UNIVERSIDADE FEDERAL DE SERGIPE

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Desafios no uso de reconhecimento facial em sistemas de vídeo monitoramento no Brasil

Dissertação de Mestrado

Sálvio Roberto Freitas Reis

São Cristóvão – Sergipe

2025

UNIVERSIDADE FEDERAL DE SERGIPE

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Sálvio Roberto Freitas Reis

Desafios no uso de reconhecimento facial em sistemas de vídeo monitoramento no Brasil

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Sergipe como requisito parcial para a obtenção do título de mestre em Ciência da Computação.

Orientador(a): Rafael Oliveira Vasconcelos

São Cristóvão – Sergipe

2025

Este trabalho é dedicado a todo aquele que, em algum momento,
sofreu ou sofre com preconceito no âmbito digital.

Agradecimentos

A jornada de um mestrado é repleta de desafios, aprendizados e transformações, e seria impossível chegar ao fim sem o apoio e a colaboração de tantas pessoas que estiveram ao meu lado ao longo desse caminho.

Primeiramente, agradeço a Deus, pela força e resiliência que me permitiram superar os momentos mais difíceis e celebrar as conquistas.

Agradeço a minha família, em especial, minha esposa Tatiane , meu filho João Guilherme, minha mãe Valdira, meu pai Saulo, minha irmã Aline, enfim, minha base inabalável, que sempre acreditou no meu potencial e me deu suporte, mesmo quando o tempo e a dedicação ao estudo pareciam afastar-me. A paciência, o amor e o incentivo de vocês foram fundamentais.

Ao meu orientador, Rafael Oliveira Vasconcelos, por todos os conselhos valiosos, puxões de orelha mais do que merecidos e principalmente todo o conhecimento que um discente pode adquirir. Agradeço também a todos os professores do PROCC - Programa de Pós-Gradução em Ciência da Computação da UFS, que compartilharam seu conhecimento com generosidade e sabedoria, guiando-me com paciência e rigor científico. Suas palavras de motivação e conselhos não apenas enriqueceram minha pesquisa, mas também me moldaram como pesquisador e como pessoa.

Ao meu eterno coordenador, professor Leonardo Nogueira Matos, igualmente, a minha querida amiga Elaine Silva Lima, que me ajudaram desde o início, tirando todas as minhas dúvidas de forma sempre paciente e amiga. Não faltaram palavras de incentivo e não tenho como agradecer por todas orientações ao longo desta jornada.

A todos os colaboradores da Universidade Federal de Sergipe, que me acolheram, oferecendo não apenas recursos materiais, mas também um ambiente desafiador e estimulante, no qual pude me desenvolver academicamente e pessoalmente.

Aos colegas de pesquisa e amigos que adquiri durante essa trajetória, minha eterna gratidão pelas discussões enriquecedoras, pelas horas de trabalho e pelas conversas que aliviaram a pressão de um percurso tão intenso. Em especial Tácito Junior, Márcio Feitoza, Rodrigo Cavalcante, entre diversos e igualmente valiosos amigos. Vocês me ensinaram que a ciência é construída coletivamente e que o apoio mútuo é a essência do progresso.

Por fim, deixo aqui meu reconhecimento a todos que, direta ou indiretamente, contribuíram para que eu pudesse realizar este sonho. Esta dissertação não é apenas o fruto do meu esforço, mas também da soma de incentivos, aprendizados e inspirações que recebi ao longo dessa jornada.

A todos, o meu mais sincero muito obrigado. Cada um de você foi muito importante nesta longa caminhada.

Justiça,
Em nome disso eles são pagos
Mas a noção que se tem
É limitada e eu sei, que a lei
É implacável com os oprimidos
Tornam bandidos os que eram pessoas de bem
Pois já é tão claro que é mais fácil dizer
Que eles são os certos e o culpado é você
Se existe ou não a culpa
Ninguém se preocupa
Pois em todo caso haverá sempre uma desculpa
O abuso é demais, pra eles tanto faz
Não passará de simples fotos nos jornais
Pois gente negra e carente
Não muito influente
E pouco frequente nas colunas sociais
(Racionais)

Resumo

Esta dissertação tem como tema os desafios no uso de reconhecimento facial em sistemas de vídeo monitoramento no Brasil, uma tecnologia que, apesar de amplamente adotada em âmbito global, apresenta uma série de complexidades específicas no contexto brasileiro. A introdução contextualiza o reconhecimento facial como uma ferramenta de crescente importância para a segurança pública e privada, destacando seu papel no fortalecimento da vigilância e seus impactos sociais. Entretanto, ao mesmo tempo em que a tecnologia se expande, surgem questões éticas, técnicas e sociais que desafiam sua implementação de forma eficaz e justa. Esta dissertação busca responder às seguintes perguntas: quais são os principais desafios desses sistemas no Brasil? E de que maneira tais desafios comprometem a confiabilidade e a aceitação pública da tecnologia? A Dissertação também discute os desafios éticos e sociais associados ao reconhecimento facial, incluindo o impacto do monitoramento em direitos civis, como a privacidade e a liberdade individual, bem como a aceitação pública dessa tecnologia e o problema da desinformação. Casos de uso indevido, como a criminalização de minorias, são analisados de forma detalhada para ilustrar as consequências de uma aplicação inadequada ou desprovida de regulamentações robustas. Nesse sentido, a análise de estudos de caso realizados em estados brasileiros complementa a discussão, oferecendo uma perspectiva concreta sobre os impactos positivos e negativos da tecnologia no contexto nacional. A metodologia adotada incluiu uma revisão sistemática da literatura acadêmica. Os resultados obtidos integram os desafios mapeados com as experiências relatadas nos estudos de caso. Ao final, propõe-se uma série de recomendações que incluem a necessidade de regulamentações mais robustas, o desenvolvimento de avanços tecnológicos capazes de reduzir vieses algorítmicos e a promoção de um uso mais responsável e transparente do reconhecimento facial no Brasil. O intuito é garantir que a tecnologia possa ser utilizada de forma simultaneamente eficiente e socialmente justa, atendendo tanto às demandas de segurança quanto às exigências éticas contemporâneas.

Palavras-chave: Reconhecimento Facial. Privacidade. Desafios. Sistemas de Videomonitoramento.

Abstract

This dissertation addresses the challenges of using facial recognition in video surveillance systems in Brazil. Although widely adopted globally, this technology presents a series of specific complexities in the Brazilian context. The introduction contextualizes facial recognition as a tool of increasing importance for public and private security, highlighting its role in strengthening surveillance and its social impacts. However, as the technology expands, ethical, technical, and social issues arise that challenge its effective and fair implementation. This dissertation seeks to answer the following questions: what are the main challenges of these systems in Brazil? And how do these challenges compromise the reliability and public acceptance of the technology? The dissertation also discusses the ethical and social challenges associated with facial recognition, including the impact of monitoring on civil rights, such as privacy and individual freedom, as well as the public acceptance of this technology and the problem of disinformation. Cases of misuse, such as the criminalization of minorities, are analyzed in detail to illustrate the consequences of inadequate application or lack of robust regulations. In this sense, the analysis of case studies conducted in Brazilian states complements the discussion, offering a concrete perspective on the positive and negative impacts of technology in the national context. The methodology adopted included a systematic review of the academic literature. The results obtained integrate the challenges mapped with the experiences reported in the case studies. In the end, a series of recommendations are proposed that include the need for more robust regulations, the development of technological advances capable of reducing algorithmic biases, and the promotion of a more responsible and transparent use of facial recognition in Brazil. The aim is to ensure that the technology can be used in a simultaneously efficient and socially fair manner, meeting both security demands and contemporary ethical requirements.

Keywords: Facial Recognition. Privacy. Challenges. Video Surveillance Systems.

Lista de tabelas

Lista de abreviaturas e siglas

ABNT	Associação Brasileira de Normas Técnicas
abnTeX	ABsurdas Normas para TeX
DCOMP	Departamento de Computação
UFS	Universidade Federal de Sergipe
PROCC	Programa de Pós-Graduação em Ciência da Computação
LGPD	Lei Geral de Proteção de Dados
GDPR	General Data Protection Law
COR	Centro de Operações Rio
VIP	Very Important Person
IA	Inteligência Artificial
US	United States
EU	European Union
UK	United Kingdom
BAME	Black, Asian, and Minority Ethnic
FRT	Facial Recognition Technology
AI	Artificial Intellligence
SVS	Snthetic Vision System
EUA	Estados Unidos da América
3D	Terceira Dimensão
HMM	Hiden Markov Model
SA	Simulated Annealing
SIM	Surface Interpenetration Measure
FAR	False Acceptance Rate
PCA	Principal Component Analysis

ICP	Interative Closest Point
MSE	Mean Squared Error
SSP	Secretaria de Segurança Pública
TRF	Tecnologia de Reconhecimento Facial

Sumário

1 Introdução

O reconhecimento facial é uma tecnologia que tem ganhado destaque no cenário global, sendo utilizada em sistemas de videomonitoramento para diversas finalidades. No Brasil, o aumento da vigilância e o impacto social levantam questões sobre a importância desse tema, especialmente no que diz respeito à privacidade e segurança dos cidadãos (BADA; OLIVEIRA, 2024).

A discussão sobre os desafios éticos, sociais e técnicos do reconhecimento facial em sistemas de videomonitoramento é fundamental para compreender em que medida essas questões afetam a implementação e confiabilidade do sistema, e quais os impactos para a sociedade como um todo (SCOPEL; PUHL, 2024).

A importância do tema é evidente, com foco especial no contexto brasileiro, onde o aumento da vigilância e o impacto social do uso do reconhecimento facial serão analisados em detalhes (COSTA; KREMER, 2022).

O reconhecimento facial em sistemas de videomonitoramento no Brasil enfrenta desafios éticos, sociais e técnicos significativos (LIMA, 2022). Do ponto de vista ético, a privacidade e o direito à imagem dos cidadãos estão em risco, levando a questões sobre a legitimidade do uso dessa tecnologia.

Em termos sociais, o reconhecimento facial pode levar à discriminação e vigilância em massa, afetando grupos minoritários de maneira desproporcional, conforme Pacheco (2025).

Já do ponto de vista técnico, a baixa precisão na identificação e a possibilidade de manipulação das imagens são preocupações relevantes (SILVA; LIMEIRA, 2023). Todos esses desafios impactam a implementação e confiabilidade do sistema, gerando desconfiança na sociedade e questionamentos sobre a eficácia real dessa ferramenta.

Socialmente, o uso dessa tecnologia pode impactar a liberdade individual e a sensação de vigilância constante, conforme explicam Moreira, Sales e Moreira (2024). Tecnicamente,

questões de precisão, segurança e confiabilidade do reconhecimento facial em diferentes condições ambientais e populacionais representam desafios significativos para a implementação desse sistema no país.

As adversidades encontradas impactam de maneira significativa tanto a implementação como a confiabilidade desses sistemas de vigilância. Esses desafios levantam questões relevantes que vão desde a possível invasão de privacidade dos cidadãos até a precisão e efetividade das tecnologias utilizadas, criando um cenário de preocupações éticas e técnicas que deve ser cuidadosamente analisado (VERISSIMO; NOVAIS, 2024). Isso gera um debate importante sobre os limites e as responsabilidades que vêm junto com a adoção dessa tecnologia.

A motivação para realizar este estudo decorre, de maneira significativa, da crescente utilização do reconhecimento facial em sistemas de vídeo monitoramento no Brasil, que levanta questões sobre privacidade, segurança e eficácia dessas tecnologias emergentes, as quais têm se tornado cada vez mais presentes na vida cotidiana da população.

Serão abordadas questões como a privacidade dos cidadãos, possíveis violações de direitos e o potencial para discriminação, ressaltando a necessidade de um debate ético e técnico aprofundado acerca dessa prática. Os impactos esperados do uso de reconhecimento facial em sistemas de vídeo monitoramento no Brasil são múltiplos e abrangem uma variedade de aspectos, tanto no que tange à segurança pública quanto em questões que envolvem a privacidade e a ética.

Esse tipo de tecnologia pode a eficiência na identificação de criminosos e na prevenção de delitos, mas também levanta preocupações acerca do monitoramento excessivo dos cidadãos e da potencial violação de direitos individuais (ARAÚJO; CARDOSO; PAULA, 2021). A discussão sobre esses temas é importante para garantir que a implementação de tais sistemas seja realizada de forma responsável, considerando a balança entre segurança e a proteção da privacidade dos indivíduos.

1.1 Objetivos

O objetivo geral desta dissertação é analisar os desafios no uso do reconhecimento facial em sistemas de videomonitoramento no Brasil, buscando compreender os obstáculos éticos, sociais e técnicos que estão presentes nesse contexto específico.

1.1.1 Objetivos Específicos

Os objetivos específicos desta dissertação incluem a identificação dos principais desafios éticos, sociais e técnicos relacionados ao uso do reconhecimento facial em sistemas de videomonitoramento no Brasil. Além disso, pretende-se analisar casos de uso específicos e seu impacto na sociedade, a fim de compreender melhor as consequências dessa tecnologia.

1. Discutir os principais desafios éticos, sociais e técnicos incluindo a questão da privacidade e da proteção de dados pessoais. Além disso, aspectos sociais como a discriminação e o viés algorítmico complementando a discussão caso também representem desafios importantes. Continuando a discussão, abordar ponto de vista técnico, a precisão e a confiabilidade do sistema são pontos de atenção, pois podem afetar diretamente a eficácia e a segurança da tecnologia.

2. Analisar casos de uso e seu impacto na sociedade. A análise de casos de uso do reconhecimento facial permitirá compreender de que forma essa tecnologia impacta a sociedade, seja no contexto da segurança pública, do comércio ou de outras áreas. Será fundamental investigar os efeitos positivos e negativos, a fim de embasar recomendações futuras para a aplicação da tecnologia de forma mais consciente e responsável.

3. Com base na identificação dos desafios éticos, sociais e técnicos, será possível propor recomendações para uma aplicação mais ética e eficaz do reconhecimento facial em sistemas de videomonitoramento no Brasil. Isso pode envolver desde a criação de regulamentações mais específicas até a implementação de medidas de segurança e transparência que garantam o uso responsável dessa tecnologia.

2

Fundamentação Teórica

2.1 Reconhecimento Facial

O reconhecimento facial tem sua origem na década de 1960, com os primeiros experimentos para identificação de indivíduos por meio de análise de imagens. Ao longo dos anos, a tecnologia evoluiu significativamente, passando por diferentes fases de desenvolvimento e aprimoramento (OLIVEIRA; MELO, 2023).

A partir dos anos 2000, com o avanço das redes neurais e algoritmos de aprendizado de máquina, o reconhecimento facial alcançou maior eficácia, tornando-se uma ferramenta amplamente utilizada em sistemas de segurança e monitoramento (DUARTE et al., 2024). No entanto, o uso indiscriminado e os desafios éticos e legais relacionados à privacidade e segurança dos dados têm gerado debates e questionamentos sobre a aplicação dessa tecnologia no Brasil e no mundo (ANTONIO, 2022).

A aplicação do reconhecimento facial em sistemas de segurança envolve a utilização de tecnologias para identificar indivíduos, proporcionando uma camada extra de proteção em ambientes sensíveis. Essa tecnologia pode ser integrada a câmeras de vigilância, sistemas de controle de acesso e monitoramento remoto, permitindo a detecção de pessoas autorizadas e identificando potenciais ameaças (MELO; SERRA, 2022). Além disso, o uso de softwares como o "Oitchau"de análise de dados por biometria facial, torna possível a identificação de comportamentos atípicos e a resposta rápida a incidentes, aumentando a eficácia na prevenção de crimes (LIMA, 2023b).

A segurança cibernética também desempenha um papel importante, assegurando que os dados capturados e os sistemas que os suportam sejam resguardados contra acessos não autorizados e ataques cibernéticos (GOMES, 2024). A formação contínua da equipe em técnicas de segurança e a atualização frequente dos equipamentos e dos protocolos são fundamentais para garantir a eficácia e a adaptabilidade dos sistemas de reconhecimento facial em um ambiente que

está em constante mudança (MACHADO, 2023).

2.2 Legislação e regulamentação

No Brasil, o uso de reconhecimento facial em sistemas de vídeo monitoramento é regulamentado pela Lei Geral de Proteção de Dados (LGPD), que estabelece regras para coleta, armazenamento e tratamento de dados pessoais (OLIVEIRA, 2024).

2.2.1 Lei Geral de Proteção de Dados (LGPD)

A LGPD, que é a Lei Geral de Proteção de Dados, é a legislação específica no Brasil que aborda a proteção de dados pessoais, incluindo a questão do uso de tecnologias como o reconhecimento facial em sistemas de vídeo monitoramento (MULHOLLAND, 2020). Conforme Vanz et al. (2023), a LGPD estabelece princípios fundamentais sobre o tratamento de dados, como a necessidade de consentimento explícito por parte dos titulares e a definição de uma finalidade específica e legítima para a coleta dos dados (CAMÊLO, 2022). Além disso, a lei também prevê penalidades para o não cumprimento das normas estabelecidas, visando sempre garantir a privacidade, a segurança e a integridade dos dados dos cidadãos brasileiros, protegendo-os contra abusos e vazamentos de informações (SOUZA et al., 2022).

2.2.2 Regulamentações internacionais.

Além da LGPD, é fundamental considerar as regulamentações internacionais que impactam o uso de reconhecimento facial (LORENZON, 2021). O GDPR da União Europeia, por exemplo, estabelece diretrizes para o tratamento de dados biométricos, incluindo restrições específicas para o reconhecimento facial, conforme trabalho de Lorenzon (2021).

Na União Europeia, conforme tabela 1, as diretrizes formuladas sobre o tratamento de dados pessoais impactam de forma direta e significativa o uso dessa tecnologia emergente (CHIARELLO; CERVI; NOSCHANG, 2023). Isso traz à tona novos desafios e variadas considerações éticas essenciais que precisam ser levadas em conta, uma vez que a proteção da privacidade, neste cenário dinâmico e em rápida evolução, se torna cada vez mais relevante. Com isso, o diálogo em torno dessas questões se intensifica, evidenciando a importância de regulamentos eficazes que garantam a segurança das informações e o respeito aos direitos dos indivíduos em um mundo digital (ALMEIDA, 2022).

Nos Estados Unidos, as leis estaduais relacionadas à tecnologia e à privacidade variam consideravelmente, refletindo uma ampla diversidade de abordagens e opiniões sobre este importante e relevante tema (COSTA; KREMER, 2022). Entretanto, há uma preocupação crescente e abrangente com a privacidade, bem como a transparência no uso dessa tecnologia emergente, impulsionada por discussões públicas intensas e pela necessidade urgente de regulamentação

Tabela 1 – Regulamentações Internacionais

Estados Unidos	As leis estaduais variam, mas existe preocupação com a privacidade e a transparência no uso dessa tecnologia.
China	Apesar do uso massivo, há poucas regulamentações em relação ao reconhecimento facial.
União Européia	As diretrizes sobre o tratamento de dados pessoais impactam diretamente o uso dessa tecnologia.

eficaz e abrangente (HOOBERMAN, 2021). Essa diversidade de leis mostra claramente como diferentes regiões enfrentam os desafios complexos impostos por essa inovação tecnológica que continua a evoluir rapidamente, cada uma tentando encontrar soluções que atendam às suas necessidades específicas e aos desejos de seus cidadãos (MONTEIRO, 2021).

Na China, apesar do uso massivo e crescente da tecnologia de reconhecimento facial em diversas esferas sociais, comerciais e até mesmo na segurança pública, há uma quantidade limitada de regulamentações que abordam essa prática que é complexa e multifacetada (HANDELMAN, 2023). Essas normas são escassas, raramente específicas e geralmente formuladas de maneira vaga, o que levanta preocupações significativas sobre privacidade, proteção dos direitos dos cidadãos e o potencial para abusos tanto por parte do Estado quanto por entidades privadas que utilizam essas tecnologias (MAGRO; FORTES, 2021). A falta de uma supervisão eficaz pode resultar em consequências indesejadas e nocivas para os indivíduos, comprometendo sua liberdade e segurança pessoal em um ambiente cada vez mais controlado e monitorado.

2.3 Teorias sobre privacidade digital

A discussão sobre ética e privacidade digital é fundamental para o uso do reconhecimento facial em sistemas de vídeo monitoramento. Questões éticas relacionadas ao consentimento e uso de dados pessoais são levantadas, bem como a importância de garantir a proteção da privacidade dos indivíduos. Além disso, a ética digital aborda a responsabilidade das empresas no uso e armazenamento de informações sensíveis, visando evitar abusos e violações de direitos (SOUZA et al., 2022).

2.3.1 Conceitos de Privacidade

Privacidade é um conceito fundamental e essencial que se refere ao direito inerente de cada indivíduo exercer controle sobre suas informações pessoais e privadas. Este direito abrange não apenas a capacidade material e legal de decidir sobre a coleta, o uso e o compartilhamento de seus dados pessoais e sensíveis, mas também a responsabilidade de assegurar que esses dados sejam tratados com respeito e segurança. No contexto do reconhecimento facial, a questão da privacidade levanta questões críticas e preocupações significativas relacionadas ao consentimento

explícito, à transparência no uso dos dados e à eficaz anonimização das informações coletadas, que deve ser uma prioridade (COSTA; OLIVEIRA, 2019).

