindo objetivo deste estudo. Essa delimitação preserva a coerência entre a proposta do artigo tecnológico e o escopo de um Trabalho de Conclusão de Curso.

Dessa forma, a metodologia adotada assegura alinhamento entre o problema identificado, a solução desenvolvida e a forma de apresentação do trabalho, conferindo rigor acadêmico à descrição do software de reconhecimento facial e estabelecendo bases consistentes para a análise de sua contribuição no contexto da inteligência policial.

4 DESENVOLVIMENTO DO SOFTWARE

O desenvolvimento do software Face Finder InsightFace Pro foi orientado pela necessidade de oferecer uma solução tecnológica capaz de apoiar atividades de inteligência policial por meio da automação do processo de reconhecimento facial, mantendo simplicidade operacional, controle local dos dados e flexibilidade de uso. O sistema foi concebido como um artefato computacional de natureza modular, desenvolvido na linguagem Python, integrando bibliotecas consolidadas de visão computacional, aprendizado profundo e construção de interfaces gráficas.

A concepção do software partiu do entendimento de que soluções voltadas à inteligência policial devem priorizar eficiência, rastreabilidade e facilidade de operação, uma vez que os usuários finais nem sempre possuem formação técnica avançada em computação. Conforme Pressman e Maxim (2020), a engenharia de software aplicada a contextos organizacionais sensíveis deve equilibrar robustez

técnica e usabilidade, garantindo que a tecnologia atue como facilitadora do trabalho humano.

4.1 Arquitetura Geral do Sistema

A arquitetura do Face Finder InsightFace Pro foi estruturada em módulos funcionais independentes, permitindo organização lógica do código e facilidade de manutenção. O sistema é composto, de forma geral, por cinco módulos principais: gerenciamento de arquivos e diretórios, processamento facial, armazenamento de *embeddings*, interface gráfica e controle de fluxo e execução. Essa organização modular segue boas práticas de engenharia de software, favorecendo a extensibilidade do sistema (Bass, Clements, Kazman, 2012).

O núcleo do processamento facial é responsável pela detecção de faces, extração de *embeddings* e normalização dos vetores gerados. Esse módulo integra o *framework* de reconhecimento facial baseado em *deep learning*, sendo acionado tanto no processamento do banco de imagens quanto na análise da imagem de referência utilizada nas buscas. A separação desse núcleo em relação à interface gráfica permite que o processamento ocorra de forma independente, reduzindo acoplamentos desnecessários.

4.2 Tecnologias Utilizadas

O software foi desenvolvido integralmente em Python, linguagem amplamente utilizada em aplicações de ciência de dados e inteligência artificial, em razão de sua legibilidade, vasto ecossistema de bibliotecas e facilidade de integração. Para o processamento de imagens, utilizou-se a biblioteca OpenCV, reconhecida por sua eficiência em operações de visão computacional. A extração de características faciais foi realizada por meio de um *framework* especializado de reconhecimento facial baseado em aprendizado profundo, previamente treinado em grandes bases de dados.

Para a construção da interface gráfica, adotou-se a biblioteca Tkinter, que permite o desenvolvimento de aplicações desktop de forma simples e multiplataforma. A escolha dessa tecnologia teve como objetivo facilitar a interação do usuário com o sistema, possibilitando a seleção de imagens, definição de parâmetros de busca e

visualização dos resultados de maneira intuitiva. Segundo Nielsen (2012), interfaces claras e objetivas são essenciais para reduzir erros operacionais em sistemas críticos.

O armazenamento dos *embeddings* faciais foi implementado utilizando a biblioteca *Pickle* do Python para serialização binária de objetos, permitindo o reaproveitamento dos vetores previamente extraídos sem a necessidade de reprocessamento constante das imagens. Essa estratégia contribui para a eficiência do sistema, especialmente em bases de dados com grande volume de arquivos, conforme ressaltam Tanenbaum e Bos (2015) ao tratarem de otimização de sistemas computacionais. O banco de dados dos *embeddings* já processados fica armazenado em uma pasta local do computador do usuário.

4.3 Fluxo de Funcionamento do Software

O fluxo operacional do Face Finder InsightFace Pro inicia-se com a definição do diretório de busca, no qual estão armazenadas as imagens a serem processadas. O sistema realiza uma varredura recursiva nesse diretório, identificando arquivos compatíveis com os formatos suportados. As imagens ainda não processadas são submetidas ao módulo de detecção facial, que identifica a presença de faces e extrai os *embeddings* correspondentes.