É importante garantir que a identidade das pessoas seja devidamente protegida em todas as etapas e fases do processo de monitoramento, assegurando sempre que suas informações não sejam utilizadas de maneira não autorizada ou de forma intrusiva (OLIVEIRA; MALDONADO, 2022). Isso é vital para preservar a dignidade, a confiança e os direitos civis dos indivíduos envolvidos, reiterando a importância de uma abordagem ética no manuseio de dados pessoais. A implementação de políticas de proteção de dados é importante para criar um ambiente em que os cidadãos possam se sentir seguros e respeitados em relação às suas informações (OLIVEIRA, 2020).

2.3.2 Conceitos de Proteção de Dados

A proteção de dados é um conceito amplo que se refere a um conjunto de medidas e políticas elaboradas para garantir a segurança e a confidencialidade das informações pessoais que são coletadas, processadas e armazenadas. No contexto do reconhecimento facial, isso envolve a implementação de diversas medidas de segurança (MAGRO; FORTES, 2021).

Por exemplo, a utilização de criptografia para proteger os dados em trânsito e em repouso, bem como um controle de acesso, é essencial para evitar que informações sensíveis acabem em mãos erradas (KUM; MENDES, 2024).

Essas medidas visam proteger as informações críticas armazenadas contra acessos não autorizados, vazamentos de dados e outros tipos de ameaças cibernéticas que estão em constante evolução. Além disso, é fundamental que haja uma conscientização contínua e abrangente sobre a importância da proteção dos dados, visando garantir que tanto as organizações quanto os indivíduos estejam cientes das melhores práticas e dos riscos associados ao uso desta tecnologia. Isso inclui não apenas a compreensão dos direitos dos usuários em relação à privacidade, mas também o reconhecimento das obrigações legais que as empresas têm em relação ao tratamento e proteção dos dados pessoais (WALLACE, 2019).

2.3.3 Conceitos de Direitos Civis

Os direitos civis são essenciais e indispensáveis para garantir que todos os indivíduos e grupos sejam assegurados uma liberdade plena e proteção adequada contra quaisquer tipos de abusos que possam ocorrer, especialmente em um contexto específico e cada vez mais relevante do uso de reconhecimento facial em sistemas de videomonitoramento (CRIPPA et al., 2021). Isso inclui, o direito à não discriminação, à privacidade, à liberdade de expressão e à participação efetiva na tomada de decisões que dizem respeito diretamente ao uso e à regulamentação da tecnologia em questão, que muitas vezes suscitam debates sobre ética e segurança (GARCIA et al., 2023).

Esses direitos garantem que todos, sem exceção, possam expressar suas opiniões livremente, acessar informação sem barreiras de qualquer natureza e ter voz ativa e significativa nas regulamentações que afetam suas vidas cotidianas e a privacidade de suas informações pessoais, assegurando assim um ambiente mais justo e equitativo para todos os cidadãos, permitindo que cada um se sinta seguro e respeitado em suas interações tanto no mundo físico quanto no digital (SILVA, 2022).

3
Metodologia

A definição da metodologia para a presente dissertação foi orientada pela necessidade de compreender, em profundidade, os desafios inerentes ao uso de reconhecimento facial em sistemas de vídeo monitoramento no Brasil. Partindo desse objetivo central, optou-se por realizar uma revisão sistemática da literatura, de modo a identificar, categorizar e analisar as principais barreiras tecnológicas, éticas e operacionais previamente apresentadas nos capítulos introdutórios desta dissertação (BRIZOLA; FANTIN, 2016).

3.1 Questões levantadas

Esta dissertação lança algumas perguntas com o objetivo de obter, por meio da pesquisa, cada uma das respostas realizadas.

A seguir as questões de pesquisa:

1. **Questão 01;** Quais são os desafios da privacidade no reconhecimento facial em videomonitoramento?
2. **Questão 02;** Quais são os desafios legais para o uso do reconhecimento facial no Brasil?
3. **Questão 03;** Existe consenso entre pesquisadores sobre a regulação ou banimento da Tecnologia de Reconhecimento Facial?
4. **Questão 04;** Quais estratégias têm sido adotadas para mitigar o viés racial no reconhecimento facial?

3.2 Processo de Seleção

A revisão de literatura foi estruturada com base nos desafios destacados na fundamentação teórica, que incluem questões como a acurácia dos algoritmos em ambientes não controlados, a privacidade e proteção de dados pessoais, os vieses algorítmicos e as limitações de infraestrutura tecnológica. Para cada um desses desafios, foram selecionados artigos, teses, dissertações e relatórios técnicos publicados em revistas científicas, anais de conferências e bancos de dados acadêmicos reconhecidos, como *IEEE Xplore*, *ACM Digital Library*, *Web of Science*, *Springer Nature*, *Scielo*, *Scopus (Elsevier)* e *Google Scholar*.

3.2.1 Palavras-chave

O processo de busca foi conduzido utilizando palavras-chave específicas para cada base, combinadas com operadores booleanos para garantir a abrangência e relevância dos resultados (JÚNIOR et al., 2023).

Na Tabela 2 são apresentadas as Palavras-Chave utilizadas utilizadas para formar a *string* de busca.

Tabela 2 – Palavras-Chave utilizadas na *string* de busca

Palavra-Chave	**Sinônimo em inglês**
Reconhecimento Facial	Facial Recognition
Vigilância por Vídeo	Video Surveillance
Privacidade	Privacy

Sendo estas palavras-chave utilizadas por meio da *string* citada a seguir, na tabela 3 em cada uma das bases científicas.

Tabela 3 – *String* utilizada para realizar as buscas nas bases

("FACIAL RECOGNITION"AND "VIDEO SURVEILLANCE"AND "PRIVACY")

3.2.2 Bases Científicas

Nesta dissertação, foram utilizadas para pesquisa e coleta de trabalhos, as seguintes bases científicas:

- ACM Digital Library <<https://dl.acm.org/>>;
- IEEE Xplore Digital Library <<http://ieeexplore.ieee.org>>;
- Springer <<https://link.springer.com/>>;
- Web of Science <<https://www.webofknowledge.com/>>;

Tendo como resultado a quantidade informada na tabela 4, sem o uso de qualquer critério de inclusão ou exclusão.

Tabela 4 – Resultados sem Critérios de Inclusão e Exclusão

Base Científica	**Resultados**
IEEE	66
Web of Science	07
ACM	86
Springer	173

3.2.3 Critérios de Inclusão e Exclusão

São critérios de inclusão [CI]:

1. Trabalhos entre 2018 e 2024.
2. Trabalhos relacionados a Ciência da Computação

São critérios de exclusão [CE]:

1. Trabalhos que não abordam o assunto específico relacionado ao reconhecimento facial.

Desta forma, a dissertação conta, conforme tabela 5, com o total de **20 artigos** escolhidos para responder responder as perguntas levantadas no começo deste capítulo.

Tabela 5 – Resultado após critérios de inclusão e exclusão

Base	**CI1**	**CI2**	**CE1**
IEEE	36	32	4
Web of Science	7	7	5
ACM	80	80	4
Springer	124	124	7
Total	**247**	**243**	**20**

3.3 Outros Trabalhos

Após a coleta inicial, mais trabalhos foram adicionados para fundamentação teórica, de acordo com novos critérios de inclusão e exclusão. Entre eles, artigos publicados nos últimos dez anos, em língua portuguesa ou inglesa, e que abordassem aplicações ou estudos relacionados ao tema específico foram considerados relevantes. Estudos puramente teóricos ou desconectados da realidade operacional de sistemas de monitoramento no Brasil foram excluídos.

Cada trabalho foi analisado em relação à sua contribuição para a compreensão dos desafios apresentados. Para isso, foram estabelecidas categorias temáticas baseadas nos seis principais eixos problemáticos identificados: viés algorítmico, infraestrutura, confiabilidade, direitos civis, aceitabilidade e criminalização, conforme tabela 6. As informações extraídas de cada artigo foram sintetizadas em tabelas e mapas conceituais, facilitando a comparação e a análise crítica dos resultados.

Tabela 6 – Desafios no uso do Reconhecimento Facial

Desafios Técnicos e Operacionais	**Desafios Éticos e Sociais**
Viés algorítmico e Impacto Social	Direitos civis e Humanos
Infraestrutura e Integração de Sistemas	Aceitação pública e Desinformação
Taxa de Erro e Confiabilidade	Criminalização e discriminação de minorias

Desta forma, esta abordagem metodológica possibilitou a construção de uma base para as proposições apresentadas nos capítulos 09 e 10, garantindo que as soluções sugeridas estejam ancoradas em evidências científicas e sejam adequadas ao contexto brasileiro. Dessa forma, a revisão de literatura sistemática não apenas fundamenta as análises realizadas, mas também contribui para avançar o debate sobre o reconhecimento facial em sistemas de vídeo monitoramento no Brasil.

4

Desafios Técnicos e Operacionais

A implementação do reconhecimento facial em sistemas de vídeo monitoramento no Brasil enfrenta desafios técnicos e operacionais significativos. Questões como iluminação, qualidade das câmeras e precisão dos algoritmos/modelos são pontos críticos a serem considerados (ZENG; QIU; SHI, 2021). Além disso, a integração dos sistemas de reconhecimento facial com a infraestrutura existente pode ser complexa, conforme evidencia Bada e Oliveira (2024), levando em conta a conectividade e a capacidade de processamento de dados. Outro desafio operacional é a necessidade de treinar e educar os usuários e operadores do sistema para utilizarem corretamente a tecnologia, garantindo sua eficácia e adequado funcionamento (BADA; OLIVEIRA, 2024).

4.1 Viés algorítmico e impacto social

Os algoritmos de reconhecimento facial apresentam uma capacidade de discriminar e diferenciar indivíduos, levando em consideração uma gama de fatores diversos que são significativos e relevantes (SANTAELLA, 2023). Entre esses fatores, se deve incluir características como a cor da pele, o gênero, a etnia, e muitos outros aspectos que são considerados importantes neste contexto.

Esta habilidade peculiar e, em muitas ocasiões, problemática desses algoritmos decorre da forma específica como são treinados e desenvolvidos ao longo do tempo. Frequentemente, esses sistemas incorporam dados que não apenas refletem, mas também perpetuam preconceitos e estereótipos já existentes na sociedade (ANJOS; FILHO; SOUSA, 2024). Tal situação pode resultar em uma série de equívocos, erros de julgamento e vieses que ocorrem nas análises produzidas pelos sistemas, levando a resultados que podem ser imprecisos e, como consequência, gerando impactos sociais negativos que afetam a vida de várias pessoas, especialmente aquelas que se encontram em situações de vulnerabilidade (CANI; NUNES, 2022).

Vários estudos e pesquisas realizadas na área de reconhecimento facial, como os de Silva

e Silva (2019) e notícias publicadas por Rossi (2019) e Oliveira (2024) evidenciam que as taxas de erro são consideravelmente mais altas para mulheres, além de também serem particularmente elevadas entre as pessoas que possuem pele em tonalidades mais escuras (OLIVEIRA, 2020).

Um estudo intitulado *"Gender Shades"*, de autoria de Buolamwini e Gebru (2018) realizou testes em 03 sistemas comerciais de classificação de gênero amplamente utilizados na época da pesquisa. Os sistemas analisados foram:

1. Microsoft Azure Face API
2. IBM Watson Visual Recognition API
3. Face++

Segundo o estudo, esses três sistemas foram escolhidos porque são oferecidos como APIs públicas comerciais, utilizadas em diversas aplicações de reconhecimento facial, incluindo segurança, verificação de identidade e análise de imagens, conforme tabela 7.

Tabela 7 – Principais Resultados para Cada Sistema

Microsoft Azure Face API
Melhor desempenho para homens de pele clara (0,0% de erro)
Pior desempenho para mulheres de pele escura (20,8% de erro)
IBM Watson Visual Recognition API
Melhor desempenho para homens de pele clara (0,3% de erro)
Pior desempenho para mulheres de pele escura (34,7% de erro)
Face++
Melhor desempenho para homens de pele escura (0,7% de erro)
Pior desempenho para mulheres de pele escura (34,5% de erro)

Em uma outra visão, o estudo evidencia, que:

1. A taxa de erro para mulheres de pele mais escura chegou a **34,7%** no sistema da IBM, **34,5%** no Face++ e **20,8%** no Microsoft
2. As taxas de erro para homens foram sempre menores do que para mulheres. A diferença na taxa de erro entre homens e mulheres variou de **8,1%** a **20,6%**, dependendo do sistema testado
3. As taxas de erro foram mais altas para pessoas de pele mais escura em comparação com pessoas de pele mais clara. A diferença nas taxas de erro entre esses grupos variou de **11,8%** a **19,2%**, dependendo do sistema

Este fato não apenas mostra a existência de discriminação algorítmica, mas também destaca um fenômeno preocupante que exige atenção e ações urgentes, uma vez que as implicações

sociais desse tipo de discriminação são vastas e profundas (JOSÉ; JÚNIOR,). No contexto brasileiro, essa questão se torna ainda mais crítica, pois pode potencializar ainda mais a exclusão social e a discriminação de determinados grupos que já se encontram marginais. Isso levanta uma série de preocupações éticas e legais que precisam ser avaliadas em relação ao uso generalizado e indiscriminado do reconhecimento facial, especialmente em sistemas de videomonitoramento utilizados no país (ANDRADE; JABORANDY, 2022).

Tabela 8 – Taxas de Erros entre Homens e Mulheres

Taxa de Erro no Serviço da Amazon			
Taxa de Erro em Homens		Taxa de Erro em Mulheres	
Homens Brancos	0%	Mulheres Brancas	13%
Homens Negros	0%	Mulheres Negras	31%

4.1.1 Como os algoritmos podem discriminar com base em cor, gênero, etnia, etc.

Conforme o estudo apresentado por Wang et al. (2019), os algoritmos podem discriminar com base em diversos fatores, como cor, gênero e etnia, entre outros, principalmente devido à falta de representatividade e diversidade nos conjuntos de dados que são utilizados para treiná-los de forma eficiente e precisa (SILVA, 2024).

No estudo de Wang et al. (2019), os números apresentados demonstram disparidades estatísticas claras no desempenho dos algoritmos de reconhecimento facial entre diferentes grupos raciais, conforme tabela 9.

Tabela 9 – Racial Faces in the Wild (RFW) (WANG et al., 2019).

Modelo	**Caucasiano**	**Indiano**	**Asiático**	**Africano**
Microsoft	87,60%	82,83%	79,67%	75,83%
Face++	93,90%	88,55%	92,47%	87,50%
Baidu	89,13%	86,53%	90,27%	77,97%
Amazon	90,45%	87,20%	84,87%	86,27%
Média (APIs)	**90,27%**	**86,28%**	**86,82%**	**81,89%**

Essa ausência de diversidade não é uma questão simples; resulta em uma incapacidade dos algoritmos de reconhecimento facial de capturar com precisão as características faciais de diferentes grupos populacionais, o que, por sua vez, leva a taxas de erro que são desproporcionalmente altas, conforme evidenciadas por Wang et al. (2019) e que refletem essa desigualdade existente na sociedade (JOSÉ; JÚNIOR,).

Além disso, a falta de consideração para nuances culturais específicas e variações étnicas distintas, conforme Costa e Kremer (2022), que são vitais e essenciais para entender a complexidade da diversidade humana, pode levar à generalização excessiva de características que não representam adequadamente a pluralidade da população. Isso aumenta ainda mais o risco

de discriminação em diversos contextos sociais, afetando a equidade e a justiça social entre os diferentes grupos que compõem a sociedade.

No cenário brasileiro, em que a população é diversificada em termos de cor de pele, origem étnica e cultura, o impacto social negativo do viés algorítmico se torna ainda mais alarmante, trazendo à tona questões que não podem ser ignoradas (COSTA; KREMER, 2022). Isso destaca a importância de considerar essas questões sensíveis ao implementar sistemas de vídeo monitoramento que utilizam reconhecimento facial, assegurando que todos os grupos sejam tratados de maneira justa, respeitosa e equitativa, promovendo assim um ambiente mais inclusivo e justo para todos os cidadãos (COIMBRA et al., 2023).

4.2 Infraestrutura utilizada no Brasil

No Brasil, os desafios técnicos e operacionais que emergem no uso de reconhecimento facial em sistemas de vídeo monitoramento são complexos, multifacetados e variados, a exemplo dos dos tipos de softwares, bancos de dados e equipamentos utilizados para captura de imagens. Esses desafios apresentam-se sob diversas formas, sendo um dos mais proeminentes os limitantes tecnológicos significativos, conforme Ribeiro (2022).

Primeiramente, a qualidade das câmeras utilizadas é um fator primordial e determina o êxito no processamento de imagens. Infelizmente, muitas das câmeras de monitoramento, que estão comumente disponíveis e são adotadas atualmente em várias regiões do Brasil, não possuem a resolução necessária e essencial para capturar imagens com a nitidez e clareza que são imprescindíveis para que se possa realizar o reconhecimento facial de maneira eficaz e adequada (BADA; OLIVEIRA, 2024). Além disso, há um agravamento na situação devido à infraestrutura de conectividade que, especialmente em áreas que são afastadas dos grandes centros urbanos, conforme estudo de Gomes e Anatel (2002) frequentemente se mostra insuficiente para garantir uma transmissão eficiente e contínua de dados entre os dispositivos utilizados (JÚNIOR,).

A falta de uma boa conexão pode comprometer severamente a operação dos sistemas de monitoramento em tempo real. Por fim, esses vários fatores, que podem parecer variados, interagem entre si e podem impactar, de forma negativa, a eficácia, a precisão e a confiabilidade do reconhecimento facial em sistemas de vídeo monitoramento (MONTEIRO, 2021). Consequentemente, isso cria desafios que precisam ser superados e que exigem soluções e adaptadas no contexto da realidade brasileira.

4.3 Taxa de erro e confiabilidade

A taxa de erro e a confiabilidade no reconhecimento facial representam um desafio no contexto brasileiro, onde estima-se uma taxa de até 8%, conforme estudo conduzido por LIMA

(2021), especialmente quando se leva em conta a ampla diversidade étnica e racial que caracteriza de forma tão rica e complexa a população (DUARTE et al., 2021).

Já quando se fala em redes neurais convolucionais *(deep learning)*, a acurácia do reconhecimento facial alcançou uma eficácia de 98,76% em testes controlados e evidenciados pelo estudo de LIMA (2021). No entanto, essa tecnologia exige máquinas mais potentes e maior tempo de processamento

A precisão do reconhecimento facial pode ser influenciada por uma série de fatores variados e complexos, que incluem não apenas condições de iluminação adversas e, muitas vezes, inesperadas, mas também a qualidade das câmeras utilizadas, que pode variar bastante, e as distintas características físicas das pessoas, que podem diferir entre si (ZENG; QIU; SHI, 2021). Essas variáveis tornam o cenário de implementação e operação de tecnologias de reconhecimento facial ainda mais desafiador. Por isso, torna-se importante avaliar a confiabilidade dos sistemas de reconhecimento facial que estão sendo utilizados atualmente (VECCI, 2023). Essa avaliação minuciosa é fundamental para minimizar os erros que podem ocorrer e garantir a máxima precisão nas identificações realizadas, assegurando um uso mais eficiente e ético dessa tecnologia.

4.3.1 Falsos positivos e falsos negativos no contexto brasileiro

No contexto brasileiro atual, a ocorrência de falsos positivos e falsos negativos no reconhecimento facial se configura como uma preocupação extremamente relevante e significativa, especialmente devido à possibilidade de impactar de maneira drástica e significativa decisões críticas que estão diretamente relacionadas à segurança pública e à justiça (FAVERI, 2023). Os falsos positivos, que são os casos em que o sistema identifica erroneamente alguém como sendo uma pessoa de interesse, podem levar a sérios e graves erros de identificação. Isso, por sua vez, pode resultar em situações profundamente injustas para cidadãos que são inocentes.

Por outro lado, os falsos negativos, que se referem à incapacidade de identificar indivíduos que realmente são de interesse das autoridades e da segurança, podem resultar em consequências extremas e graves, como a não detecção de ameaças reais que possam colocar em risco a sociedade (VALMORBIDA; ETGETON, 2020). Diante dessa complexa e alarmante realidade, torna-se absolutamente essencial compreender a frequência com que esses erros ocorrem na prática e as causas subjacentes que contribuem para sua ocorrência (FARIA; MOTA et al., 2023).

Isso é fundamental para que sejam implementadas medidas eficazes que ajudem a reduzir a incidência desses erros e, dessa forma, aumentem a precisão e a confiabilidade do reconhecimento facial em operações de segurança, bem como na administração da justiça em nosso país.

4.4 Considerações sobre os Desafios Técnicos Operacionais

É essencial considerar, as várias implicações que a utilização desses algoritmos podem ter na vida das pessoas afetadas, incluindo não apenas a possibilidade de agravamento de desigualdades sociais e raciais que estão presentes já no tecido social, mas também questionar a legitimidade e a justiça nos processos que favorecem esses sistemas (CARVALHO,). É essencial que haja um debate público robusto sobre a moralidade e a eficácia desses algoritmos, e que medidas corretivas sejam pensadas e implementadas de forma a garantir que não haja violação dos direitos humanos e que haja um compromisso claro com a igualdade e a justiça social em nossa sociedade.

5

Desafios Éticos e Sociais

Questões relacionadas à privacidade, supervisão e potencial abuso levantam preocupações sobre o impacto do uso dessa tecnologia. Além disso, a falta de regulamentação clara e a possibilidade de discriminação levantam questões fundamentais sobre a implementação justa e equitativa do reconhecimento facial no contexto brasileiro (VIEIRA et al., 2024).

5.1 Impacto nos direitos civis e humanos

Embora se tenha um avanço relacionado a legislação, conforme LIMA (2023a) aborda em seu estudo, o uso do reconhecimento facial em sistemas de vídeo monitoramento no Brasil, conforme tabela 10, e levanta preocupações sobre o impacto nos direitos civis e humanos dos cidadãos (SILVA, 2022).