Uma vez extraídos, os *embeddings* são normalizados e armazenados em um banco local, associado a metadados que registram informações como data de processamento e quantidade de faces detectadas. Esse banco de dados local constitui a base de comparação utilizada nas buscas posteriores, permitindo que o sistema opere de forma incremental e eficiente.

Na etapa de busca, o usuário seleciona uma imagem de referência, que é submetida ao mesmo processo de detecção e extração de características. O *embedding* gerado é então comparado com os vetores armazenados no banco local, utilizando uma métrica de similaridade baseada em cálculo vetorial. Os resultados são ordenados de acordo com o grau de similaridade e apresentados ao usuário de forma visual, acompanhados de informações percentuais que auxiliam a interpretação dos achados.

4.4 Modos de Busca e Parâmetros Operacionais

O software disponibiliza diferentes modos de busca, permitindo ao usuário ajustar o nível de rigor da comparação facial conforme o contexto da análise. Modos mais restritivos priorizam maior similaridade entre os vetores, reduzindo a quantidade de resultados retornados, enquanto modos mais amplos permitem a identificação de correspondências com menor grau de similaridade. Essa flexibilidade é fundamental em atividades de inteligência, nas quais diferentes cenários demandam estratégias analíticas distintas (Ratcliffe, 2016).

Os parâmetros operacionais foram definidos de modo a equilibrar sensibilidade e precisão, evitando tanto a geração excessiva de falsos positivos quanto a perda de correspondências relevantes. Ressalta-se que os valores adotados não possuem caráter determinístico, devendo ser interpretados como apoio à análise humana e não como conclusão automática.

4.5 Empacotamento e Execução

Com o objetivo de facilitar a distribuição e o uso do software em ambientes institucionais, o sistema foi empacotado como aplicação executável independente. Essa estratégia elimina a necessidade de instalação manual de dependências e configurações complexas, reduzindo barreiras técnicas à adoção da ferramenta. A simplificação do processo de implantação é fator determinante para a aceitação de sistemas computacionais em organizações públicas (Sommerville, 2016).

Dessa forma, o desenvolvimento do Face Finder InsightFace Pro resultou em um artefato tecnológico funcional, modular e orientado ao contexto da inteligência policial, cuja descrição técnica fornece base sólida para a compreensão de seu funcionamento, de suas potencialidades e de suas limitações, aspectos que serão discutidos na seção seguinte.

5 RESULTADOS ESPERADOS E DISCUSSÃO

Os resultados esperados com o desenvolvimento do software Face Finder InsightFace Pro estão diretamente relacionados à otimização dos processos de identificação facial no contexto da inteligência policial, especialmente no que se refere à redução do tempo de análise e à padronização dos procedimentos. A automação da detecção e comparação de faces tende a minimizar a dependência de análises

exclusivamente manuais, permitindo que os analistas concentrem seus esforços em atividades de maior complexidade interpretativa. Segundo Davenport e Harris (2017), o uso estratégico de tecnologias analíticas contribui para o aumento da eficiência organizacional quando integrado a fluxos decisórios bem definidos.

Espera-se que o software possibilite a realização de buscas em grandes volumes de imagens de forma mais célere e sistemática, ampliando a capacidade de exploração de bases visuais acumuladas ao longo das atividades policiais. A utilização de *embeddings* faciais e métricas matemáticas de similaridade favorece a uniformização das análises, reduzindo variações subjetivas inerentes à comparação visual humana. Conforme destacam Jain, Ross e Nandakumar (2011), a padronização é um dos principais benefícios da adoção de sistemas biométricos em ambientes institucionais.

Outro resultado esperado refere-se ao fortalecimento da rastreabilidade das análises realizadas. Ao estruturar o processo de reconhecimento facial em etapas claramente definidas, o software contribui para a documentação dos procedimentos adotados, aspecto fundamental para a transparência e a responsabilização institucional. Mittelstadt et al. (2016) ressaltam que a explicitação dos processos técnicos é condição essencial para a legitimidade do uso de sistemas baseados em inteligência artificial em contextos sensíveis.