Tabela 10 – Leis Brasileiras Aplicáveis

Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018	
A favor	Regula a coleta, processamento e armazenamento de dados pessoais no Brasil.
A favor	Exige consentimento explícito para o uso de dados biométricos, incluindo reconhecimento facial.
Contra	Há brechas na aplicação da LGPD para segurança pública, permitindo que órgãos governamentais utilizem reconhecimento facial sem consentimento formal
Projeto de Lei 2392/2022	
A favor	Propõe a regulamentação do uso do reconhecimento facial no Brasil.
A favor	Prevê a proibição do uso da tecnologia para identificação pública e privada, salvo em casos em que haja um relatório prévio de impacto à privacidade
Contra	Ainda está em tramitação, o que significa que não há regulamentação específica atualmente.

A vigilância constante por meio de tecnologias de reconhecimento facial pode interferir na

liberdade individual dos cidadãos, criando um ambiente de constante escrutínio e monitoramento que pode ser opressivo. Além disso, a utilização dessas tecnologias de reconhecimento facial pode violar o direito à privacidade, uma vez que as pessoas têm o direito fundamental de não serem constantemente observadas e identificadas sem seu consentimento expresso (STEFFEN, 2023). Essa situação gera um debate sobre a ética e a regulamentação necessárias para garantir que os direitos dos indivíduos sejam respeitados em um mundo cada vez mais monitorado e digitalizado.

5.1.1 Como a vigilância interfere na liberdade individual e no direito à privacidade

A vigilância por meio do reconhecimento facial pode interferir na liberdade individual das pessoas, uma vez que essa prática gera um clima de desconfiança e insegurança, inibindo a livre circulação e a genuína expressão das individualidades (LIMA, 2023a). Além disso, o direito à privacidade é comprometido. A falta de regulamentação vigente sobre o uso da tecnologia de reconhecimento facial ampliam ainda mais as preocupações que surgem relacionadas ao impacto na liberdade individual e no direito fundamental à privacidade (VARGAS, 2022).

5.2 Aceitação pública e desinformação

A aceitação pública do uso do reconhecimento facial no Brasil tem sido influenciada pela desinformação disseminada e pela falta de compreensão a respeito das implicações éticas e sociais que essa tecnologia envolve. Muitos cidadãos não possuem uma compreensão clara de como o funcionamento do reconhecimento facial se dá, nem estão cientes de como ele pode, de fato, impactar sua privacidade e sua liberdade individual (MELO, 2024).

A falta de transparência, por parte das autoridades governamentais responsáveis e também das empresas que implementam a tecnologia, contribui para a desinformação e para a crescente desconfiança pública em relação ao uso do reconhecimento facial em sistemas de vídeo monitoramento, o artigo de Steffen (2023) aponta os principais pontos de preocupação, conforme tabela 11.

Tabela 11 – Principais preocupações sobre o Reconhecimento Facial

Pode reforçar preconceitos existentes, principalmente contra grupos marginalizados
Possui altas taxas de erro para pessoas negras e pode levar a injustiças
Falta regulamentação no Brasil para controlar o uso no processo penal
Sem transparência e supervisão, pode ser usado para vigilância abusiva

É determinante que haja um esforço conjunto para educar a população, promovendo uma discussão mais ampla sobre os direitos dos cidadãos, as implicações legais e os mecanismos

de proteção que podem ser implementados para salvaguardar a privacidade e a liberdade das pessoas em um mundo cada vez mais digital e vigiado.

5.2.1 Como o público percebe e entende o uso do reconhecimento facial

A percepção do público em relação ao uso do reconhecimento facial é um tema que varia significativamente entre diferentes grupos sociais. Enquanto alguns indivíduos expressam preocupações sérias sobre a invasão de privacidade, destacando o potencial para abusos e vigilância excessiva, outros acreditam fortemente que a tecnologia pode trazer benefícios significativos para a segurança pública e para a prevenção de crimes (LIMA, 2023a).

A complexidade do assunto é ampliada pela falta de informação precisa e pela compreensão ainda bastante limitada sobre as capacidades e limitações do reconhecimento facial, o que, por sua vez, contribui para uma crescente desconfiança e incerteza entre os cidadãos. As percepções que as pessoas têm em relação a essas tecnologias são moldadas, em grande parte, pela ausência de clareza sobre quais entidades ou organizações têm acesso aos dados coletados através desse sistema e de que maneira, de fato, essas informações são utilizadas, conforme Baccarin (2023) que faz um comparativo descrito na tabela 12 entre LGPD e GDPR.

Essa situação leva a um debate sobre a necessidade de regulamentação e supervisão mais rigorosas, para garantir que os direitos individuais sejam respeitados e que os dados não sejam utilizados de maneira inadequada ou abusiva. A discussão a respeito do reconhecimento facial é, portanto, não apenas uma questão tecnológica, mas também uma questão ética e social que merece uma atenção cuidadosa e crítica.

5.3 Criminalização e discriminação de minorias

O uso de reconhecimento facial em sistemas de vídeo monitoramento no Brasil tem gerado preocupações sobre a possibilidade de criminalização e discriminação de minorias étnicas e sociais. Além do mais, a implementação desse tipo de tecnologia em espaços públicos pode acarretar um monitoramento intensificado dessas minorias, contribuindo para a criação de um ambiente que favorece a discriminação e reforça estereótipos prejudiciais que já existem na sociedade. Essas dificuldades levantam preocupações éticas e sociais quanto ao emprego do reconhecimento facial, exigindo uma análise sobre os potenciais impactos negativos que podem surgir, especialmente em comunidades já vulneráveis e marginalizadas (MELO, 2024). O debate em torno desse tema é urgentemente necessário, considerando que a proteção dos direitos humanos e a equidade social devem estar em primeiro plano nas discussões pertinentes ao avanço tecnológico e suas aplicações.

Tabela 12 – Quadro Comparativo: LGPD vs. GDPR

Critério	**LGPD (Brasil)**	**GDPR (União Europeia)**
Entrada em Vigor	Setembro de 2020	Maio de 2018
Autoridade Responsável	ANPD (Autoridade Nacional de Proteção de Dados), vinculada ao Ministério da Justiça	Comissões de proteção de dados de cada país da UE, supervisionadas pelo Conselho Europeu de Proteção de Dados
Aplicação Territorial	Aplicável a qualquer organização que processe dados pessoais de cidadãos brasileiros, independentemente da localização da empresa	Aplicável a qualquer organização que processe dados de cidadãos da UE, mesmo que a empresa esteja fora da UE
Definição de Dados Sensíveis	Inclui dados biométricos, como reconhecimento facial, exigindo tratamento especial	Também inclui dados biométricos, mas impõe regras mais rígidas para consentimento e processamento
Direitos dos Usuários	Acesso, retificação, exclusão, portabilidade, oposição e revisão de decisões automatizadas	Acesso, retificação, exclusão ("direito ao esquecimento"), portabilidade, limitação de processamento e oposição
Consentimento	Deve ser explícito para dados sensíveis, mas permite tratamento sem consentimento em algumas exceções, como segurança pública	Consentimento deve ser livre, específico, informado e inequívoco; decisões automatizadas devem ser justificáveis
Responsabilidade e Prestação de Contas	Exige que empresas documentem práticas e realizem Relatórios de Impacto à Proteção de Dados para atividades de alto risco	Empresas devem demonstrar conformidade contínua e realizar avaliações de impacto de privacidade (DPIA)
Penalidades por Descumprimento	Multas de até 2% do faturamento anual da empresa, limitadas a R$ 50 milhões por infração	Multas podem chegar a 4% do faturamento global anual da empresa, com limite de € 20 milhões
Transferência Internacional de Dados	Permitida apenas para países que garantam um nível de proteção adequado ou mediante cláusulas contratuais específicas	Apenas permitida para países considerados "adequados" pela Comissão Europeia ou mediante cláusulas contratuais padrão

6

Casos de Uso no Brasil

6.1 Exemplos reais de sistemas implementados em estados brasileiros

O reconhecimento facial tem sido implementado em vários estados brasileiros, a exemplo de Rio de Janeiro, São Paulo e Bahia, para fins de segurança pública (PEREIRA, 2022). Alguns exemplos notáveis incluem a utilização da tecnologia no Estado de São Paulo, para identificação no controle de acesso a grandes eventos (RODRIGUES, 2023), e no Estado do Rio de Janeiro, onde a polícia utiliza a tecnologia para identificar criminosos em locais de grande aglomeração (JUNIOR, 2019).

Paralelamente a isso, o uso de sistemas de videomonitoramento está cada vez mais ligado ao conceito de cidades inteligentes. Em cidades como Curitiba, o uso da tecnologia é empregado no monitoramento e controle de tráfego, na iluminação pública, em apoio a sistemas meteorológicos e até mesmo em projetos ambientais (SANTOS et al., 2022).

O videomonitoramento por meio de dispositivos espalhados pelas ruas e até mesmo de trânsito auxiliam sensores de tráfego, bem como agem diretamente na detecção de acidentes e muitos outros incidentes em tempo real. Tal incidência procura auxiliar no processo de tomada de decisões em relação à gestão dos recursos urbanos (SILVA, 2023).

Através da coleta de imagens de câmeras de vigilância em locais públicos e privados, a tecnologia pode identificar e localizar indivíduos que estão desaparecidos (CABRAL et al., 2024). O Estado de São Paulo, por exemplo, lançou um programa onde fotos de pessoas desaparecidas são comparadas com imagens capturadas em tempo real por câmeras instaladas no metrô (ANDRÉA; SILVA; GUNDIM, 2022). Essa iniciativa tem o potencial de acelerar o processo de localização, reunindo famílias mais rapidamente reduzindo o sofrimento causado pela ausência de entes queridos, conforme Resende e Pereira (2015).

6.1.1 Exemplos no Estado de São Paulo

No Estado de São Paulo, a tecnologia de reconhecimento facial tem se tornado cada vez mais utilizada na identificação de foragidos da justiça (SCOPEL; PUHL, 2024). Essa tecnologia está proporcionando às autoridades competentes a capacidade de realizar capturas, conforme trabalho de Santos (2021), especialmente em relação a suspeitos que tentavam se esconder da polícia e evitar a prisão.

Além disso, o reconhecimento facial está sendo utilizado em ambientes que exigem controle rigoroso, tais como os locais de grande aglomeração na cidade de São Paulo (JUNIOR[1]; TEIXEIRA; HOMEM,). Esses locais incluem estádios de futebol, sistemas de transportes públicos e eventos públicos, nos quais o elevado fluxo de pessoas faz com que seja necessário um monitoramento ágil e uma resposta efetiva em situações emergenciais (BADA; OLIVEIRA, 2024).

Em São Paulo, o uso do reconhecimento facial na segurança pública tem se expandido de forma significativa desde 2017, com a implementação de câmeras no sistema de transporte público, que resultou no bloqueio de mais de **300 mil** bilhetes nos dois primeiros anos por suposto uso indevido. A tecnologia também foi aplicada no Allianz Parque, em parceria com a Secretaria de Segurança Pública, contribuindo para a identificação de **275** pessoas desaparecidas e a prisão de **52** indivíduos procurados pela Justiça. Além disso, a cidade de Praia Grande conta com **3.036** câmeras integradas ao Centro Integrado de Comando e Operações Especiais (Cicoe), e a adoção desse sistema proporcionou uma redução superior a **60%** nos índices de roubo e furto de veículos, demonstrando o impacto positivo da tecnologia na prevenção e combate à criminalidade (SCOPEL; PUHL, 2024).

6.1.2 Exemplos no Estado do Rio de Janeiro

No Estado do Rio de Janeiro, a tecnologia de reconhecimento facial tem sido utilizada pela polícia para identificar criminosos que possam estar presentes em locais de grande aglomeração de pessoas e movimento intenso, como festas, shows, eventos esportivos e outras grandes reuniões que atraem multidões, além de diversas atividades sociais que têm o potencial de reunir um grande número de indivíduos (TERRA, 2021).

Scopel e Puhl (2024) relata que o sistema de reconhecimento facial foi adotado em 2019, inicialmente durante um projeto-piloto no Carnaval, quando foram instaladas **34** câmeras para monitoramento. Com o avanço da iniciativa, esse número foi posteriormente ampliado para **140** câmeras espalhadas por diferentes pontos da cidade. No entanto, apesar do uso crescente da tecnologia, ao menos duas pessoas foram presas de forma equivocada devido a falsos positivos gerados pelo sistema, evidenciando limitações e riscos associados à sua precisão.

6.1.3 Exemplos no Estado da Bahia

No Estado da Bahia, o uso da tecnologia de reconhecimento facial tem sido utilizada especialmente para fins de segurança pública (FAGUNDES; FERNANDES, 2024). Essa ferramenta tecnológica tem auxiliado as autoridades competentes na identificação não só de foragidos da justiça, mas também na identificação de pessoas que exibem comportamentos suspeitos.

Segundo Scopel e Puhl (2024), o uso do sistema de reconhecimento facial na segurança pública da Bahia tem se intensificado nos últimos anos, resultando na prisão de **1.438** pessoas com base nessa tecnologia. Somente nos primeiros meses de 2024, **185** prisões foram realizadas por meio do sistema, que emite, em média, de três a quatro alertas por dia. Apesar da intensidade no uso da ferramenta, foram registrados apenas dois casos de falsos positivos, ambos relacionados a mandados de prisão que já haviam sido revogados, o que evidencia uma taxa de precisão relativamente alta no funcionamento do sistema.

Na Bahia, os investimentos em reconhecimento facial vêm crescendo de forma expressiva, com o governo estadual destinando **R$ 665 milhões** para a ampliação do sistema, elevando o total de gastos para quase **R$ 900 milhões**. Como parte das políticas de segurança pública, o programa foi expandido para mais de **77** municípios, com câmeras instaladas em postes, viaturas e até em dispositivos móveis utilizados pelos próprios policiais, possibilitando abordagens em tempo real e maior agilidade nas ações de monitoramento e identificação (FAGUNDES; FERNANDES, 2024).

O programa de reconhecimento facial opera com uma taxa de similaridade de **95%**, ou seja, quando um indivíduo atinge esse nível de compatibilidade com o banco de dados da polícia, é automaticamente abordado pelas autoridades. No entanto, o trabalho de Fagundes e Fernandes (2024) destaca uma importante crítica ao sistema: a maioria das pessoas abordadas e presas são negras e de baixa renda, o que evidencia a reprodução de um viés racial na aplicação da tecnologia e levanta preocupações sobre desigualdades estruturais sendo potencializadas por ferramentas tecnológicas.

6.1.4 Uso em Sistemas de Segurança Privada

No que diz respeito ao uso em sistemas de segurança, o reconhecimento facial tem sido amplamente adotado por diversas empresas para reforçar a proteção de suas instalações, bens e propriedades, bem como para garantir a integridade e segurança de todos os seus funcionários e clientes (CAMPOS; FRANÇA; ROCHA, 2019). Além disso, a tecnologia avançada tem sido cada vez mais aplicada para identificar e prevenir situações de risco, como invasões indesejadas, roubos e atos de vandalismo. A integração do reconhecimento facial com outros sistemas de segurança visa fortalecer a segurança em todo o ambiente corporativo, criando um entorno de maior proteção e tranquilidade para todos os envolvidos (REIS, 2018).

7

Perspectivas Futuras

7.1 Aspectos legais e regulatórios

No Brasil, o uso de reconhecimento facial em sistemas de vídeo monitoramento está sujeito a regulamentação específica, com legislação que visa proteger a privacidade e os direitos individuais dos cidadãos (OLIVEIRA et al., 2022). Questões como a necessidade de consentimento prévio para a coleta e uso de dados biométricos, a transparência no uso da tecnologia e a responsabilidade pelo armazenamento e segurança das informações são temas frequentemente abordados. Além disso, existem discussões em andamento sobre a regulamentação do uso do reconhecimento facial em espaços públicos e privados, evidenciando a importância de um marco legal claro e abrangente para garantir a utilização ética e responsável dessa tecnologia.

O trabalho de Oliveira et al. (2022) aponta que, diante da crescente adoção do reconhecimento facial no Brasil, torna-se essencial avançar na regulamentação do uso dessa tecnologia, sugerindo que o país se inspire em modelos regulatórios já estabelecidos em nações como Reino Unido, França e Estados Unidos, que contam com regras mais robustas e mecanismos de controle mais desenvolvidos para garantir o uso ético, transparente e responsável desses sistemas.

7.1.1 Legislação e Regulamentação

A legislação brasileira, referente ao reconhecimento facial em sistemas de vídeo monitoramento, ainda está em um processo de evolução, com intensas discussões sobre a real necessidade de uma regulamentação específica que possa garantir a proteção efetiva de dados pessoais (SILVA, 2022). Atualmente, o uso dessa tecnologia é pautado pela Lei Geral de Proteção de Dados (LGPD) e pelo Marco Civil da Internet, que estabelecem diretrizes importantes. No entanto, existem perspectivas promissoras de que novas leis e regulamentações sejam aprovadas, como por exemplo o "PL 3069/2022"em breve para abordar de forma mais abrangente e detalhada a utilização do reconhecimento facial, visando não apenas a proteção de dados, mas também

assegurando a segurança e a privacidade dos cidadãos em um ambiente cada vez mais digital e conectado (LOPES; KOCH,).

7.1.2 Marco legal atual e perspectivas de evolução

O marco legal atualmente vigente sobre o uso de reconhecimento facial em sistemas de vídeo monitoramento no Brasil é fundamentado principalmente pela Lei Geral de Proteção de Dados (LGPD) e pelo Marco Civil da Internet (OLIVEIRA et al., 2022). Esses dois pilares legais estabelecem diretrizes importantes, mas existem grandes perspectivas de evolução para a criação de novas leis e regulamentações específicas que abordem, de maneira mais detalhada, as diretrizes e práticas para o uso dessa tecnologia emergente. É fundamental que essas diretrizes considerem não apenas a proteção de dados pessoais, mas também a privacidade dos cidadãos, garantindo assim a transparência e a segurança nos processos que envolvem a coleta, armazenamento e tratamento de informações biométricas (NOBRE, 2020). A discussão sobre o reconhecimento facial deve incorporar a participação ativa da sociedade, a fim de assegurar que os direitos dos indivíduos sejam respeitados e que haja um equilíbrio entre inovação tecnológica e proteção dos direitos humanos.

7.1.3 Projeto de Lei 3069/22

O Projeto de Lei 3069/22 tem como objetivo principal regulamentar de forma abrangente o uso das tecnologias de reconhecimento facial em território brasileiro, estabelecendo diretrizes claras e específicas para sua aplicação em sistemas de vídeo monitoramento. Entre as principais propostas contempladas no projeto, destaca-se a exigência de uma autorização prévia e expressa para a utilização do reconhecimento facial em diversas circunstâncias, assim como a garantia de total transparência em todo o processo, assegurando que os direitos individuais dos cidadãos sejam respeitados e protegidos (SANTOS; PRADO; RODRIGUEZ, 2023).

O projeto dedica-se a estabelecer diretrizes rigorosas para a coleta e o armazenamento de dados pessoais, visando garantir não apenas a segurança, mas também a privacidade das informações sensíveis dos cidadãos (ZOGAHIB et al., 2024). Assim, a proposta visa proporcionar um ambiente regulatório equilibrado, que permita a utilização da tecnologia moderna de forma responsável, sem comprometer a proteção dos direitos fundamentais que cada indivíduo possui dentro da sociedade. Por meio de tais medidas, espera-se que se crie um cenário onde a inovação não ultrapasse os limites éticos e legais, promovendo um uso consciente e respeitoso da tecnologia no dia a dia das pessoas.

7.2 Avanços tecnológicos

A evolução das tecnologias de reconhecimento facial trouxe avanços significativos na redução de vieses e aumento da confiabilidade (SOUZA; FERREIRA; NETO, 2022).

Novos algoritmos têm sido desenvolvidos para minimizar a ocorrência de erros e vieses em sistemas de vídeo monitoramento, buscando aprimorar a precisão e acurácia na identificação de indivíduos. Essas inovações tecnológicas são fundamentais para mitigar os desafios associados com falsas identificações e garantir a confiabilidade das informações fornecidas pelos sistemas de reconhecimento facial.

7.2.1 Redução de vieses e aumento da confiabilidade

As pesquisas em redução de vieses e aumento da confiabilidade em sistemas de reconhecimento facial têm se concentrado em estratégias para minimizar disparidades relacionadas a raça, gênero e idade (SILVA, 2022). Além disso, a utilização de conjuntos de dados mais diversificados e representativos tem contribuído para reduzir os vieses existentes nesse tipo de tecnologia, conforme estudos de Freitas et al. (2023) e Menezes (2024). A implementação de técnicas de verificação e validação dos dados também tem se mostrado eficaz na melhoria da confiabilidade dos resultados obtidos.

7.2.2 Inovações em algoritmos

As inovações em algoritmos de reconhecimento facial têm se concentrado na melhoria da precisão e no aumento da eficiência dos sistemas, conforme retrata Andrade e Jaborandy (2022). Novos métodos de aprendizado de máquina, como o uso de redes neurais convolucionais e algoritmos de *deep learning*, têm permitido avanços significativos na capacidade de identificação de faces em tempo real e em diferentes condições ambientais (SILVA, 2023). Além disso, a incorporação de técnicas de processamento de imagem e reconhecimento de padrões tem possibilitado aperfeiçoamentos constantes na performance dos algoritmos de reconhecimento facial.