No âmbito da discussão, é importante destacar que os resultados gerados pelo software devem ser interpretados como indícios analíticos, e não como conclusões definitivas. O reconhecimento facial opera de forma probabilística, fornecendo graus de similaridade que necessitam ser avaliados em conjunto com outras informações disponíveis no processo investigativo. Ratcliffe (2016) enfatiza que a inteligência policial eficaz depende da integração de múltiplas fontes de dados e da análise contextualizada das informações, não sendo recomendável a adoção de soluções tecnológicas como mecanismos decisórios autônomos.

Entre as limitações esperadas do sistema, destaca-se a dependência da qualidade das imagens utilizadas. Fatores como iluminação inadequada, baixa resolução, ângulos desfavoráveis e obstruções faciais podem comprometer a precisão dos *embeddings* gerados, impactando os resultados das comparações. Conforme

apontam Bowyer, Chang e Flynn (2016), tais limitações são inerentes aos sistemas de reconhecimento facial e devem ser consideradas na definição de protocolos de uso.

Outra limitação refere-se à ausência de validação empírica formal no contexto institucional, uma vez que este trabalho não contempla testes operacionais ou mensuração estatística de desempenho. Essa delimitação metodológica restringe a possibilidade de generalização dos resultados, mas é coerente com a natureza descritiva do artigo tecnológico. Conforme Peffers et al. (2007), a avaliação empírica constitui etapa posterior na *Design Science Research*, podendo ser explorada em estudos futuros.

Apesar dessas limitações, o software apresenta potencial significativo como ferramenta de apoio à inteligência policial, especialmente por operar de forma local, permitir controle institucional dos dados e oferecer flexibilidade na definição dos parâmetros de busca. Esses aspectos contribuem para a adequação da solução às exigências legais e operacionais do contexto brasileiro (LGPD, 2018).

Assim, os resultados esperados indicam que o Face Finder InsightFace Pro pode atuar como instrumento complementar às práticas existentes de inteligência policial, ampliando a eficiência analítica sem substituir o julgamento humano, desde que utilizado de forma responsável, supervisionada e alinhada a protocolos institucionais claros.

6 CONCLUSÃO

Este Trabalho de Conclusão de Curso teve como objetivo descrever o desenvolvimento de um software de reconhecimento facial aplicado ao contexto da inteligência policial, tomando como estudo de caso o Face Finder InsightFace Pro. Partindo da constatação das limitações dos métodos manuais de identificação facial, especialmente diante do aumento exponencial do volume de imagens disponíveis, o trabalho buscou apresentar uma solução tecnológica orientada à automação, padronização e apoio à análise humana, sem a pretensão de substituir o julgamento do analista.

Ao longo do estudo, foram apresentados os fundamentos teóricos do reconhecimento facial, do *deep learning* e da visão computacional, bem como as especificidades do uso dessas tecnologias no âmbito da segurança pública. A adoção de modelos baseados em *embeddings* faciais e métricas de similaridade demonstrou-se adequada para operações de busca em bases extensas de imagens, conforme indicado pela literatura especializada. Autores como Jain, Ross e Nandakumar (2011) e Zhao et al. (2019) ressaltam que tais abordagens representam o estado da arte em sistemas biométricos contemporâneos.

A metodologia adotada, fundamentada na Design Science Research, mostrou-se coerente com a natureza tecnológica do trabalho, permitindo estruturar a descrição do artefato a partir de um problema prático relevante. A organização do desenvolvimento em etapas claras, desde a identificação do problema até a comunicação do conhecimento produzido, conferiu rigor acadêmico à apresentação do software (Hevner et al., 2004; Peffers et al., 2007).

A descrição técnica do Face Finder InsightFace Pro evidenciou uma arquitetura modular, orientada à eficiência operacional e ao controle local dos dados, características especialmente relevantes no contexto da inteligência policial. A possibilidade de operar sem dependência de serviços externos, aliada à flexibilidade na definição dos parâmetros de busca, contribuiu para a adequação do software às exigências legais e institucionais brasileiras (LGPD, 2018).

Os resultados esperados indicam que o software pode atuar como ferramenta de apoio à inteligência policial, reduzindo o tempo de análise, padronizando procedimentos e ampliando a capacidade de exploração de bases visuais. Contudo, reforça-se que os resultados gerados devem ser interpretados como indícios analíticos, estando sujeitos à avaliação crítica dos profissionais responsáveis. Conforme aponta Ratcliffe (2016), a inteligência policial eficaz depende da integração entre tecnologia, análise humana e contexto investigativo.