7.3 Implicações éticas e sociais

O uso de reconhecimento facial levanta questões éticas e de privacidade, uma vez que envolve a coleta e processamento de dados pessoais. A necessidade de garantir o respeito aos direitos individuais e a proteção da privacidade das pessoas se torna fundamental nesse contexto, exigindo uma análise aprofundada dos impactos dessas tecnologias na sociedade (MOREIRA; RIBEIRO, 2023). Além disso, é essencial considerar os princípios éticos no uso do reconhecimento facial para orientar o desenvolvimento e aplicação desses sistemas de forma responsável.

Os princípios éticos no uso de reconhecimento facial incluem a transparência no funcionamento dos sistemas, a finalidade específica e legítima do processamento de dados, a minimização da coleta de informações, a anonimização dos dados quando possível, a garantia de segurança e integridade dos dados, bem como o respeito à autodeterminação informativa

das pessoas (OLIVEIRA et al., 2022). Esses princípios orientam a adoção responsável do reconhecimento facial, contribuindo para mitigar potenciais impactos negativos e proteger os direitos individuais (KUBOTA; ROSA, 2024).

No que se refere à proteção de dados pessoais, os desafios do uso de reconhecimento facial estão relacionados à segurança dessas informações, ao consentimento dos indivíduos para a coleta e processamento de dados, à necessidade de garantir a qualidade e atualização dos dados, e à prevenção de usos inadequados ou abusivos (MONTEIRO, 2021). Para enfrentar tais desafios, é fundamental implementar soluções como tecnologias de criptografia, mecanismos de consentimento informado, políticas de retenção de dados e auditorias de conformidade, visando assegurar a proteção efetiva dos dados pessoais nos sistemas de reconhecimento facial (COSTA; KREMER, 2022).

O uso do reconhecimento facial em sistemas de vídeo monitoramento pode trazer diversos impactos sociais e econômicos. Socialmente, há preocupações com a privacidade e a possibilidade de violação de direitos individuais, além de potenciais impactos psicológicos gerados pela vigilância constante. Economicamente, a implementação desses sistemas pode gerar empregos na área de tecnologia e segurança, mas também levanta questões sobre custo-benefício e o investimento necessário para garantir a eficácia e a segurança dos sistemas (BENTO, 2024).

8

Revisão de Literatura

8.1 Viés algorítmico e impacto social

A análise dos desafios brasileiros relacionados ao viés algorítmico no uso de reconhecimento facial em sistemas de vídeo monitoramento revela uma preocupação crescente com as implicações sociais e éticas dessa tecnologia. O estudo de Larsson (2019) destaca que sistemas como o Compas tendem a prever incorretamente taxas de criminalidade entre grupos raciais, evidenciando um viés social que pode complicar a compreensão das normas e valores culturais em tecnologias autônomas. A pesquisa aponta para a necessidade de refletir sobre como esses sistemas reproduzem desigualdades sociais e culturais, uma questão que se torna ainda mais relevante no contexto brasileiro.

Em 2020, Drozdowski et al. (2020) ampliam essa discussão ao explorar a emergência de viés demográfico em algoritmos biométricos. O estudo enfatiza que a falta de precisão em sistemas de reconhecimento facial pode resultar em danos reais, especialmente em cenários de vigilância estatal, onde erros de identificação podem ter consequências graves para grupos demográficos marginalizados. A pesquisa indica que a precisão dos algoritmos pode variar significativamente entre diferentes grupos, levantando questões sobre a justiça e a equidade no uso dessas tecnologias.

Leavy, O'Sullivan e Siapera (2020) também abordam os efeitos prejudiciais do viés racial em sistemas de inteligência artificial, ressaltando que as tecnologias biométricas, como o reconhecimento facial, tendem a ter menor precisão em indivíduos de pele mais escura, particularmente mulheres. O estudo sugere que a injustiça histórica na representação e classificação de dados contribui para a perpetuação de discriminações, o que é especialmente pertinente no Brasil, onde a desigualdade racial é uma questão crítica.

Moraes, Almeida e Pereira (2021) analisam o uso do reconhecimento facial em espaços públicos no Brasil, questionando sua eficácia e as implicações para a privacidade dos indivíduos.

A pesquisa destaca que, embora essa tecnologia seja promovida como uma ferramenta de segurança, suas aplicações podem levar a um aumento da vigilância e à exploração de dados pessoais, levantando preocupações éticas sobre o uso de tecnologia em contextos sociais.

A análise comparativa de Almeida, Shmarko e Lomas (2022) sobre as regulamentações de reconhecimento facial em diferentes contextos revela que a falta de responsabilidade e a perpetuação de preconceitos podem resultar em discriminação e desconfiança nas relações entre a população e as agências de segurança. A pesquisa sugere que a formação de viés nos algoritmos reflete a composição demográfica dos desenvolvedores, o que pode intensificar as desigualdades existentes.

Solarova et al. (2023) ressaltam que a tecnologia de reconhecimento facial falha em identificar corretamente populações de pele mais escura, com dados mostrando que uma porcentagem alarmante de indivíduos identificados incorretamente são negros. O estudo destaca que essas falhas não apenas afetam a confiança nas tecnologias, mas também têm implicações sérias para a saúde mental e a inclusão social de grupos marginalizados.

Noiret, Lumetzberger e Kampel (2021) discutem as práticas discriminatórias envolvendo o uso de IA na polícia, enfatizando a necessidade de mitigar os riscos de injustiça associados a essas tecnologias. A pesquisa fornece uma visão crítica sobre as intersecções entre tecnologia e justiça social, sugerindo que a transparência e a responsabilidade são essenciais para evitar a perpetuação de práticas discriminatórias.

Finalmente, DeAlcala et al. (2023) introduzem uma abordagem estatística para medir o viés em modelos de IA, destacando que o reconhecimento facial é um dos campos mais estudados em relação à análise de viés. A pesquisa aponta que a variação no desempenho dos algoritmos entre grupos populacionais é um tema recorrente, enfatizando a necessidade de uma definição clara de viés e a consideração de fatores demográficos na avaliação da eficácia dos sistemas de reconhecimento facial.

8.1.1 Revisão de Literatura de Viés algorítmico e impacto social

O trabalho de Larsson (2019) apresenta uma análise crítica sobre o viés social presente em sistemas de reconhecimento facial, com foco em sua aplicação comercial. A pesquisa revela que os sistemas de reconhecimento de imagem baseados em gênero apresentam uma taxa de erro significativamente maior ao categorizar mulheres de pele escura, enquanto a margem de erro é consideravelmente menor para homens brancos. Essa constatação levanta questões importantes sobre a eficácia e a justiça desses sistemas, especialmente em contextos onde a diversidade racial e de gênero é uma realidade.

Larsson (2019) utiliza o termo "viés social"para descrever essas discrepâncias, fundamentando-se em uma compreensão socio-legal das normas sociais e dos valores culturais. Essa abordagem é importante para entender como os sistemas de inteligência artificial (IA) não apenas refletem,

mas também reproduzem e reforçam desigualdades existentes na sociedade. A discussão enfatiza a necessidade de uma reflexão crítica sobre os valores e normas que permeiam o desenvolvimento da IA, considerando seu impacto na sociedade e nas oportunidades que oferece.

Os desafios enfrentados no Brasil em relação ao viés algorítmico no reconhecimento facial são evidentes quando se considera a diversidade racial do país. O estudo de Larsson (2019) sugere que a implementação de sistemas de vídeo monitoramento que utilizam reconhecimento facial pode exacerbar as desigualdades sociais, especialmente se esses sistemas forem baseados em dados que não representam adequadamente a população. Isso pode levar a uma vigilância desproporcional sobre grupos marginalizados, perpetuando estigmas e preconceitos.

Além disso, a análise de Larsson (2019) aponta para a necessidade de um diálogo mais amplo sobre as implicações éticas e sociais da IA. É fundamental que desenvolvedores, legisladores e a sociedade civil colaborem para garantir que os sistemas de reconhecimento facial sejam projetados e implementados de maneira justa e equitativa. A falta de atenção a esses aspectos pode resultar em consequências negativas não apenas para indivíduos, mas também para a coesão social e a confiança nas instituições.

O trabalho de Drozdowski et al. (2020) aborda a questão dos viéses demográficos em sistemas biométricos, com um foco particular nas tecnologias de reconhecimento facial. Os autores destacam que a utilização de algoritmos de decisão em sistemas de reconhecimento facial pode levar a consequências prejudiciais significativas, especialmente em contextos de vigilância estatal.

Um dos pontos centrais do artigo de Drozdowski et al. (2020) é a diferenciação dos impactos do viés algorítmico, que podem variar conforme o cenário de aplicação. No caso de sistemas de controle de acesso cooperativo, os viéses demográficos podem resultar em tentativas adicionais de autenticação para certos grupos demográficos, devido a erros de falso negativo. Essa situação, embora inconveniente, é menos grave do que os impactos observados em cenários de vigilância, onde os erros de falso positivo podem levar a detenções injustificadas e danos pessoais substanciais. Assim, a discussão sobre o viés algorítmico em reconhecimento facial é particularmente relevante no contexto brasileiro, onde questões sociais e raciais estão profundamente entrelaçadas com a aplicação de tecnologias de vigilância.

Drozdowski et al. (2020) também ressaltam que, embora a tecnologia de reconhecimento biométrico possa ser altamente precisa sob condições ideais, como iluminação adequada e câmeras de alta resolução, os viéses não são introduzidos deliberadamente nos algoritmos. Em vez disso, eles emergem do conjunto de dados utilizados para treinar os sistemas. Essa observação é essencial, pois indica que a solução para os problemas de viés algorítmico não reside apenas na melhoria dos algoritmos, mas também na curadoria cuidadosa dos dados de treinamento.

Além disso, o artigo de Drozdowski et al. (2020) sugere que é fundamental desenvolver uma estrutura para avaliações de impacto humano em biometria, para mitigar os riscos associados

ao uso de tecnologias de reconhecimento facial em contextos de vigilância. Essa proposta é particularmente pertinente em um cenário brasileiro, onde a aplicação de tais tecnologias pode exacerbar desigualdades sociais existentes e levar a um aumento na discriminação racial e social.

O trabalho de Leavy, O'Sullivan e Siapera (2020) aborda de maneira incisiva os efeitos prejudiciais da injustiça e do viés nos sistemas de inteligência artificial (IA), especialmente no contexto do reconhecimento facial e suas implicações para os direitos iguais na sociedade. Os autores destacam que a tecnologia de reconhecimento facial, embora esteja se tornando cada vez mais comum em infraestruturas de segurança e controle de fronteiras, apresenta uma precisão alarmantemente baixa, especialmente em indivíduos de pele mais escura, particularmente mulheres. Essa questão é fundamental para a análise dos desafios enfrentados no Brasil, onde a diversidade racial é uma característica marcante da população.

Leavy, O'Sullivan e Siapera (2020) argumentam que o viés e a discriminação em IA não são fenômenos novos, mas sim uma continuação de uma longa história de injustiça que se manifesta na forma como os dados são coletados, representados e classificados. Essa perspectiva é particularmente relevante no contexto brasileiro, onde as desigualdades raciais e sociais são profundas e persistentes. O reconhecimento facial, quando implementado sem uma consideração crítica sobre esses viéses, pode perpetuar e até exacerbar as desigualdades existentes, levando a decisões injustas que afetam as comunidades mais vulneráveis.

Além disso, o artigo de Leavy, O'Sullivan e Siapera (2020) sugere que a pesquisa fundamentada na justiça social, estudos críticos de raça e feminismo pode servir como base para uma nova abordagem na coleta e curadoria de dados para IA. Essa proposta é primordial, pois implica que a solução para os problemas de viés algorítmico não reside apenas em ajustes técnicos, mas também na reavaliação das estruturas sociais que sustentam a coleta de dados. Os desafios técnicos mencionados pelos autores, como a dificuldade em mitigar preconceitos existentes nos dados, são questões que precisam ser abordadas de forma colaborativa entre tecnólogos, formuladores de políticas e a sociedade civil.

O trabalho de Moraes, Almeida e Pereira (2021) oferece uma análise abrangente sobre o uso do reconhecimento facial no Brasil, com foco nas implicações de privacidade e segurança associadas a essa tecnologia. A pesquisa é particularmente relevante no contexto brasileiro, onde a implementação de sistemas de reconhecimento facial tem se expandido em locais como blocos de carnaval no Rio de Janeiro e Salvador, além de projetos de cidades inteligentes em Campinas.

Moraes, Almeida e Pereira (2021) destacam que a principal motivação para a adoção do reconhecimento facial no Brasil é a segurança, uma vez que essa tecnologia é vista como uma ferramenta eficaz para identificar indivíduos que cometeram ou estão prestes a cometer crimes. No entanto, a questão levantada é se essa tecnologia realmente proporciona um benefício significativo em comparação com câmeras de vigilância tradicionais, que podem ter um impacto menor na privacidade das pessoas. Essa crítica é fundamental, pois sugere que a eficácia do reconhecimento facial em termos de segurança deve ser reavaliada à luz das preocupações éticas

e de privacidade.

Além disso, Moraes, Almeida e Pereira (2021) abordam a questão do uso dos dados coletados por empresas que operam esses sistemas, levantando preocupações sobre a possibilidade de que esses dados sejam utilizados para fins além da segurança, como o perfilamento de usuários para serviços de marketing personalizados. Essa questão é particularmente pertinente em um contexto onde a proteção de dados pessoais é uma preocupação crescente, e a falta de regulamentação adequada pode levar a abusos.

O artigo de Moraes, Almeida e Pereira (2021) também discute as medidas técnicas e legais que podem ser implementadas para proteger os dados pessoais e a privacidade dos indivíduos no Brasil. Os autores enfatizam a importância de entender as características técnicas do reconhecimento facial para avaliar seu impacto e as diferentes finalidades de uso em espaços públicos, tanto por entidades estatais quanto por partes privadas. Essa análise é vital para desenvolver um entendimento mais profundo sobre as implicações do reconhecimento facial e para formular políticas que garantam a proteção dos direitos dos cidadãos.

O trabalho escrito por Almeida, Shmarko e Lomas (2022) apresenta uma análise crítica sobre as implicações éticas e sociais do uso de tecnologias de reconhecimento facial, especialmente em contextos de monitoramento policial. A obra destaca a necessidade de uma maior responsabilidade e prestação de contas na implementação dessas tecnologias, enfatizando as preocupações com viés e discriminação.

Almeida, Shmarko e Lomas (2022) argumentam que a vigilância digital, como a monitorização de mídias sociais, pode ser comparada a uma prática de "parada e revistagem digital", levantando questões sobre a credibilidade das agências de segurança pública. Essa analogia é particularmente pertinente no contexto brasileiro, onde a confiança nas instituições de segurança é frequentemente abalada por escândalos de corrupção e abuso de poder. A falta de responsabilidade no uso de algoritmos de reconhecimento facial pode exacerbar a discriminação contra comunidades já marginalizadas, levando a um ciclo de desconfiança entre a população e as autoridades, conforme Almeida, Shmarko e Lomas (2022).

Outro ponto crítico abordado no artigo é a questão do viés de entrada, que se refere à influência dos desenvolvedores na criação de algoritmos. Os autores observam que a maioria dos profissionais de tecnologia nas regiões ocidentais é composta por homens brancos, o que pode resultar em um viés não intencional no desenvolvimento de tecnologias como o reconhecimento facial. Essa observação é particularmente relevante no contexto brasileiro, onde a diversidade racial e de gênero é significativa, e a aplicação de tecnologias que não consideram essa pluralidade pode levar a falhas de identificação e discriminação ((ALMEIDA; SHMARKO; LOMAS, 2022)).

O artigo também menciona que a eficácia dos sistemas de reconhecimento facial pode ser comprometida se forem treinados predominantemente com dados de rostos de homens brancos. Isso levanta preocupações sobre a capacidade desses sistemas de operar de maneira justa e

equitativa em uma sociedade diversificada. A análise dos autores sugere que a falta de supervisão humana e a dependência excessiva de algoritmos podem aumentar o risco de decisões errôneas e preconceituosas, especialmente em um cenário onde a vigilância é ampliada ((ALMEIDA; SHMARKO; LOMAS, 2022)).

O trabalho de Solarova et al. (2023) apresenta uma análise crítica sobre o uso de tecnologias de reconhecimento facial em espaços públicos, destacando os desafios enfrentados por populações negras, asiáticas e de minorias étnicas (BAME). A pesquisa revela que essas populações são desproporcionalmente mal identificadas ou não identificadas, um problema que se agrava em contextos como o brasileiro, onde 90,5% das pessoas presas devido ao uso de Reconhecimento Facial para segurança pública eram negras.

Solarova et al. (2023) argumentam que as falhas do FRT em identificar corretamente indivíduos de pele mais escura não são meramente limitações tecnológicas, mas refletem um viés social e racial que permeia os dados de treinamento utilizados para desenvolver esses sistemas. Essa constatação é alarmante, pois sugere que as tecnologias, longe de serem neutras, podem perpetuar e amplificar desigualdades existentes, resultando em consequências sociais e psicológicas significativas para os indivíduos afetados.

Além disso, o trabalho de Solarova et al. (2023) discute como a implementação de sistemas de reconhecimento facial pode exacerbar fenômenos de classificação social corporal, onde informações sensíveis podem ser expostas e utilizadas por *stakeholders* para hierarquizar populações. Essa dinâmica não apenas reforça a exclusão social de minorias, mas também pode impactar a saúde mental dos indivíduos, afetando sua autoestima e respeito próprio.

Solarova et al. (2023) chamam a atenção para a necessidade de uma regulação mais rigorosa e consciente do uso de FRT, especialmente em contextos onde o viés racial pode ter consequências devastadoras. A abordagem proposta sugere que, para mitigar esses riscos, é fundamental que as políticas de implementação considerem o contexto social e racial das populações afetadas, garantindo que as tecnologias não sejam utilizadas como ferramentas de opressão.

O trabalho escrito por Noiret, Lumetzberger e Kampel (2021), aborda questões cruciais relacionadas ao viés algorítmico em sistemas de reconhecimento facial, especialmente no contexto do sistema de justiça criminal. Os autores discutem como práticas discriminatórias envolvendo o uso de inteligência artificial (IA) na atuação policial têm gerado controvérsias significativas nos últimos anos. Esse tema é particularmente relevante no Brasil, onde a implementação de tecnologias de reconhecimento facial em sistemas de vídeo monitoramento levanta preocupações sobre a equidade e a justiça.

Noiret, Lumetzberger e Kampel (2021) iniciam o artigo contextualizando a origem dessas práticas discriminatórias, destacando que, apesar do avanço tecnológico, a implementação de algoritmos de reconhecimento facial frequentemente reproduz e amplifica preconceitos existentes

na sociedade. A análise crítica dos autores revela que a falta de diversidade nos dados utilizados para treinar esses sistemas é um fator central que contribui para a perpetuação de viéses raciais e socioeconômicos. Essa preocupação é especialmente pertinente no Brasil, onde as desigualdades sociais e raciais são profundas e historicamente enraizadas.

Além disso, o artigo de Noiret, Lumetzberger e Kampel (2021) explora três aplicações em desenvolvimento que utilizam reconhecimento facial, enfatizando os riscos associados à falta de equidade. Os autores discutem como esses riscos podem ser mitigados, sugerindo a necessidade de uma abordagem mais crítica e reflexiva na implementação de tecnologias de IA. Eles argumentam que é fundamental que as instituições responsáveis pela aplicação da lei adotem práticas que garantam a transparência e a responsabilidade na utilização de algoritmos, bem como a inclusão de vozes diversas no processo de desenvolvimento e avaliação dessas tecnologias.

Em uma avaliação crítica, o trabalho de Noiret, Lumetzberger e Kampel (2021) oferece uma contribuição significativa para a discussão sobre viés algorítmico e justiça no uso de reconhecimento facial. No entanto, seria enriquecedor que os autores também abordassem exemplos práticos de como essas diretrizes poderiam ser implementadas no contexto brasileiro, considerando as especificidades culturais e sociais do país. A discussão sobre como as políticas públicas podem ser moldadas para garantir a equidade no uso de tecnologias de reconhecimento facial é um aspecto que merece maior atenção, especialmente em um cenário onde a tecnologia avança rapidamente, mas as desigualdades persistem.

O trabalho de DeAlcala et al. (2023), aborda de maneira abrangente o viés presente em sistemas de reconhecimento facial, um aspecto crítico no contexto brasileiro, onde questões de desigualdade social e racial são particularmente relevantes. Os autores destacam que o viés em modelos de aprendizado de máquina (ML) é um tema em crescente investigação, especialmente no campo da biometria facial, onde a análise de viés se torna essencial devido à sua aplicação em sistemas de vídeo monitoramento.

Um dos pontos centrais do artigo de DeAlcala et al. (2023) é a inadequação do critério de paridade estatística para modelos de reconhecimento facial. Os autores argumentam que um modelo considerado perfeito não garante paridade demográfica, especialmente em contextos onde variáveis entrelaçadas, como etnia e cor da pele, influenciam os resultados. Essa perspectiva é fundamental para entender os desafios enfrentados no Brasil, onde a diversidade étnica e racial pode levar a disparidades significativas na eficácia dos sistemas de reconhecimento facial. A ideia de que os resultados de um sistema de reconhecimento facial não são independentes da etnia de um indivíduo é um alerta importante para a implementação dessas tecnologias, especialmente em um país com um histórico de discriminação racial.

DeAlcala et al. (2023) também discutem o conceito de "odds igualados", que se refere à medição de falsos negativos e falsos positivos entre diferentes grupos demográficos como uma forma de avaliar a justiça dos algoritmos de reconhecimento facial. Essa abordagem é particularmente relevante no contexto brasileiro, onde a aplicação de tais sistemas pode exacerbar

desigualdades existentes se não forem adequadamente calibrados para diferentes grupos étnicos.

Além disso, o trabalho de DeAlcala et al. (2023) ressalta que a literatura existente frequentemente falha em definir claramente o que constitui viés, limitando-se a demonstrar que o desempenho dos algoritmos varia entre grupos populacionais. Essa lacuna na definição é preocupante, pois impede uma análise mais profunda e uma mitigação eficaz dos viéses identificados. A crescente quantidade de estudos acadêmicos focados na equidade dos algoritmos de reconhecimento facial, conforme mencionado pelos autores, é um sinal positivo, mas ainda há um longo caminho a percorrer para garantir que as tecnologias de reconhecimento facial sejam justas e equitativas para todos os grupos.

Por fim, a menção aos fatores ambientais e demográficos, como a cor da pele, como influências significativas no desempenho dos sistemas de reconhecimento facial, destaca a complexidade do problema. No Brasil, onde a diversidade racial é vasta, é imperativo que os desenvolvedores e implementadores de tecnologias de reconhecimento facial considerem essas variáveis para evitar discriminações e garantir a eficácia dos sistemas.

8.2 Infraestrutura e Integração de Sistemas

A revisão da literatura a seguir explora os desafios enfrentados pelo Brasil no que diz respeito à infraestrutura e à integração de sistemas no uso de reconhecimento facial em sistemas de vídeo monitoramento. A discussão é fundamentada em uma série de artigos que abordam questões críticas relacionadas à privacidade, segurança e regulamentação das tecnologias de reconhecimento facial.

O trabalho de Leslie (2020) destaca a questão do consentimento individual no uso de imagens pessoais coletadas de redes sociais para a criação de conjuntos de dados utilizados em sistemas de reconhecimento facial. O autor argumenta que a exploração indevida dessas imagens tem levado a violações sistemáticas dos direitos de privacidade e consentimento, especialmente em contextos que deveriam respeitar convenções de direitos humanos e leis de proteção de dados. Essa problemática se torna ainda mais relevante no Brasil, onde a Lei Geral de Proteção de Dados (LGPD) estabelece diretrizes rigorosas para a coleta e o tratamento de dados pessoais.

Em 2022, Teixeira, Januzi e Faria (2022) abordam a falta de algoritmos eficazes nas Secretarias Estaduais de Segurança Pública do Brasil, que não utilizam técnicas de detecção automática para avaliar imagens de identificação. O estudo enfatiza a necessidade urgente de treinamento para os agentes envolvidos na identificação, além de destacar a vulnerabilidade dos sistemas biométricos em relação à proteção dos dados pessoais. A implementação de práticas recomendadas é essencial para evitar consequências negativas para a sociedade, especialmente no contexto da LGPD.

Ainda em 2022, Solarova et al. (2023) discutem a necessidade de regulamentação do

uso de tecnologias de reconhecimento facial em espaços públicos. O artigo propõe que a distinção entre espaços públicos semi-abertos e abertos pode facilitar uma abordagem mais clara e transparente para a regulamentação dessas tecnologias. A questão da segurança e da autenticação confiável é central, ressaltando a importância de técnicas que respeitem a privacidade dos cidadãos.

O trabalho de Ardabili et al. (2022) explora o impacto da vigilância por vídeo inteligente (SVS) na segurança pública, levantando preocupações éticas em torno da privacidade e da proteção de dados. A pesquisa aponta que a regulamentação das tecnologias deve garantir que as preocupações éticas do público sejam abordadas, refletindo sobre a necessidade de um design de sistema que equilibre segurança e privacidade.

O trabalho de Ramos (2023) complementa essa discussão ao analisar como a legislação abrangente pode levar à proibição de tecnologias biométricas específicas, citando exemplos de cidades nos Estados Unidos que baniram o uso de reconhecimento facial. O autor argumenta que, embora as proibições não resolvam todos os problemas de privacidade, a necessidade de uma legislação detalhada é importante para proteger os dados pessoais e a privacidade dos cidadãos.

Por fim, o trabalho de Negri, Hupont e Gomez (2024) revela a resistência e desconfiança dos brasileiros em relação ao reconhecimento facial por parte das autoridades de segurança. A aceitação dessa tecnologia é influenciada pela confiança nas entidades que coletam informações faciais e pela percepção cultural do seu uso. A pesquisa destaca a importância de considerar essas perspectivas culturais ao decidir sobre a adoção de sistemas de reconhecimento facial por órgãos públicos.

Esses estudos coletivos demonstram a complexidade dos desafios enfrentados pelo Brasil na implementação de sistemas de reconhecimento facial, enfatizando a necessidade de um equilíbrio entre segurança, privacidade e confiança pública.

8.2.1 Revisão de Literatura de Infraestrutura e Integração de Sistemas

O trabalho de Leslie (2020), aborda questões cruciais relacionadas ao uso de tecnologias de reconhecimento facial, especialmente no que tange ao consentimento individual e à privacidade. A análise crítica do material revela um cenário preocupante no que diz respeito à coleta e uso de imagens pessoais extraídas da internet, particularmente de redes sociais, para a formação de grandes conjuntos de dados utilizados por sistemas de reconhecimento facial.

Leslie (2020) argumenta que a forma como as tecnologias têm sido desenvolvidas e implementadas demonstra uma falta de consideração pelos direitos de privacidade e consentimento dos indivíduos. O autor destaca que os desenvolvedores têm tratado o acesso aberto e a reutilização de dados como uma autorização irrestrita, resultando em violações sistemáticas de direitos. Essa prática é especialmente relevante no contexto brasileiro, onde a infraestrutura de tecnologia e os sistemas de vídeo monitoramento estão em rápida expansão, mas muitas vezes carecem de

regulamentações adequadas que protejam os cidadãos.

Além disso, o trabalho de Leslie (2020) menciona a necessidade de avaliações de impacto sobre a proteção de dados, conforme estipulado pelo Regulamento Geral sobre a Proteção de Dados (GDPR) na Europa. Essa exigência enfatiza a importância de considerar os efeitos potenciais do processamento de dados em larga escala, algo que poderia ser igualmente aplicado ao Brasil, onde a Lei Geral de Proteção de Dados (LGPD) busca estabelecer diretrizes semelhantes.

O trabalho de Leslie (2020) sobre a falta de responsabilidade e a ausência de um *framework* legal robusto para governar o uso de tecnologias de reconhecimento facial é um ponto central que ressoa com os desafios brasileiros. O autor sugere que a implementação de salvaguardas que respeitem os direitos humanos e as normas de proteção de dados é essencial para evitar abusos, promovendo uma abordagem mais ética e responsável no desenvolvimento e uso dessas tecnologias.

O trabalho de Teixeira, Januzi e Faria (2022) aborda questões cruciais relacionadas à segurança pública no Brasil, especialmente no que diz respeito ao uso de tecnologias de reconhecimento facial em sistemas de vídeo monitoramento. Os autores destacam a ausência de algoritmos de detecção automática de ataques de metamorfose nas Secretarias Estaduais de Segurança Pública (SSPs), o que representa uma lacuna significativa na robustez dos processos de aquisição e armazenamento de imagens.

Um dos principais desafios mencionados por Teixeira, Januzi e Faria (2022) é a falta de bases de dados públicas que possam ser utilizadas para o desenvolvimento e teste desses algoritmos. Essa deficiência limita a capacidade dos pesquisadores e profissionais de segurança em criar soluções eficazes e confiáveis. A necessidade de treinamento adequado para todos os agentes envolvidos no processo de identificação é enfatizada, pois a compreensão das vulnerabilidades do sistema é fundamental para mitigar riscos associados à implementação de tecnologias de reconhecimento facial.

Teixeira, Januzi e Faria (2022) também discutem o impacto da Lei Geral de Proteção de Dados (LGPD) na utilização de sistemas biométricos. A legislação estabelece diretrizes rigorosas para a coleta e processamento de dados pessoais, e a utilização indiscriminada de sistemas vulneráveis pode levar a consequências graves, tanto para os indivíduos quanto para a sociedade como um todo. Essa preocupação é especialmente relevante em um contexto onde a automação de tarefas, possibilitada pela inteligência artificial, está se tornando cada vez mais comum.

O trabalho escrito por Solarova et al. (2023) aborda as complexidades e os desafios associados ao uso de tecnologias de reconhecimento facial (FRT) em espaços públicos, especialmente no contexto das preocupações sociais e éticas que surgem com sua implementação. A discussão é particularmente relevante para o Brasil, onde a integração de sistemas de vídeo monitoramento com reconhecimento facial se torna cada vez mais comum, mas também suscita questões sobre

privacidade e segurança.

Solarova et al. (2023) destacam a crescente necessidade de regulamentação das tecnologias de reconhecimento facial, enfatizando que a extração e comparação automatizada de características faciais para identificação de indivíduos é uma prática que deve ser cuidadosamente avaliada. No Brasil, onde a infraestrutura de segurança pública enfrenta desafios significativos, a adoção de FRT pode oferecer benefícios substanciais, como o aumento da eficiência na identificação de suspeitos e a melhoria na segurança pública. No entanto, essa implementação não deve ser feita sem uma análise crítica das implicações éticas e sociais que ela acarreta.

Um dos pontos centrais do trabalho de Solarova et al. (2023) é a distinção entre espaços públicos semi-abertos e abertos, o que é determinante para a discussão sobre a regulamentação do uso de FRT. Essa diferenciação pode ser aplicada ao contexto brasileiro, onde a diversidade de ambientes urbanos e rurais requer abordagens específicas para a implementação de tecnologias de reconhecimento facial. A regulamentação adequada pode ajudar a mitigar os riscos de abusos e garantir que os direitos dos cidadãos sejam respeitados.

Além disso, Solarova et al. (2023) mencionam que a necessidade de técnicas de autenticação confiáveis se torna cada vez mais crítica em um mundo onde as ameaças à segurança estão em constante evolução. No Brasil, as questões de segurança nacional e pública são frequentemente debatidas, e a integração de FRT em sistemas de vídeo monitoramento pode ser uma ferramenta poderosa, desde que utilizada de forma responsável e sob uma regulamentação robusta.

O trabalho de Ardabili et al. (2022) aborda de forma crítica os desafios enfrentados pelo uso de reconhecimento facial em sistemas de vídeo monitoramento, com ênfase nas questões de privacidade e segurança dos dados. A análise apresentada pelos autores destaca que, embora a tecnologia de vigilância por vídeo tenha avançado significativamente, sua aceitação e implementação são frequentemente obstaculizadas por preocupações éticas e pela falta de uma regulamentação uniforme no Brasil.

Ardabili et al. (2022) argumentam que a confiança na tecnologia é um fator inapelável para sua adoção por entidades públicas, privadas e pela população em geral. No entanto, a ausência de diretrizes federais claras e a abordagem fragmentada entre os estados resultam em restrições que dificultam a implementação eficaz do reconhecimento facial. Exemplos de regiões que proibiram essa tecnologia, como Berkeley e San Francisco, ilustram a hesitação de muitos locais em adotar sistemas que potencialmente invadem a privacidade dos cidadãos.

Além disso, o trabalho de Ardabili et al. (2022) enfatiza que a falta de regulamentações específicas não apenas limita o uso de tecnologias de reconhecimento facial, mas também impacta as grandes empresas de tecnologia que dependem dessas ferramentas. A análise crítica dos autores sugere que, para que o reconhecimento facial contribua de forma efetiva para a segurança pública, é imperativo que os sistemas sejam projetados com um enfoque ético que respeite a privacidade dos indivíduos. Isso implica a necessidade de um equilíbrio entre a segurança e os

direitos dos cidadãos, o que se torna um desafio significativo no contexto brasileiro.

O trabalho de Ramos (2023) oferece uma análise crítica sobre o uso de tecnologias biométricas, especialmente sistemas de reconhecimento facial, em contextos de vigilância governamental. A obra destaca a crescente preocupação com a privacidade individual e os desafios legais associados à implementação dessas tecnologias, que se tornam ainda mais relevantes no contexto brasileiro.

Ramos (2023) menciona que diversas cidades dos Estados Unidos, como San Francisco e Boston, já tomaram a iniciativa de proibir o uso de sistemas de reconhecimento facial por órgãos públicos, refletindo uma resposta a evidências de que tais sistemas tendem a apresentar taxas elevadas de erro, especialmente em relação a pessoas de cor. Essa situação levanta questões sobre a eficácia e a ética do uso de reconhecimento facial, que também se aplicam ao Brasil, onde a integração de sistemas de videomonitoramento com tecnologias de reconhecimento facial ainda está em desenvolvimento.

No Brasil, a implementação de sistemas de reconhecimento facial enfrenta desafios semelhantes, incluindo a necessidade de regulamentação adequada que proteja os dados pessoais e a privacidade dos cidadãos.

Ramos (2023) argumenta que a mera proibição de tecnologias específicas não resolve os problemas subjacentes, pois pode levar a uma transição para outras formas de vigilância que não são necessariamente mais seguras ou éticas. Esta perspectiva é particularmente pertinente ao considerar a infraestrutura existente no Brasil, que muitas vezes carece de diretrizes claras e robustas para o uso responsável de tecnologias avançadas.

Além disso, Ramos (2023) sugere que a criação de legislações mais detalhadas, que levem em conta as particularidades dos sistemas biométricos, é essencial para estabelecer um quadro legal que não apenas proteja a privacidade, mas também permita o desenvolvimento de novas tecnologias. No contexto brasileiro, onde a implementação de sistemas de videomonitoramento é ampla, a necessidade de um banco de dados biométrico centralizado pode aumentar os riscos à privacidade, enfatizando a importância de considerar abordagens descentralizadas.

O trabalho de Negri, Hupont e Gomez (2024), de apresenta uma análise crítica sobre o uso de sistemas de reconhecimento facial em cenários de monitoramento, destacando a complexidade e os desafios enfrentados na implementação dessas tecnologias, especialmente no contexto brasileiro.

Negri, Hupont e Gomez (2024) abordam a relutância e a desconfiança do público em relação ao uso do reconhecimento facial por agências de segurança. Essa resistência é particularmente relevante no Brasil, onde questões de privacidade e confiança nas instituições frequentemente permeiam o debate sobre segurança pública.

A pesquisa revela que a aceitação do reconhecimento facial está intimamente ligada à percepção de confiança nas entidades que coletam e gerenciam os dados faciais. Em cenários

onde os indivíduos sentem que suas informações estão sob controle e segurança, a aceitação tende a ser maior. Essa dinâmica é fundamental para entender os desafios de integração de sistemas de vídeo monitoramento, uma vez que a desconfiança pode levar a uma resistência generalizada à adoção dessas tecnologias.

Além disso, o artigo de Negri, Hupont e Gomez (2024) destaca que a percepção pública do reconhecimento facial é influenciada por fatores culturais, o que implica que uma abordagem única pode não ser eficaz em um país tão diverso quanto o Brasil. A necessidade de considerar a perspectiva cultural nas decisões sobre a implementação de sistemas de reconhecimento facial é um ponto central da discussão. Os autores argumentam que, sem uma compreensão adequada do contexto cultural, as iniciativas para integrar essas tecnologias podem falhar em obter a aceitação necessária, resultando em um uso ineficaz e potencialmente invasivo.

Outro aspecto relevante abordado por Negri, Hupont e Gomez (2024) é a questão da utilidade percebida do reconhecimento facial. Quando os usuários não identificam um benefício claro em sua aplicação, tendem a vê-lo como uma invasão de privacidade, o que pode agravar ainda mais a resistência à sua adoção. Este ponto é especialmente crítico para a implementação de sistemas de vídeo monitoramento no Brasil, onde a transparência e a comunicação eficaz sobre os benefícios e a segurança do uso dessas tecnologias são fundamentais para conquistar a confiança do público.

8.3 Taxa de Erro e Confiabilidade

A revisão da literatura sobre os desafios brasileiros relacionados à taxa de erro e confiabilidade no uso de reconhecimento facial em sistemas de vídeo monitoramento revela uma evolução significativa na pesquisa e desenvolvimento dessas tecnologias ao longo dos anos.

Desde os primeiros estudos, como o de Marin (2006), que introduziu métodos estatísticos para o reconhecimento de padrões faciais, enfatizando a importância da correlação e da normalização das condições de iluminação, até a análise mais recente das implicações legais e éticas do uso da biometria, a literatura demonstra um crescente reconhecimento dos desafios técnicos e sociais envolvidos.

Queirolo, Silva e Bellon (2009) avançou na discussão ao apresentar um sistema automático de reconhecimento facial em 3D, utilizando o algoritmo *Simulated Annealing*, que mostrou resultados promissores em termos de taxa de verificação e identificação. Este estudo destacou a importância de abordar a complexidade das expressões faciais, um fator que pode impactar diretamente a precisão dos sistemas de reconhecimento.

Mais tarde, Manuel et al. (2016) exploraram a aplicação da visão computacional para segurança pública, ressaltando as dificuldades enfrentadas na tarefa de rastreamento de pessoas em ambientes dinâmicos. A pesquisa indicou que, apesar dos avanços, a análise ainda depende

fortemente da intervenção humana, revelando a necessidade de sistemas automáticos mais eficientes.

Marcondes (2023) trouxe à tona as implicações do reconhecimento facial no contexto da segurança pública, discutindo suas aplicações e os riscos associados ao uso indevido da tecnologia. A capacidade de reconhecer rostos em alta velocidade e a acessibilidade dos sistemas foram destacados como fatores que podem levar a abusos, especialmente em contextos sensíveis.

Em 2018, MOURA et al. (2016) focou no agrupamento de faces em vídeos digitais, abordando a crescente necessidade de sistemas que possam extrair informações relevantes de uma quantidade massiva de dados visuais. A pesquisa enfatizou a importância de desenvolver técnicas eficazes para melhorar a vigilância e a segurança.

Ainda em 2018, Brito (2018) investigou a análise facial utilizando mapas de profundidade e aprendizado profundo, apontando a importância de sistemas em tempo real que possam adaptar-se e melhorar continuamente. Este estudo destacou a necessidade de integrar diferentes tipos de dados para alcançar um reconhecimento facial mais robusto.

Loureiro e Carneiro (2020) discutiu as limitações do reconhecimento facial como uma forma de identificação biométrica, ressaltando que, apesar de sua implementação em políticas de segurança, a precisão não é garantida. Essa análise crítica evidencia a necessidade de cautela no uso dessas tecnologias.

Finalmente, Teixeira, Januzi e Faria (2022) abordaram a vulnerabilidade dos sistemas de identificação biométrica no Brasil, destacando a falta de algoritmos adequados para garantir a segurança das imagens capturadas e a importância da formação dos agentes de segurança. A pesquisa também enfatizou os desafios impostos pela Lei Geral de Proteção de Dados (LGPD) e as consequências potenciais do uso inadequado dessas tecnologias.

8.3.1 Revisão de Literatura da Taxa de Erro e Confiabilidade

O trabalho de Marin (2006) oferece uma análise aprofundada das abordagens estatísticas aplicadas ao reconhecimento facial, um tema de crescente relevância em sistemas de vídeo monitoramento no Brasil. A autora destaca que, embora o método de correlação apresente alta precisão, sua complexidade computacional limita sua aplicabilidade em cenários práticos. Em contraste, o método *autoface*, apesar de um desempenho inferior, se mostra mais viável devido à sua simplicidade, o que é um fator irrefutável em ambientes com restrições de recursos computacionais.

Marin (2006) também enfatiza a importância da escolha adequada do número de componentes principais no método *autoface*, onde uma maior quantidade pode resultar em uma taxa de reconhecimento superior. Isso sugere que, para melhorar a confiabilidade dos sistemas de reconhecimento facial, é fundamental considerar a otimização dos parâmetros do modelo. Além disso, a autora menciona que o método baseado em Modelos Ocultos de Markov (HMM)

se destaca como uma alternativa superior ao *autoface*, indicando que a pesquisa nesta área deve continuar a explorar técnicas que ofereçam tanto precisão quanto eficiência.

Outro ponto indiscutível abordado no artigo é a necessidade de uma abordagem multifacetada no desenvolvimento de sistemas de reconhecimento facial.

Marin (2006) argumenta que a combinação de diferentes classificadores e a consideração das condições de iluminação são essenciais para a robustez do sistema. Essa perspectiva é particularmente relevante no contexto brasileiro, onde a variabilidade nas condições de iluminação e a diversidade demográfica podem afetar significativamente a taxa de erro nos sistemas de reconhecimento facial.

O trabalho de Queirolo, Silva e Bellon (2009), apresenta uma abordagem inovadora para o reconhecimento facial que utiliza imagens tridimensionais. O autor propõe um sistema automático baseado no algoritmo *Simulated Annealing* (SA) para o alinhamento de imagens de profundidade, empregando a *Surface Interpenetration Measure* (SIM) como métrica de similaridade entre as imagens faciais. Essa metodologia é particularmente relevante no contexto do reconhecimento facial, onde a precisão e a confiabilidade são cruciais, especialmente em aplicações de segurança e vigilância.

Um dos principais pontos abordados no trabalho de Queirolo, Silva e Bellon (2009) é a combinação da SIM para quatro regiões da face, o que permite uma análise mais detalhada e robusta das características faciais. Essa técnica é significativa, pois a variação nas expressões faciais pode impactar negativamente a eficácia dos sistemas de reconhecimento, e a abordagem modificada do SA busca mitigar esses efeitos durante o processo de alinhamento. Os resultados experimentais indicam uma taxa de verificação impressionante de 96,5% e uma Taxa de Falsa Aceitação (FAR) de apenas 0,1%, destacando a eficácia do método proposto em comparação com abordagens anteriores.