Entre as limitações do estudo, destaca-se a ausência de validação empírica formal e de métricas quantitativas de desempenho, as quais não constituíram objetivo deste trabalho. Essas limitações abrem espaço para pesquisas futuras, que poderão explorar avaliações comparativas, testes operacionais controlados e análises de

impacto organizacional, aprofundando a compreensão sobre o uso do reconhecimento facial em ambientes policiais.

Conclui-se, portanto, que o desenvolvimento do Face Finder InsightFace Pro representa uma contribuição relevante no campo dos artigos tecnológicos aplicados à segurança pública, ao demonstrar como soluções baseadas em inteligência artificial podem ser concebidas de forma responsável, contextualizada e alinhada às demandas reais da inteligência policial, preservando princípios legais, éticos e institucionais.

REFERÊNCIAS

ACKOFF, Russell L. From data to wisdom. **Journal of Applied Systems Analysis**, Lancaster, v. 16, p. 3-9, 1989.

BARROSO, Luís Roberto. Inteligência artificial, direitos fundamentais e o direito. **Revista Brasileira de Direito Público**, Belo Horizonte, v. 18, n. 99, p. 9-36, abr./jun. 2020.

BASS, Len; CLEMENTS, Paul; KAZMAN, Rick. **Software architecture in practice**. 3. ed. Boston: Addison-Wesley, 2012.

BOWYER, Kevin W.; CHANG, Kyong I.; FLYNN, Patrick J. A survey of approaches and challenges in 3D and multi-modal 3D+2D face recognition. **Computer Vision and Image Understanding**, San Diego, v. 101, n. 1, p. 1-15, 2006.

BRAKEL, Rosamunde van. Pre-emptive big data surveillance and its (dis)empowering consequences: the case of predictive policing. **Netherlands Journal of Legal Philosophy**, The Hague, v. 45, n. 1, p. 117-135, 2016.

BRASIL. [Lei Geral de Proteção de Dados Pessoais (LGPD)]. **Lei nº 13.709, de 14 de agosto de 2018**. Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 fev. 2026.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: intersectional accuracy disparities in commercial gender classification. *In*: CONFERENCE ON FAIRNESS,

ACCOUNTABILITY AND TRANSPARENCY, 1., 2018, New York. **Proceedings** [...]. New York: PMLR, 2018. p. 77-91.

(Proceedings of Machine Learning Research, v. 81). Disponível em: <http://proceedings.mlr.press/v81/buolamwini18a.html>. Acesso em: 9 fev. 2026.

DAVENPORT, Thomas H.; HARRIS, Jeanne G. **Competing on analytics: the new science of winning**. Boston: Harvard Business Review Press, 2017.

DAVENPORT, Thomas H.; KIRBY, Julia. **Only humans need apply: winners and losers in the age of smart machines**. New York: Harper Business, 2016.

DENG, Jiankang *et al.* ArcFace: additive angular margin loss for deep face recognition. *In: IEEE/CVF CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION (CVPR), 2019, Long Beach. Proceedings* [...]. Los Alamitos: IEEE, 2019. p. 4690-4699.

DRESCH, Aline; LACERDA, Daniel Pacheco; ANTUNES JÚNIOR, José Antônio Valle. **Design science research**: método de pesquisa para avanço da ciência e tecnologia. Porto Alegre: Bookman, 2015.

FLORIDI, Luciano *et al.* AI4People: an ethical framework for a good AI society: opportunities, risks, principles, and recommendations. **Minds and Machines**, Dordrecht, v. 28, n. 4, p. 689-707, dez. 2018.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 7. ed. São Paulo: Atlas, 2019.

GOODFELLOW, Ian; BENGIO, Yoshua; COURVILLE, Aaron. **Deep learning**. Cambridge: MIT Press, 2016.

HEVNER, Alan R. *et al.* Design science in information systems research. **MIS Quarterly**, Minneapolis, v. 28, n. 1, p. 75-105, mar. 2004.

HOWARD, Andrew G. *et al.* MobileNets: efficient convolutional neural networks for mobile vision applications. Ithaca: Cornell University Library, 2017.

arXiv:1704.04861. Disponível em: <https://arxiv.org/abs/1704.04861>. Acesso em: 10 fev. 2026.

INTRONA, Lucas D.; WOOD, David. Picturing algorithmic surveillance: the politics of facial recognition systems. **Surveillance & Society**, Newcastle upon Tyne, v. 2, n. 2/3, p. 177-198, 2004.