Além disso, o trabalho de Queirolo, Silva e Bellon (2009) discute as duas principais abordagens para o tratamento de informações faciais em 3D: imagens de profundidade e nuvens de pontos. A utilização de técnicas estatísticas, como a Análise de Componentes Principais (PCA), e o método *Iterative Closest Point* (ICP) são mencionados como ferramentas fundamentais para o alinhamento e comparação de imagens faciais. O uso do Erro Quadrático Médio (MSE) como critério de similaridade oferece uma base sólida para a avaliação da precisão do reconhecimento.

Entretanto, é importante considerar as implicações práticas da implementação de sistemas de reconhecimento facial 3D, especialmente no Brasil, onde os desafios relacionados à taxa de erro e confiabilidade são preponderantes. A alta taxa de verificação apresentada no estudo pode não se traduzir em resultados equivalentes em cenários do mundo real, onde variáveis como iluminação, ângulo de captura e diversidade demográfica podem impactar a eficácia dos sistemas. Portanto, é essencial que futuras pesquisas abordem essas questões, buscando melhorar ainda mais a confiabilidade dos sistemas de reconhecimento facial em ambientes complexos.

O trabalho de Manuel et al. (2016), aborda as complexidades e desafios associados ao uso de sistemas de reconhecimento facial em ambientes de vídeo monitoramento. A pesquisa destaca a importância da visão computacional na segurança pública, enfatizando que, apesar dos avanços tecnológicos, a maioria dos sistemas ainda depende da interpretação humana para a análise de imagens.

Um dos principais pontos discutidos é a dificuldade de rastrear pessoas em locais públicos, que é amplamente afetada por fatores como mudanças de iluminação, velocidade de locomoção dos indivíduos, oclusões e alterações bruscas na trajetória conforme Manuel et al. (2016).

Esses desafios não apenas dificultam a precisão do reconhecimento facial, mas também contribuem para uma alta taxa de erro nos sistemas atualmente implementados. A dependência de operadores humanos para a análise de vídeo, como mencionado pelos autores, acentua a necessidade de um sistema automatizado mais robusto e confiável.

Manuel et al. (2016) argumentam que, embora os modelos de reconhecimento de características faciais tenham o potencial de melhorar a eficiência do monitoramento, a implementação eficaz desses sistemas ainda enfrenta barreiras significativas. A falta de um monitoramento eletrônico completamente eficiente representa um desafio computacional que deve ser superado para garantir a confiabilidade e a precisão do reconhecimento facial em aplicações de segurança. Assim, a pesquisa sugere que melhorias na tecnologia de visão computacional são essenciais para reduzir as taxas de erro e aumentar a confiança nos sistemas de vídeo monitoramento.

O trabalho de Marcondes (2023), aborda a aplicação do reconhecimento facial no contexto da segurança pública e suas implicações, tanto tecnológicas quanto jurídicas. A análise desse material revela importantes aspectos sobre os desafios enfrentados no Brasil em relação à taxa de erro e à confiabilidade dessa tecnologia.

Um dos pontos centrais do trabalho de Marcondes (2023) é a inevitabilidade das mudanças faciais ao longo do tempo, que podem impactar a eficácia dos sistemas de reconhecimento facial. Essa questão é conclusiva, pois a precisão do reconhecimento facial depende da capacidade de identificar características faciais que podem variar com a idade, saúde ou outros fatores. Assim, a taxa de erro associada a esses sistemas pode ser elevada, especialmente se considerarmos a diversidade populacional brasileira, que apresenta uma ampla gama de características físicas.

Além disso, Marcondes (2023) menciona que a tecnologia de reconhecimento facial é amplamente utilizada em países desenvolvidos para combater o terrorismo em locais públicos. Contudo, no Brasil, a implementação dessa tecnologia enfrenta barreiras financeiras significativas, o que pode limitar seu acesso e eficácia. O custo reduzido dos sensores, que podem ser adquiridos por aproximadamente 300 dólares, é um atrativo; no entanto, a infraestrutura necessária para garantir a confiabilidade do sistema ainda é um desafio a ser superado.

Outro aspecto relevante abordado no trabalho de Marcondes (2023) é a capacidade do reconhecimento facial de mapear 80 pontos do rosto, o que demonstra um avanço tecnológico

significativo. No entanto, essa mesma tecnologia pode ser potencialmente maliciosa, levantando preocupações sobre privacidade e segurança. A possibilidade de um uso inadequado ou abusivo dessa tecnologia em sistemas de vídeo monitoramento é um tema que merece atenção, especialmente em um contexto onde os direitos civis e a proteção de dados pessoais estão em discussão.

O trabalho de MOURA et al. (2016) aborda um tema relevante dentro da área de Visão Computacional, focando especificamente na identificação e agrupamento de faces em vídeos. O autor destaca a importância do reconhecimento facial, especialmente no contexto da crescente produção de vídeos digitais, que se tornou uma parte integral da vida cotidiana, abrangendo áreas como segurança, entretenimento e pesquisa científica.

MOURA et al. (2016) apresenta uma análise detalhada dos desafios associados ao agrupamento de faces, enfatizando que as faces humanas são características semânticas de alto nível que desempenham um papel incondicional na extração de informações relevantes de vídeos. A formalização do problema em estudo é um ponto forte do artigo, pois permite que o leitor compreenda as motivações que justificam a pesquisa e a necessidade de sistemas mais eficientes para a recuperação de dados em vídeos conforme MOURA et al. (2016).

Apesar das contribuições significativas, o trabalho de MOURA et al. (2016) também levanta questões críticas sobre a confiabilidade e a taxa de erro dos sistemas de reconhecimento facial. A eficácia desses sistemas é frequentemente comprometida por variáveis como iluminação, ângulos de captura e a qualidade dos vídeos, o que pode resultar em altas taxas de erro na identificação de indivíduos.

Além disso, MOURA et al. (2016) menciona que o desenvolvimento de métodos de agrupamento de faces deve considerar a diversidade das faces humanas e as diferentes condições em que os vídeos são gravados. Essa consideração é categórica para minimizar os erros e aumentar a confiança nos sistemas implementados. A pesquisa aponta para a necessidade de um avanço contínuo nas técnicas de aprendizado de máquina e inteligência artificial para enfrentar esses desafios.

O trabalho de Brito (2018) aborda a complexidade da análise facial por meio de dados multimodais, enfatizando sua relevância em aplicações de segurança, como sistemas de vídeo monitoramento. A proposta central do estudo é investigar a aplicabilidade de uma abordagem que utiliza algoritmos de aprendizagem profunda para mapear e avaliar padrões faciais humanos, o que é inapelável para a confiabilidade e precisão desses sistemas.

Brito (2018) destaca que a coleta e análise sequencial de dados faciais é um desafio significativo, especialmente em ambientes de trabalho onde a detecção em tempo real é necessária. A falta de sistemas acessíveis e fáceis de usar, que operem de forma eficaz em condições variadas, é um ponto crítico que o autor menciona. Isso está diretamente relacionado aos desafios enfrentados no Brasil, onde a implementação de tecnologias de reconhecimento facial frequentemente encontra

barreiras, como a variabilidade das condições de iluminação e a diversidade da população.

O trabalho de Brito (2018) também discute a necessidade de um sistema que não apenas detecte, mas que também interprete dados de sensores multimodais, incluindo a capacidade de anotações e análise tridimensional. Essa abordagem é fundamental para melhorar continuamente o modelo de classificação e, por conseguinte, a precisão dos sistemas de reconhecimento facial. A capacidade de reanalisar dados é especialmente relevante, pois permite que os sistemas aprendam e se adaptem a novas informações, o que é essencial em um contexto onde a taxa de erro pode impactar severamente a confiabilidade dos resultados.

Uma crítica que pode ser feita ao trabalho de Brito (2018) é a falta de uma discussão mais aprofundada sobre as implicações éticas e sociais do uso de reconhecimento facial em sistemas de vídeo monitoramento. Embora a análise técnica e a proposta de um modelo mais robusto sejam valiosas, a implementação de tais sistemas no Brasil deve considerar as preocupações com privacidade e segurança, que são frequentemente levantadas em debates sobre essa tecnologia.

O trabalho de Loureiro e Carneiro (2020), aborda de forma crítica a utilização do reconhecimento facial como uma modalidade de identificação biométrica. A autora destaca que essa tecnologia se fundamenta em algoritmos que analisam características faciais específicas para identificar indivíduos, sendo amplamente aplicada em sistemas de vídeo monitoramento, tanto em contextos públicos quanto privados.

Um dos principais desafios discutidos no trabalho é a questão da precisão e confiabilidade dos sistemas de reconhecimento facial.

Loureiro e Carneiro (2020) enfatiza que, embora esses sistemas sejam frequentemente promovidos como soluções eficazes para a segurança, não é possível garantir uma precisão absoluta. A incerteza inerente aos algoritmos utilizados para o reconhecimento facial levanta preocupações significativas sobre a taxa de erro, que pode resultar em identificações incorretas e, consequentemente, em violações de direitos individuais.

Além disso, Loureiro e Carneiro (2020) menciona que a falta de confiabilidade dos sistemas de reconhecimento facial impõe desafios adicionais, como a necessidade de regulamentações jurídicas que possam proteger os cidadãos de potenciais abusos. A ausência de uma legislação clara e eficaz pode levar a um uso indiscriminado da tecnologia, exacerbando problemas de discriminação e vigilância excessiva, especialmente em um contexto social marcado por desigualdades.

O trabalho de Teixeira, Januzi e Faria (2022) apresenta uma discussão crítica sobre os desafios enfrentados pelas Secretarias Estaduais de Segurança Pública (SSPs) no Brasil em relação ao uso de algoritmos de reconhecimento facial e a confiabilidade desses sistemas. A principal ideia do artigo destaca a ausência de algoritmos de detecção automática de ataques de metamorfose nas práticas atuais de identificação, o que compromete a robustez do processo de aquisição e armazenamento de imagens.

Teixeira, Januzi e Faria (2022) argumentam que, desde 2018, existe uma recomendação para a implementação de práticas que garantam maior segurança no manejo das imagens. No entanto, a falta de bases de dados públicas para o desenvolvimento de algoritmos eficazes representa um obstáculo significativo para a pesquisa e inovação nessa área. Essa carência de dados não apenas limita o avanço tecnológico, mas também aumenta a vulnerabilidade dos sistemas de reconhecimento facial, que podem ser facilmente manipulados por ataques sofisticados.

Outro ponto relevante abordado no trabalho de Teixeira, Januzi e Faria (2022) é a necessidade de treinamento adequado para todos os agentes envolvidos no processo de identificação. A compreensão das vulnerabilidades dos sistemas é importante, uma vez que os ataques estão em constante evolução, acompanhando o avanço das tecnologias. A formação contínua dos profissionais da segurança é, portanto, uma medida essencial para mitigar os riscos associados ao uso de sistemas biométricos.

Ademais, o trabalho de Teixeira, Januzi e Faria (2022) menciona a Lei Geral de Proteção de Dados (LGPD), que estabelece diretrizes rigorosas para a coleta e armazenamento de dados pessoais no Brasil. Os autores ressaltam que a utilização de sistemas biométricos vulneráveis pode resultar em consequências graves para a sociedade, uma vez que não há garantias de proteção contra ataques que esses sistemas possam sofrer. Essa realidade levanta questões éticas e legais sobre a privacidade e a segurança dos dados dos cidadãos.

8.4 Impacto nos direitos civis e humanos

A revisão da literatura que se segue explora os desafios enfrentados no Brasil em relação ao impacto dos sistemas de reconhecimento facial sobre os direitos civis e humanos, especialmente no contexto de populações vulneráveis.

A análise começa com o trabalho de Silva e Oliveira (2021), que discute as peculiaridades da violência de gênero em comunidades de favelas e a interseção dessa problemática com o uso de tecnologias. O estudo revela como as soluções tecnológicas, frequentemente aplicadas de maneira padrão, podem agravar as vulnerabilidades das mulheres nas favelas, que já enfrentam um ambiente de violência urbana e desconfiança em relação à polícia. A pesquisa sugere que uma abordagem única para a mitigação de abusos tecnológicos pode ser ineficaz e que é essencial considerar as realidades específicas dessas populações ao desenvolver políticas e tecnologias.

Em seguida, Sarabdeen (2022) analisa a proteção dos direitos individuais no uso da tecnologia de reconhecimento facial, destacando como essa tecnologia, embora possa melhorar a gestão em diversos setores, também levanta sérias preocupações sobre a privacidade. O autor argumenta que a falta de transparência na utilização do reconhecimento facial pode resultar em violações de privacidade e discriminação, especialmente em contextos como o de contratação e seguros. A pesquisa enfatiza a necessidade urgente de um arcabouço legal adequado que proteja

os dados biométricos e assegure a responsabilidade dos usuários da tecnologia.

Por fim, Teixeira, Januzi e Faria (2022) abordam as implicações da adoção de sistemas de reconhecimento biométrico pelo governo brasileiro, questionando a segurança dos dados dos cidadãos na era da inteligência artificial. O artigo propõe uma discussão crítica sobre os riscos associados à implementação desses sistemas, especialmente se não forem projetados e geridos de maneira adequada, e destaca a importância de respeitar a Lei Geral de Proteção de Dados (LGPD) no processo. A pesquisa levanta questões fundamentais sobre a integridade e a proteção dos dados pessoais, sugerindo que a falta de um planejamento cuidadoso pode resultar em sérias consequências para os direitos civis dos brasileiros.

8.4.1 Revisão de Literatura sobre o impacto nos direitos civis e humanos

O trabalho de Silva e Oliveira (2021), aborda as complexidades e os desafios enfrentados por mulheres que vivem em favelas brasileiras, especialmente no contexto do uso de tecnologias de monitoramento e reconhecimento facial. A pesquisa destaca como as soluções tecnológicas convencionais, frequentemente aplicadas de maneira padronizada, podem, na verdade, exacerbar as vulnerabilidades dessas mulheres, que já estão em uma posição precária devido a fatores como a violência urbana e a desconfiança em relação às autoridades.

Silva e Oliveira (2021) argumentam que o Brasil, sendo o maior país da América Latina e com uma população de mais de 200 milhões de pessoas, apresenta desigualdades etnoraciais acentuadas e um acesso generalizado à Internet. Dentro desse contexto, as favelas, onde cerca de 11,4 milhões de brasileiros residem, são caracterizadas por alta densidade populacional e falta de regulamentação governamental, frequentemente dominadas por narcotraficantes ou milícias. Essas condições tornam as mulheres em favelas particularmente vulneráveis à violência urbana e ao feminicídio, criando um cenário onde muitas evitam buscar ajuda das forças de segurança devido à desconfiança.

A análise dos autores se aprofunda na necessidade de considerar as especificidades culturais e sociais dessas comunidades ao implementar soluções tecnológicas. Ao utilizar o referencial teórico de Chua et al. (2019), Silva e Oliveira (2021) exploram as consequências não intencionais que podem surgir da aplicação de tecnologias de mitigação de abusos, destacando que soluções universais são inadequadas para atender as necessidades de populações vulneráveis. Essa crítica é especialmente relevante no contexto do reconhecimento facial, que pode ser utilizado de forma a aumentar a vigilância sobre essas mulheres, em vez de protegê-las.

O trabalho de Silva e Oliveira (2021) também levanta questões de pesquisa pertinentes para futuros estudos sobre a proteção da privacidade online de vítimas de violência de gênero, enfatizando a importância de um enfoque que leve em consideração a realidade específica das favelas. Essa abordagem pode contribuir para o desenvolvimento de políticas públicas mais eficazes e sensíveis às necessidades das mulheres em contextos de vulnerabilidade.

O traballho de Sarabdeen (2022) aborda questões cruciais relacionadas ao uso da tecnologia de reconhecimento facial (FRT) e suas implicações para os direitos civis e humanos, especialmente no contexto da privacidade. A análise apresentada destaca a ausência de notificação sobre a utilização de FRT em ambientes como lojas, o que pode ser considerado uma violação da privacidade dos indivíduos. Essa falta de transparência é um ponto crítico, pois a coleta de informações biométricas sensíveis sem o consentimento adequado pode levar a consequências severas, incluindo a autocensura e a limitação da liberdade de expressão.

Sarabdeen (2022) argumenta que a coleta e o uso indevido de dados biométricos não apenas afetam a privacidade, mas também criam um ambiente de estresse para os indivíduos, comprometendo seu bem-estar psicológico. A inalterabilidade dos dados gerados pela FRT requer uma proteção especial, uma vez que a manipulação ou o uso indevido dessas informações pode resultar em violações significativas dos direitos humanos. A autora também menciona que muitos países de *common law* ainda não implementaram legislações específicas para a proteção de dados biométricos, o que resulta em lacunas legais que dificultam o controle sobre violações de privacidade.

O trabalho de Sarabdeen (2022) se propõe a analisar a adequação das leis existentes que regulam o uso da FRT, enfatizando a necessidade de um arcabouço legal que não apenas aborde as violações de privacidade, mas que também crie mecanismos de responsabilização para os usuários da tecnologia. A autora sugere que, apesar do potencial lucrativo da FRT, é imperativo que as empresas respeitem a privacidade dos consumidores, evitando compromissos éticos que possam surgir em função da busca por lucro.

O trabalho de Teixeira, Januzi e Faria (2022) aborda questões cruciais relacionadas à implementação de sistemas de reconhecimento biométrico no Brasil. A proposta do governo de adquirir um sistema de reconhecimento facial para uso em todo o território nacional levanta preocupações significativas sobre a proteção dos dados pessoais e os direitos civis e humanos dos cidadãos.

Teixeira, Januzi e Faria (2022) discutem que, embora a tecnologia de reconhecimento facial possa oferecer benefícios em termos de segurança pública, sua adoção sem um planejamento adequado pode resultar em sérios problemas. Eles enfatizam a necessidade de um projeto e gerenciamento cuidadosos para evitar a violação de direitos fundamentais, como a privacidade e a liberdade individual. A falta de diretrizes claras e de um arcabouço legal robusto pode levar à manipulação indevida de dados e à discriminação, especialmente em um país com uma diversidade étnica e social tão ampla como o Brasil.

Uma das contribuições mais relevantes do trabalho de Teixeira, Januzi e Faria (2022) é a lista de dez questões que os autores elaboraram para iniciar um debate sobre a segurança dos dados na era da Inteligência Artificial. Essas questões não apenas destacam os riscos associados à implementação de sistemas de reconhecimento facial, mas também ressaltam a importância do cumprimento da Lei Geral de Proteção de Dados (LGPD). A LGPD estabelece normas rigorosas

para o tratamento de dados pessoais, e sua aplicação é fundamental para garantir que a tecnologia não seja utilizada de maneira a comprometer os direitos dos cidadãos.

Teixeira, Januzi e Faria (2022) também alertam para o potencial de abusos de poder que podem surgir com a utilização inadequada dessas tecnologias. A história recente do Brasil já mostra exemplos de como a vigilância estatal pode ser utilizada para reprimir manifestações e controlar a população. Portanto, a implementação de sistemas de reconhecimento facial deve ser acompanhada de um debate ético e jurídico profundo.

8.5 Aceitação pública e desinformação

A análise dos desafios brasileiros relacionados à aceitação pública e à desinformação no uso de reconhecimento facial em sistemas de vídeo monitoramento revela um panorama complexo, onde a intersecção entre tecnologia e direitos fundamentais se torna cada vez mais evidente. O trabalho de Aires e Gregori (2017) discute as transformações que a era digital impôs aos direitos à privacidade e à proteção de dados, enfatizando a necessidade de compreender como o direito ao esquecimento pode servir como um mecanismo de proteção nesse novo contexto.

Aires argumenta que a evolução das relações interpessoais mediadas pela internet demanda uma reavaliação dos direitos garantidos no ordenamento jurídico brasileiro, especialmente no que tange à privacidade em um mundo onde a informação circula de forma rápida e acessível.

Em continuidade, Santos (2018) traz à tona uma crítica contundente sobre a forma como tanto organizações públicas quanto privadas têm manejado informações pessoais, destacando a insatisfação popular em relação à vigilância sistemática proporcionada pelo reconhecimento facial. Santos (2018) discute a falta de comunicação eficaz e a exclusão da participação cidadã nos processos de implementação dessas tecnologias, sugerindo que essa vigilância não apenas infringe direitos, mas também perpetua desigualdades sociais. Sua pesquisa enfatiza a importância de refletir sobre a contra vigilância e os direitos à imagem e à cidade, ressaltando o papel do ativismo e da arte na contestação dessas práticas.

Por fim, Loureiro e Carneiro (2020) complementa essa discussão ao abordar a regulação jurídica e as tecnologias do poder, enfatizando como a utilização de biometria facial pode desconfigurar a noção do humano como sujeito de direito.

Loureiro e Carneiro (2020) observa que a aplicação de tecnologias de identificação está se tornando uma prática comum no Brasil, com exemplos como o 'Projeto de Identificação Biométrica da Justiça Eleitoral', que busca não apenas a segurança do processo eleitoral, mas também levanta questões sobre a privacidade e a coleta de dados corporais. Loureiro e Carneiro (2020) destaca a preocupação com a amplitude da aplicação dessas tecnologias e suas implicações para os direitos individuais, sugerindo que o reconhecimento facial, embora possa ter benefícios, também traz riscos significativos que precisam ser cuidadosamente considerados.

8.5.1 Revisão de Literatura da aceitação pública e desinformação

O trabalho de Aires e Gregori (2017), aborda a complexa relação entre a era digital e os direitos fundamentais, destacando especialmente o direito à privacidade e a aplicação do direito ao esquecimento. A análise proposta pelo autor é relevante para o entendimento dos desafios enfrentados pelo Brasil em relação à aceitação pública e à desinformação no uso de tecnologias como o reconhecimento facial em sistemas de vídeo monitoramento.

A pesquisa de Aires e Gregori (2017) se fundamenta em uma abordagem dedutiva e utiliza o método de estudo de caso, o que permite uma análise aprofundada dos conflitos envolvendo o direito à privacidade em um contexto tecnológico. O autor argumenta que, embora o direito ao esquecimento tenha o potencial de proteger a privacidade dos indivíduos, sua aplicação efetiva ainda enfrenta diversas barreiras, especialmente em um ambiente onde a informação é amplamente acessível e frequentemente mal interpretada.

Um dos pontos críticos abordados no trabalho de Aires e Gregori (2017) é a necessidade de uma compreensão mais clara dos direitos garantidos pelo ordenamento jurídico brasileiro e como esses direitos têm se transformado com o avanço das tecnologias digitais. A desinformação, um dos principais desafios no cenário atual, pode comprometer a aceitação pública de sistemas de reconhecimento facial, uma vez que a falta de compreensão sobre como esses sistemas operam e suas implicações para a privacidade pode gerar resistência por parte da população.

Além disso, Aires e Gregori (2017) destaca que a aplicação do direito ao esquecimento não é uma solução definitiva, mas sim uma ferramenta que deve ser utilizada com cautela, levando em consideração os direitos de terceiros e o interesse público. Essa reflexão é essencial para o debate sobre a implementação de tecnologias de monitoramento facial no Brasil, onde a aceitação pública é frequentemente minada por preocupações relacionadas à privacidade e à segurança dos dados.

O trabalho de Santos (2018), oferece uma análise crítica sobre a implementação de sistemas de reconhecimento facial no Brasil, destacando os desafios relacionados à aceitação pública e à desinformação. A pesquisa evidencia a preocupação com a forma como tanto organizações públicas quanto privadas têm utilizado as informações pessoais dos cidadãos, levantando questões fundamentais sobre privacidade, vigilância e os direitos dos indivíduos na sociedade contemporânea.

Santos (2018) argumenta que a vigilância, por meio de tecnologias de reconhecimento facial, se tornou uma prática cotidiana e está cada vez mais disseminada, o que gera um ambiente de insegurança e desconfiança entre os cidadãos. O autor ressalta que essa situação não apenas ameaça a privacidade, mas também reforça desigualdades sociais existentes, onde certos grupos podem ser mais vulneráveis à vigilância e à manipulação de dados. Essa crítica é essencial para entender a dinâmica de poder que se estabelece entre o Estado, o mercado e os indivíduos, e como essa relação pode ser utilizada para controlar e reprimir.

Além disso, o trabalho de Santos (2018) sugere que a desinformação em torno das tecnologias de reconhecimento facial contribui para uma aceitação acrítica por parte do público. A falta de compreensão sobre como essas tecnologias funcionam e suas implicações éticas e sociais pode levar a uma normalização da vigilância, sem que os cidadãos estejam plenamente cientes dos riscos envolvidos. Santos chama a atenção para a necessidade de promover um debate mais amplo sobre contra-vigilância e os direitos à cidade, à imagem e ao esquecimento, enfatizando que a sociedade deve estar atenta aos perigos que essas tecnologias representam.

O trabalho de Loureiro e Carneiro (2020) aborda a crescente utilização de tecnologias de reconhecimento facial no Brasil, inserindo essa prática dentro de um contexto mais amplo de vigilância e controle social. A autora destaca que a identificação biométrica, embora não seja uma novidade, está se expandindo rapidamente, especialmente com a implementação do "Projeto de Identificação Biométrica da Justiça Eleitoral". Este projeto visa aumentar a segurança do processo eleitoral, utilizando informações corporais para prevenir fraudes.

A análise crítica do trabalho de Loureiro e Carneiro (2020) revela que, apesar dos benefícios potenciais dessas tecnologias, como a segurança e eficiência na identificação, existem desafios significativos relacionados à aceitação pública e à desinformação. Loureiro e Carneiro (2020) sugere que a implementação de sistemas de reconhecimento facial enfrenta resistência devido a preocupações com a privacidade e a vigilância excessiva. Essa resistência é exacerbada pela falta de informação clara e acessível sobre como essas tecnologias funcionam e quais são suas implicações sociais e éticas.

Loureiro e Carneiro (2020) também discute a necessidade de um arcabouço jurídico que regule o uso dessas tecnologias, enfatizando que a ausência de uma legislação robusta pode levar a abusos e à desconfiança da população. O reconhecimento facial, quando mal utilizado, pode resultar em discriminação e violação de direitos individuais, o que reforça a importância de um debate público informado sobre o tema.

Criminalização e discriminação de minorias

A discussão sobre o uso de tecnologia de reconhecimento facial e seus impactos nas minorias no Brasil é complexa e multifacetada, refletindo preocupações éticas, sociais e legais que emergem à medida que essa tecnologia se torna mais prevalente nos sistemas de vídeo monitoramento.

O trabalho de Gentzel (2021) destaca as armadilhas morais associadas ao reconhecimento facial, enfatizando que a utilização de tecnologias tendenciosas por parte das forças de segurança não apenas compromete os valores democráticos, mas também perpetua desigualdades raciais ao desconsiderar o princípio de tratamento igualitário perante a lei.

Gentzel (2021) argumenta que a aplicação de tal tecnologia em contextos de vigilância pode resultar em consequências políticas e sociais adversas, especialmente para grupos marginalizados.

Sannon e Forte (2022) expandem essa discussão ao abordar como as comunidades marginalizadas enfrentam riscos elevados de violação de privacidade ao interagir com tecnologias. O estudo revela que a falta de consideração pelas necessidades dessas populações na concepção de tecnologias, como o reconhecimento facial, pode acentuar a exclusão social e a marginalização. As barreiras tecnológicas e culturais enfrentadas por essas comunidades dificultam ainda mais a proteção de sua privacidade, ressaltando a necessidade de uma abordagem mais inclusiva no desenvolvimento tecnológico.

No contexto da aplicação de algoritmos na polícia, Burkhardt, Borradaile e Gelvin (2023) identificam como as disparidades raciais se manifestam através do uso de softwares de monitoramento social. Eles discutem a possibilidade de "circuitos de *feedback*"raciais, onde algoritmos que analisam dados históricos podem intensificar a vigilância sobre comunidades minoritárias, exacerbando as desigualdades já existentes no sistema de justiça. Este fenômeno é particularmente preocupante, pois sugere que a tecnologia, longe de ser uma solução neutra, pode reforçar preconceitos históricos e contribuir para a super-representação de pessoas de cor no sistema prisional.

Por fim, o trabalho de Ardabili et al. (2023) oferece uma perspectiva sobre como as percepções de segurança em relação à tecnologia de vigilância variam entre diferentes grupos demográficos. A pesquisa revela que a preocupação com a identificação equivocada de minorias por sistemas de reconhecimento facial é um tema recorrente, evidenciado pelo caso de Ardabili et al. (2023), que ilustra as falhas desses sistemas e a necessidade urgente de abordar os preconceitos raciais inerentes a essas tecnologias. A literatura sugere que a digitalização e a implementação de tecnologias de vigilância têm impactos desiguais, moldados por fatores como alfabetização digital e acesso a recursos, o que requer uma análise crítica e cuidadosa das implicações sociais dessas práticas no Brasil.

8.5.2 Revisão de Literatura da criminalização e discriminação de minorias

O trabalho de Gentzel (2021), oferece uma análise crítica sobre o uso da tecnologia de reconhecimento facial (TRF) por órgãos de segurança pública, destacando as implicações morais e políticas associadas a essa prática. O autor argumenta que a utilização de TRF enviesada por parte da polícia não apenas compromete a igualdade de tratamento perante a lei, mas também representa uma ameaça aos princípios fundamentais da democracia liberal.

Gentzel (2021) elabora um argumento liberal contra a TRF enviesada, sustentando que essa tecnologia é incompatível com os valores clássicos do liberalismo, que defendem que todos os indivíduos devem ser tratados de forma equitativa. O autor enfatiza que a aplicação da TRF, em sua forma atual, perpetua desigualdades e discriminações, especialmente em relação a minorias, que frequentemente são alvos desproporcionais de vigilância e criminalização. Essa dinâmica não apenas reforça estigmas sociais, mas também pode levar a um ciclo vicioso de marginalização e exclusão.

Além disso, o trabalho de Gentzel (2021) aborda a necessidade de maior transparência e regulamentação no uso de algoritmos de aprendizado de máquina. Gentzel (2021) discute como a TRF pode ameaçar a autodeterminação, interferindo nas interações sociais que fundamentam a noção de livre arbítrio. A crítica à falta de consentimento informado na utilização da TRF por governos e empresas reforça a ideia de que a implementação dessa tecnologia carece de uma base ética sólida.

O trabalho de Sannon e Forte (2022), oferece uma análise crítica sobre os desafios enfrentados por grupos marginalizados no contexto da tecnologia, especialmente no que se refere ao uso de sistemas de reconhecimento facial e vídeo monitoramento. Os autores destacam que esses grupos não apenas precisam utilizar tecnologias que podem comprometer sua privacidade, mas também enfrentam riscos elevados associados a essas tecnologias.

Um dos principais pontos abordados por Sannon e Forte (2022) é a maneira como as violações de privacidade impactam desproporcionalmente essas populações. Os pesquisadores ressaltam que a exclusão tecnológica e social dos grupos marginalizados é um fator importante que deve ser considerado ao desenvolver e implementar tecnologias de reconhecimento facial. Essa exclusão não apenas limita o acesso a recursos e oportunidades, mas também aumenta a vulnerabilidade desses grupos a abusos e discriminações, perpetuando um ciclo de marginalização.

Sannon e Forte (2022) também discutem as limitações dos sistemas de reconhecimento facial, que frequentemente não são projetados com as necessidades dos grupos marginalizados em mente. Isso leva a uma série de desafios relacionados à privacidade, que merecem uma investigação mais aprofundada. A falta de representação desses grupos no processo de design tecnológico resulta em soluções que não atendem às suas realidades, o que pode amplificar a discriminação e a criminalização.

Além disso, o trabalho de Sannon e Forte (2022) sugere que a pesquisa sobre privacidade deve incluir uma perspectiva mais inclusiva, que leve em conta as experiências e necessidades específicas dos grupos marginalizados. Essa abordagem não apenas ajudaria a mitigar os riscos associados ao uso de tecnologias invasivas, mas também promoveria um desenvolvimento mais equitativo e socialmente responsável dessas tecnologias.

O trabalho escrito por Burkhardt, Borradaile e Gelvin (2023), aborda a questão das disparidades raciais dentro do sistema de justiça, especialmente no que diz respeito ao uso de algoritmos em contextos de policiamento e monitoramento social. Os autores destacam que essas disparidades não são apenas um reflexo de práticas policiais tradicionais, mas também são exacerbadas pelo uso de tecnologia, como softwares de monitoramento de mídias sociais e algoritmos de reconhecimento facial.

Um dos pontos centrais do trabalho de Burkhardt, Borradaile e Gelvin (2023) é a identificação de "circuitos de retroalimentação"baseados em raça que podem surgir a partir da aplicação de algoritmos em comunidades minoritárias. Esses circuitos ocorrem quando

algoritmos identificam padrões de dados que levam a uma intensificação do policiamento em comunidades raciais minoritárias, resultando em um ciclo vicioso que perpetua e agrava as disparidades raciais na punição criminal. Essa análise é particularmente relevante para o contexto brasileiro, onde o uso de reconhecimento facial em sistemas de videomonitoramento pode, de maneira análoga, criar e reforçar desigualdades raciais.

Burkhardt, Borradaile e Gelvin (2023) também discutem o uso de algoritmos para quantificar o risco de reincidência em suspeitos ou condenados, mencionando o algoritmo COMPAS como um exemplo notório que foi criticado por apresentar viés contra réus negros. Essa crítica ressalta uma preocupação fundamental: a confiança em algoritmos que não levam em consideração as complexidades sociais e raciais pode resultar em decisões judiciais que não apenas são injustas, mas também profundamente prejudiciais para as comunidades minoritárias.

A análise crítica apresentada no trabalho de Burkhardt, Borradaile e Gelvin (2023) sugere que a implementação de tecnologias de monitoramento e reconhecimento facial deve ser acompanhada de uma avaliação cuidadosa de seus impactos raciais e sociais. O uso indiscriminado dessas tecnologias pode não apenas falhar em resolver problemas de segurança pública, mas também exacerbar a discriminação e a criminalização de minorias, refletindo um padrão de injustiça que já está presente em muitos sistemas de justiça.

O trabalho de Ardabili et al. (2023) aborda a complexidade das percepções públicas sobre a segurança e a tecnologia de vigilância por vídeo, destacando como essas percepções variam significativamente entre diferentes grupos demográficos. A principal ideia do artigo enfatiza que as preocupações com a segurança pública não são homogêneas, refletindo uma diversidade de experiências e sentimentos que são moldados por fatores como idade, gênero e status socioeconômico. Um aspecto cabal discutido é a relação entre o reconhecimento facial e a criminalização de minorias.

O trabalho de Ardabili et al. (2023) menciona a preocupação generalizada sobre a tendência dos sistemas de reconhecimento facial em cometer erros de identificação, particularmente em relação a minorias étnicas. O caso de um indivíduo que foi erroneamente preso em 2020 devido a falhas na tecnologia, serve como um exemplo emblemático das ineficiências e preconceitos raciais que podem estar embutidos nesses sistemas. Este incidente não apenas ilustra as limitações técnicas, mas também levanta questões éticas sobre o uso dessas tecnologias por autoridades policiais, especialmente em um contexto onde a discriminação racial é uma preocupação premente.

Além disso, o artigo de Ardabili et al. (2023) destaca a importância de considerar a inclusão no paradigma das cidades inteligentes, sugerindo que a origem étnica e o contexto cultural desempenham papéis significativos nas percepções de segurança e inclusão. Essa perspectiva é fundamental para entender como diferentes grupos demográficos interagem com a tecnologia de vigilância e como suas experiências podem influenciar suas opiniões sobre a eficácia e a justiça dessas ferramentas. A pesquisa indica que a percepção da eficácia dos sistemas de vigilância por vídeo não é apenas uma questão técnica, mas está profundamente entrelaçada com questões

sociais e culturais.

Ardabili et al. (2023) também abordam a questão do viés algorítmico na polícia preditiva, que tende a afetar desproporcionalmente comunidades de cor. Isso sugere que as percepções sobre a justiça e a equidade na aplicação da lei são moldadas por experiências vividas e contextos sociais. A inclusão de vozes diversas na discussão sobre segurança pública e tecnologia é, portanto, essencial para garantir que as soluções propostas não perpetuem desigualdades existentes.

9

Resultados e Discussão

Para melhor compreender os caminhos percorridos nesta pesquisa, este capítulo apresenta as respostas às principais questões que orientaram a elaboração da metodologia. A partir delas, busca-se esclarecer as escolhas teóricas e práticas que fundamentaram o desenvolvimento do trabalho, detalhando os procedimentos adotados, os métodos de abordagem, as técnicas de coleta e análise de dados, bem como as justificativas para cada uma dessas decisões.

9.1 Resposta para as questões levantadas

9.1.1 Quais são os desafios da privacidade no reconhecimento facial em videomonitoramento?

O uso do reconhecimento facial traz preocupações significativas em relação à privacidade e à proteção de dados, uma vez que pode facilitar vazamentos de informações sensíveis e tornar os sistemas vulneráveis a ataques externos. Além disso, os métodos tradicionais de desidentificação, como o desfoque e a pixelização, têm se mostrado ineficazes diante de técnicas avançadas de reconstrução facial, que conseguem reverter essas alterações e identificar os indivíduos. Outro ponto crítico é o uso de dados faciais sem o devido consentimento, o que pode configurar uma violação direta dos direitos individuais e gerar sérias implicações legais e éticas (PARK; NA; CHOI, 2024).

9.1.2 Quais são os desafios legais para o uso do reconhecimento facial no Brasil?

No Brasil, a Lei Geral de Proteção de Dados (LGPD) impõe restrições ao uso de dados biométricos, exigindo justificativas claras e específicas para seu processamento. No entanto, a legislação não abrange diretamente o setor de segurança pública, o que gera lacunas jurídicas

sobre o uso do reconhecimento facial por parte do poder público. Além disso, questões como a transparência na utilização dos dados e o consentimento dos usuários ainda representam desafios significativos e não totalmente resolvidos na implementação dessa tecnologia no país (MORAES; ALMEIDA; PEREIRA, 2021).

9.1.3 Existe consenso entre pesquisadores sobre a regulação ou banimento da Tecnologia de Reconhecimento Facial?

Não há consenso. Enquanto alguns pesquisadores propõem um banimento total do reconhecimento facial, outros defendem uma regulação robusta com salvaguardas específicas. Todos, no entanto, concordam quanto ao alto potencial de violações de direitos humanos (DOKMANOVIĆ; CVETIĆANIN, 2023).

9.1.4 Quais estratégias têm sido adotadas para mitigar o viés racial no reconhecimento facial?

Algumas estratégias têm sido desenvolvidas com o objetivo de reduzir os vieses raciais nos sistemas de reconhecimento facial. Entre elas, destaca-se a utilização de conjuntos de dados mais diversos e equilibrados, como o "Diversity in Faces", da IBM, que visa representar melhor as diferentes características faciais da população. Além disso, avanços na melhoria dos algoritmos têm sido incorporados por meio de técnicas como a normalização de pontuação justa (Fair Score Normalization), que busca minimizar disparidades raciais nos resultados. Outra abordagem promissora é o treinamento baseado em perda assimétrica, como o método conhecido como "Asymmetric Rejection Loss", que tem como objetivo equilibrar o desempenho dos sistemas entre diferentes grupos raciais, promovendo maior equidade na identificação (WANG et al., 2019).

9.2 Outros resultados apresentados

O estudo evidencia as implicações do uso de sistemas de reconhecimento facial no contexto brasileiro, especialmente à luz das recentes aquisições governamentais e dos avanços em processamento de imagem. Autores, como Teixeira, Januzi e Faria (2022), destacam a crescente adoção de sistemas biométricos, que têm se tornado parte integrante de diversas atividades cotidianas, e a necessidade urgente de discutir as vulnerabilidades associadas a esses sistemas, particularmente no que tange à modalidade facial.

Foram levados em consideração os desafios e as medidas necessárias para garantir a proteção de dados pessoais no uso de sistemas de reconhecimento facial em espaços públicos e semi-públicos. Moraes, Almeida e Pereira (2021) revela a complexidade e a urgência do tema,

especialmente no contexto brasileiro, onde a implementação dessas tecnologias traz à tona questões éticas e legais significativas.

9.2.1 Privacidade no uso de tecnologias

A dissertação aponta a crescente controvérsia em torno do uso de tecnologias de reconhecimento facial, destacando tanto os benefícios quanto os riscos associados a esses sistemas (LESLIE, 2020).

Uma das principais questões discutidas é a confiança que os usuários potenciais precisam ter na tecnologia. A falta de confiança pode ser um obstáculo significativo para a adoção generalizada do reconhecimento facial, especialmente em um país como o Brasil, onde preocupações com a privacidade e a segurança dos dados são frequentemente levantadas (ARDABILI et al., 2022).

A implementação de sistemas de reconhecimento facial pode gerar desconfiança nas comunidades, levando a um sentimento de vigilância constante e à erosão da privacidade. A tensão entre segurança e direitos civis é uma questão complexa que merece consideração cuidadosa, especialmente em um país como o Brasil, onde a história de vigilância estatal e repressão é significativa (LESLIE, 2020).

9.2.2 Desigualdades Sociais

A proliferação de tecnologias de reconhecimento facial pode exacerbar desigualdades sociais existentes, uma vez que esses sistemas frequentemente apresentam vieses que afetam desproporcionalmente minorias étnicas e raciais.

A falta de representatividade nos conjuntos de dados utilizados para treinar esses algoritmos pode levar a taxas de erro mais altas, resultando em identificação incorreta e, consequentemente, em consequências legais e sociais negativas para os indivíduos afetados. Esse ponto é determinante, especialmente no contexto brasileiro, onde questões de desigualdade racial e social são proeminentes (LESLIE, 2020).

A dissertação aponta que os algoritmos de reconhecimento facial não são isentos de viés, e que a eficácia desses sistemas pode variar significativamente de acordo com a raça e gênero dos indivíduos. Esse viés pode levar a uma identificação incorreta, resultando em discriminação e injustiças, especialmente em comunidades marginalizadas (LESLIE, 2020).

9.2.3 Proposições de mitigação

A utilização do reconhecimento facial exige a adoção de salvaguardas eficazes para proteger os dados pessoais coletados durante o trânsito de indivíduos. Entre as medidas propostas, são mencionados mecanismos de *soft law*, que consistem na publicação de diretrizes e

recomendações de efeito não vinculativo. Essa abordagem é particularmente relevante em um cenário onde a legislação formal pode ser insuficiente para lidar com as nuances das tecnologias em rápida evolução (MORAES; ALMEIDA; PEREIRA, 2021).

A discussão sobre a eficácia das medidas propostas é um ponto que merece mais atenção. Embora os autores, como Moraes, Almeida e Pereira (2021), reconheçam a importância de uma abordagem regulatória abrangente, a aplicação prática dessas diretrizes em um país como o Brasil, com suas particularidades sociais e econômicas, pode ser desafiadora. A falta de uma estrutura regulatória robusta e a resistência de setores da sociedade em aceitar a vigilância em massa podem dificultar a implementação das recomendações.