JAIN, Anil K.; FLYNN, Patrick; ROSS, Arun A. (Ed.). **Handbook of biometrics**. New York: Springer, 2008.

JAIN, Anil K.; ROSS, Arun A.; NANDAKUMAR, Karthik. **Introduction to biometrics**. New York: Springer, 2011.

KITCHIN, Rob. **The data revolution: big data, open data, data infrastructures and their consequences**. London: Sage, 2014.

LECUN, Yann; BENGIO, Yoshua; HINTON, Geoffrey. Deep learning. **Nature**, London, v. 521, n. 7553, p. 436-444, maio 2015.

LI, Stan Z.; JAIN, Anil K. Face recognition. *In*: JAIN, Anil K.; FLYNN, Patrick; ROSS, Arun A. (Ed.). **Handbook of biometrics**. New York: Springer, 2008. p. 1-30.

LI, Haoxiang *et al.* A convolutional neural network cascade for face detection. *In*: IEEE CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION (CVPR), 2015, Boston. **Proceedings** [...]. Los Alamitos: IEEE, 2015. p. 5325-5334.

LYON, David (Ed.). **Surveillance as social sorting: privacy, risk and digital discrimination**. London: Routledge, 2003.

LYON, David. **The culture of surveillance: watching as a way of life**. Cambridge: Polity Press, 2018.

MARR, David. **Vision: a computational investigation into the human representation and processing of visual information**. San Francisco: W. H. Freeman, 1982.

MEHRABI, Ninareh *et al.* A survey on bias and fairness in machine learning. **ACM Computing Surveys**, New York, v. 54, n. 6, art. 115, p. 1-35, jul. 2021.

MITTELSTADT, Brent D. *et al.* The ethics of algorithms: mapping the debate. **Big Data & Society**, London, v. 3, n. 2, p. 1-21, jul./dez. 2016.

NIELSEN, Jakob. **Usability engineering**. San Diego: Morgan Kaufmann, 1993.

PAN, Sinno Jialin; YANG, Qiang. A survey on transfer learning. **IEEE Transactions on Knowledge and Data Engineering**, Los Alamitos, v. 22, n. 10, p. 1345-1359, out. 2010.

PARKHI, Omkar M.; VEDALDI, Andrea; ZISSERMAN, Andrew. Deep face recognition. *In: BRITISH MACHINE VISION CONFERENCE (BMVC), 2015, Swansea. Proceedings [...]*. Swansea: BMVA Press, 2015. art. 41, p. 1-12

PEFFERS, Ken *et al.* A design science research methodology for information systems research. **Journal of Management Information Systems**, Armonk, v. 24, n. 3, p. 45-77, 2007.

PRESSMAN, Roger S.; MAXIM, Bruce R. **Software engineering: a practitioner's approach**. 9. ed. New York: McGraw-Hill, 2020.

RATCLIFFE, Jerry H. **Intelligence-led policing**. 2. ed. London: Routledge, 2016.

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 [...]*. Los Alamitos: IEEE, 2015. p. 815-823.

SILVA, Tarcizio. **Racismo algorítmico: inteligência artificial e discriminação nas redes digitais**. São Paulo: Edições Sesc São Paulo, 2022.

SOMMERVILLE, Ian. **Software engineering**. 10. ed. Boston: Pearson, 2016.

TAIGMAN, Yaniv *et al.* DeepFace: closing the gap to human-level performance in face verification. *In: IEEE CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION (CVPR), 2014, Columbus. Proceedings [...]*. Los Alamitos: IEEE, 2014. p. 1701-1708.

TANENBAUM, Andrew S.; BOS, Herbert. **Modern operating systems**. 4. ed. Boston: Pearson, 2015.

TURK, Matthew; PENTLAND, Alex. Eigenfaces for recognition. **Journal of Cognitive Neuroscience**, Cambridge, v. 3, n. 1, p. 71-86, 1991.

WAZLAWICK, Raul S. **Metodologia de pesquisa para ciência da computação**. 3. ed. Rio de Janeiro: LTC, 2021.

ZHAO, Wenyi *et al.* Face recognition: a literature survey. **ACM Computing Surveys**, New York, v. 35, n. 4, p. 399-458, dez. 2003.

ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. New York: PublicAffairs, 2019.