Embora alguns autores discutam que a implementação de tecnologias de reconhecimento facial nos Estados Unidos e na Europa está imersa em um debate que gira em torno da proibição ou restrições severas ao seu uso em espaços públicos (SOLAROVA et al., 2023). Essa discussão é particularmente relevante para o Brasil, onde a regulamentação desse tipo de tecnologia ainda é incipiente.

O estudo elenca ainda, a necessidade de requisitos adicionais de cibersegurança para bancos de dados centralizados, o que é essencial para proteger as informações pessoais dos cidadãos. Essa perspectiva é crítica, dado o aumento das preocupações com a segurança cibernética e a proteção de dados no Brasil (RAMOS, 2023).

Apesar dos benefícios potenciais do reconhecimento facial, como a melhoria na segurança pública e a eficiência em processos administrativos, existem riscos significativos que não podem ser ignorados. Entre essas preocupações estão a possibilidade de violações de privacidade, discriminação algorítmica e a falta de transparência nos sistemas utilizados. A análise crítica apresentada no trabalho de Teixeira, Januzi e Faria (2022) sugere que a implementação de tais sistemas deve ser acompanhada de regulamentações rigorosas e de um debate público abrangente sobre as implicações éticas e sociais.

A discussão sobre a segurança dos dados e a privacidade é especialmente relevante em um país como o Brasil, onde as desigualdades sociais podem ser exacerbadas pelo uso inadequado dessas tecnologias. é Preciso pensar na criação de legislações amplas e genéricas, destinadas à proteção de dados pessoais, pode levar à proibição ou a requisitos rigorosos para o uso de determinadas tecnologias biométricas, como o reconhecimento facial (RAMOS, 2023).

10
Considerações Finais

Esta dissertação trouxe à tona que o uso do reconhecimento facial em sistemas de vigilância por vídeo no Brasil, embora tenha o potencial de melhorar a segurança pública e a eficácia operacional, está repleto de desafios complexos que vão além da implementação tecnológica.

A aplicação dessa tecnologia efetivamente nos estados da Bahia, São Paulo, Rio de Janeiro, Sergipe e Roraima prova que, apesar de seu uso em diferentes tipos de iniciativas, muitos desafios devem ser superados para torná-la uma ferramenta ética, segura e eficaz. Alguns dos desafios mais evidentes apontados referem-se às questões éticas e sociais que se relacionariam à privacidade dos cidadãos e à possibilidade de discriminação algorítmica, porque a precisão dos sistemas é diferente entre os vários perfis demográficos e, por sua vez, pode reforçar as desigualdades sociais e estigmatizações.

Limitações de infraestrutura também fornecem um obstáculo na utilização eficaz e confiável da tecnologia em todo o país, principalmente em regiões menos desenvolvidas do Brasil. Outro ponto que carece de atenção se encontra na forma como é conduzida a regulamentação para o uso do reconhecimento facial no país. A ausência de tal arcabouço legal implica incertezas sobre o uso correto da mesma tecnologia, o que pode sujeitar os cidadãos locais a riscos relacionados à violação de seus direitos básicos.

10.1 Recomendações Futuras

A legislação brasileira, ainda em gestação, será obrigada a conter preceitos fortes na busca por esse equilíbrio entre o uso da tecnologia e a proteção dos direitos individuais com foco em transparência, responsabilização e controle sobre o uso de dados biométricos. Isso pode levar a grandes resultados em algumas circunstâncias, principalmente ligadas à segurança pública, incluindo a identificação e prisão de criminosos e maior segurança no controle de acesso em

grandes eventos.

Nesses casos, esse mesmo fato também percebe as melhorias técnicas ainda necessárias para, por exemplo, a redução de falsos positivos ou o aumento da imparcialidade dos algoritmos de reconhecimento facial em geral. O futuro da tecnologia de reconhecimento facial no Brasil dependerá se esses desafios podem ser coordenados de forma a servir os interesses do poder público, do setor empresarial, da academia e da sociedade civil como um todo. Para esse efeito, a inteligência artificial e novos algoritmos que tendem a ser mais inclusivos e precisos contribuirão para corrigir algumas das falhas, entre elas o viés algorítmico.

Todas essas melhorias devem ser feitas somente em paralelo com a discussão geral na sociedade sobre os limites éticos e legais do uso de tecnologias. Essa é a única maneira pela qual tais resultados podem ser obtidos no melhor interesse de cada parte sem quebrar os direitos individuais dos cidadãos brasileiros.

10.2 Limitações do trabalho

Esta dissertação apresenta algumas limitações que merecem ser consideradas, como a limitação de um recorte temático, uma vez que a pesquisa abordou apenas alguns aspectos específicos do tema, deixando de lado outras dimensões igualmente relevantes que poderiam enriquecer a análise.

Da mesma forma, enfrentou-se uma limitação de acesso a dados, devido à escassez de informações atualizadas, à restrição no acesso a dados oficiais e à falta de transparência por parte de alguns órgãos públicos, o que dificultou uma investigação mais aprofundada.

Enfim, é importante destacar que os resultados e conclusões aqui apresentados estão diretamente relacionados ao contexto estudado e, portanto, não podem ser generalizados automaticamente para outras realidades, regiões ou países.

Referências

AIRES, M. A. P.; GREGORI, I. C. S. D. As implicações dos direitos fundamentais na era das novas tecnologias: o direito ao esquecimento como mecanismo apto a tutelar o direito à privacidade. *Revista Brasileira de Direitos e Garantias Fundamentais*, v. 3, n. 2, p. 106–127, 2017. Citado 2 vezes nas páginas 63 e 64.

ALMEIDA, D.; SHMARKO, K.; LOMAS, E. The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of us, eu, and uk regulatory frameworks. *AI and Ethics*, Springer, v. 2, n. 3, p. 377–387, 2022. Citado 3 vezes nas páginas 43, 46 e 47.

ALMEIDA, E. C. Os grandes irmãos: o uso de tecnologias de reconhecimento facial para persecução penal. *Revista Brasileira de Segurança Pública*, v. 16, n. 2, p. 264–283, 2022. Citado na página 17.

ANDRADE, C. M.; JABORANDY, C. C. M. Algoritmos raciais e a sua ocorrência no reconhecimento facial na segurança pública como entrave aos direitos humanos. *PESQUISAS E INOVAÇÕES EM CIÊNCIAS HUMANAS E SOCIAIS: PRODUÇÕES CIENTÍFICAS MULTIDISCIPLINARES NO SÉCULO XXI, VOL 2*, p. 181, 2022. Citado 2 vezes nas páginas 27 e 40.

ANDRÉA, G. F. M.; SILVA, D. C. da; GUNDIM, W. W. D. Tecnologia de reconhecimento facial como política de segurança pública: O caso do metrô de são paulo. *Revista da Faculdade de Direito do Sul de Minas*, v. 38, n. 2, p. 279–298, 2022. Citado na página 35.

ANJOS, R. E. S. D.; FILHO, R. A. F.; SOUSA, J. M. D. A (im) parcialidade dos algoritmos em decisões automatizadas nos processos de reconhecimento facial de pessoas. *LexLab–Revista Eletrônica de Direito*, v. 1, n. 2, p. 66–76, 2024. Citado na página 25.

ANTONIO, I. C. S. Direito à privacidade em risco?: reflexões sobre o avanço das tecnologias de reconhecimento facial pela segurança pública no brasil. *Trabalho de Conclusão de Curso (Bacharelado em Direito)-Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro*, 2022. Citado na página 16.

ARAÚJO, R. de A.; CARDOSO, N. D.; PAULA, A. M. de. Regulação e uso do reconhecimento facial na segurança pública do brasil. *Revista de Doutrina Jurídica*, v. 112, p. e021009–e021009, 2021. Citado na página 14.

ARDABILI, B. R. et al. Understanding ethics, privacy, and regulations in smart video surveillance for public safety. *arXiv preprint arXiv:2212.12936*, 2022. Citado 3 vezes nas páginas 50, 52 e 72.

ARDABILI, B. R. et al. Exploring public's perception of safety and video surveillance. *Ghazal and Katariya, Vinit and Hull, Gordon and Reid, Shannon and Tabkhi, Hamed, Exploring Public's Perception of Safety and Video Surveillance*, 2023. Citado 3 vezes nas páginas 66, 68 e 69.

BACCARIN, C. Limitações aos sistemas de reconhecimento facial no setor privado: boas práticas em proteção de dados biométricos faciais. Universidade Estadual Paulista (Unesp), 2023. Citado na página 33.

BADA, M. M.; OLIVEIRA, M. Inteligência artificial na segurança pública: o uso do reconhecimento facial para identificação de infratores. 2024. Citado 4 vezes nas páginas 13, 25, 28 e 36.

BENTO, E. F. *Qual a expectativa do uso de reconhecimento facial pela Guarda Civil Municipal de Vitória/ES? um estudo de caso sobre os riscos do racismo e do sexismo algorítmico*. Tese (Doutorado) — brasil, 2024. Citado na página 41.

BRITO, P. M. F. C. de. *Facial analysis with depth maps and deep learning*. Tese (Doutorado) — Universidade Aberta (Portugal), 2018. Citado 3 vezes nas páginas 55, 58 e 59.

BRIZOLA, J.; FANTIN, N. Revisão da literatura e revisão sistemática da literatura. *Revista de Educação do Vale do Arinos-RELVA*, v. 3, n. 2, 2016. Citado na página 21.

BUOLAMWINI, J.; GEBRU, T. Gender shades: Intersectional accuracy disparities in commercial gender classification. In: PMLR. *Conference on fairness, accountability and transparency*. [S.l.], 2018. p. 77–91. Citado na página 26.

BURKHARDT, B.; BORRADAILE, G.; GELVIN, B. Racial equity in police use of social media monitoring software. SocArXiv, 2023. Citado 3 vezes nas páginas 66, 67 e 68.

CABRAL, G. A. et al. Ferramenta de reconhecimento facial para auxiliar na busca de pessoas consideradas desaparecidas. *Revista Científica da UNIFENAS-ISSN: 2596-3481*, v. 6, n. 5, 2024. Citado na página 35.

CAMÊLO, M. N. G-priv: um guia para especificação de requisitos de privacidade em conformidade com a lgpd. 2022. Citado na página 17.

CAMPOS, V. A. V. A.; FRANÇA, A. L. A. L.; ROCHA, K. P. Automação residencial aplicada para idosos e portadores de necessidades especiais. 2019. Citado na página 37.

CANI, L. E.; NUNES, J. A. Erros judiciários em tempos de digital surveillance: os algoritmos de reconhecimento facial em questão. *Revista Brasileira de Direito Processual Penal*, SciELO Brasil, v. 8, p. 679–712, 2022. Citado na página 25.

CARVALHO, L. L. d. O racismo estrutural no âmbito do reconhecimento facial como meio de prova. Citado na página 30.

CHIARELLO, P. da L.; CERVI, J. R.; NOSCHANG, P. Inteligência artificial e migrações:: Um estudo sobre a liberdade de circulação de pessoas e o uso de reconhecimento facial para o controle migratório no âmbito da união europeia. *Revista Digital Constituição e Garantia de Direitos*, v. 16, n. 2, 2023. Citado na página 17.

CHUA, Y. T. et al. Identifying unintended harms of cybersecurity countermeasures. In: IEEE. *2019 APWG Symposium on Electronic Crime Research (eCrime)*. [S.l.], 2019. p. 1–15. Citado na página 61.

COIMBRA, J. P. M. et al. Interseções entre racismo algorítmico, reconhecimento facial e segurança pública no brasil. *Revista Jurídica do Cesupa*, v. 4, n. 2, p. 136–160, 2023. Citado na página 28.

COSTA, R. S.; KREMER, B. Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial. *Revista Brasileira de Direitos Fundamentais & Justiça*, v. 16, n. 1, 2022. Citado 5 vezes nas páginas 13, 17, 27, 28 e 41.

COSTA, R. S.; OLIVEIRA, S. R. d. O uso de tecnologias de reconhecimento facial em sistemas de vigilância e suas implicações no direito à privacidade. *Revista de Direito, Governança e Novas Tecnologias*, v. 5, n. 2, p. 01–2, 2019. Citado na página 19.

CRIPPA, M. E. N. et al. Uso do reconhecimento facial aplicado à segurança pública no brasil. 2021. Citado na página 19.

DEALCALA, D. et al. Measuring bias in ai models: an statistical approach introducing n-sigma. In: IEEE. *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*. [S.l.], 2023. p. 1167–1172. Citado 3 vezes nas páginas 43, 48 e 49.

DOKMANOVIĆ, M.; CVETIĆANIN, N. Regulation of the use of facial recognition technology–limitations and challenges from a human rights perspective. *Teorija in praksa*, University of Ljubljana, Faculty of Social Sciences, n. 3, p. 548–564, 2023. Citado na página 71.

DROZDOWSKI, P. et al. Demographic bias in biometrics: A survey on an emerging challenge. *IEEE Transactions on Technology and Society*, IEEE, v. 1, n. 2, p. 89–103, 2020. Citado 2 vezes nas páginas 42 e 44.

DUARTE, M. G. et al. Contagem e identificação de pessoas em sala de aula através de visão computacional e internet das coisas. 2024. Citado na página 16.

DUARTE, R. et al. Aplicação dos sistemas biométricos de reconhecimento facial na segurança pública. *Brazilian Journal of Forensic Sciences, Medical Law and Bioethics*, v. 11, n. 1, p. 1–21, 2021. Citado na página 29.

FAGUNDES, B. D. A.; FERNANDES, P. W. T. Os "novos olhos" da segurança pública da bahia:: Rúidos de uma necropolítica nos programas de reconhecimento facial. *Revista Eletrônica Direito & TI*, v. 1, n. 18, p. 39–58, 2024. Citado na página 37.

FARIA, R. B. de; MOTA, R. G. da et al. Breves considerações acerca da utilização do reconhecimento facial como instrumento de segurança pública e persecução. *Boletim IBCCRIM*, v. 31, n. 362, p. 14–17, 2023. Citado na página 29.

FAVERI, E. M. Estudo da eficácia dos algoritmos de reconhecimento facial. Universidade Estadual Paulista (Unesp), 2023. Citado na página 29.

FREITAS, R. T. et al. Uma abordagem multi-nível baseada em redes neurais convolucionais para redução do viés algorítmico na localização de pontos faciais. Universidade Federal do Maranhão, 2023. Citado na página 40.

GARCIA, K. P. et al. A (in) constitucionalidade do uso do reconhecimento facial em espaços públicos e privados diante dos direitos da personalidade. Faculdade de Direito de Vitoria, 2023. Citado na página 19.

GENTZEL, M. Biased face recognition technology used by government: A problem for liberal democracy. *Philosophy & Technology*, Springer, v. 34, n. 4, p. 1639–1663, 2021. Citado 3 vezes nas páginas 65, 66 e 67.

GOMES, E.; ANATEL, A. d. P. da. Exclusão digital: um problema tecnológico ou social. *Instituto de Estudos do Trabalho e Sociedade, Rio de Janeiro: Trabalho e Sociedade, ano*, v. 2, 2002. Citado na página 28.

GOMES, N. L. d. S. A segurança e a defesa cibernética no brasil: análise dos discursos das forças armadas brasileiras (2016-2021). Escola Superior de Guerra, 2024. Citado na página 16.

HANDELMAN, T. A. Comparing the legal implications of ai-powered facial recognition technology in the usa, the eu, and china: Safeguarding privacy, bias, and civil liberties. *J. Int'l L. & Comp. Stud.*, HeinOnline, v. 1, p. 63, 2023. Citado na página 18.

HOOBERMAN, L. The coded gaze: algorithmic bias, facial recognition and beyond: How research can change the law and influence people. In: *Proceedings of the 13th ACM Web Science Conference 2021*. [S.l.: s.n.], 2021. p. 7–8. Citado na página 18.

JOSÉ, J.; JÚNIOR, S. Redes neurais profundas para reconhecimento facial no contexto de segurança pública. Citado na página 27.

JUNIOR, M. A. d. S. *Utilização eficiente em larga escala de reconhecimento facial para análise preditiva de segurança em cidades inteligentes.* Tese (Doutorado) — Universidade de São Paulo, 2019. Citado na página 35.

JÚNIOR, R. N. C. C. et al. Revisão integrativa, sistemática e narrativa-aspectos importantes na elaboração de uma revisão de literatura. *Revista ACB: Biblioteconomia em Santa Catarina*, Associação Catarinense de Bibliotecários, v. 28, n. 1, p. 11, 2023. Citado na página 22.

JÚNIOR, T. T. B. As cidades inteligentes e a inteligência artificial. *CIDADES INTELIGENTES*, p. 355. Citado na página 28.

JUNIOR[1], A. P.; TEIXEIRA, F. O.; HOMEM, T. P. D. 11º congresso de inovação, ciência e tecnologia do ifsp-2020 aplicação de visão computacional para o monitoramento do uso de máscaras de proteção. Citado na página 36.

KUBOTA, L. C.; ROSA, M. B. Inteligência artificial no brasil: Adoção, produção científica e regulamentação. digitalização e tecnologias da informação e comunicação. *Digitalização e tecnologias da informação e comunicação: oportunidades e desafios para o Brasil. Rio de Janeiro: Ipea*, 2024. Citado na página 41.

KUM, L. C.; MENDES, P. A. C. A importância da criptografia para proteção de dados pessoais. 121, 2024. Citado na página 19.

LARSSON, S. The socio-legal relevance of artificial intelligence. *Droit et société*, Cairn/Cairn, v. 103, n. 3, p. 573–593, 2019. Citado 3 vezes nas páginas 42, 43 e 44.

LEAVY, S.; O'SULLIVAN, B.; SIAPERA, E. Data, power and bias in artificial intelligence. *arXiv preprint arXiv:2008.07341*, 2020. Citado 2 vezes nas páginas 42 e 45.

LESLIE, D. Understanding bias in facial recognition technologies. *arXiv preprint arXiv:2010.07023*, 2020. Citado 4 vezes nas páginas 49, 50, 51 e 72.

LIMA, B. D. F. Racismo algorítmico: o enviesamento tecnológico e o impacto aos direitos fundamentais no brasil. Pós-Graduação em Direito, 2022. Citado na página 13.

LIMA, D. d. S. Relação entre o reconhecimento facial e a sua responsabilidade jurídica: a luz dos direitos humanos essa tecnologia pode vir a enlear a dignidade humana?. Universidade Federal de Campina Grande, 2023. Citado 3 vezes nas páginas 31, 32 e 33.

LIMA, L. B. D. *DETECÇÃO DE ANOMALIAS EM TEMPO DE RESPOSTA DE SERVIDORES WEB: UMA ABORDAGEM AUTOMATIZADA PARA APRIMORAR A SEGURANÇA E A EFICIÊNCIA*. Tese (Doutorado) — Dissertação de Engenharia Elétrica e de Computação 2023. Tese de Doutorado . . . , 2023. Citado na página 16.

LIMA, P. H. R. Uma abordagem baseada em redes neurais para reconhecimento facial aplicado ao tribunal regional eleitoral do amapá. UNIFAP–Universidade Federal do Amapá, 2021. Citado na página 29.

LOPES, R. V. de M.; KOCH, W. Do reconhecimento facial a partir da inteligência artificial: A possibilidade de sua utilização como prova no processo penal brasileiro1. Citado na página 39.

LORENZON, L. N. Análise comparada entre regulamentações de dados pessoais no brasil e na união europeia (lgpd e gdpr) e seus respectivos instrumentos de enforcement. *Revista do Programa de Direito da União Europeia*, v. 1, p. 39–52, 2021. Citado na página 17.

LOUREIRO, M. F. B.; CARNEIRO, J. V. V. Problematizando o direito à privacidade e à proteção de dados pes-soais em face da vigilância biométrica. *Teknokultura: Revista de Cultura Digital y Movimientos Sociales*, Grupo de Investigación Cibersomosaguas, v. 17, n. 2, p. 204–213, 2020. Citado 4 vezes nas páginas 55, 59, 63 e 65.

MACHADO, T. J. X. A cibersegurança para adolescentes: uma proposta para a sua comunicação. 2023. Citado na página 17.

MAGRO, D. D.; FORTES, V. B. O reconhecimento facial nas smart cities e a garantia dos direitos à privacidade e à proteção de dados pessoais. *Revista de Direito Internacional*, v. 18, n. 2, 2021. Citado 2 vezes nas páginas 18 e 19.

MANUEL, L. do V. et al. Identificação e rastreamento de pessoas por meio de imagens digitais capturadas a partir de câmeras de video. In: *Colloquium Exactarum. ISSN: 2178-8332*. [S.l.: s.n.], 2016. v. 8, n. 1, p. 22–34. Citado 2 vezes nas páginas 54 e 57.

MARCONDES, J. Biometria, sistema biométrico: O que é, como funciona. *link]. Acesso em*, v. 18, 2023. Citado 2 vezes nas páginas 55 e 57.

MARIN, L. de O. Métodos estatísticos no reconhecimento de faces. *Revista Eletrônica de Sistemas de Informação*, v. 5, n. 2, 2006. Citado 3 vezes nas páginas 54, 55 e 56.

MELO, P. V.; SERRA, P. Tecnologia de reconhecimento facial e segurança pública nas capitais brasileiras: apontamentos e problematizações. *Comunicação e sociedade*, Centro de estudos de comunicação e sociedade, n. 42, p. 205–220, 2022. Citado na página 16.

MELO, S. R. de. *E quando o suspeito for você?: Reconhecimento facial na segurança pública*. [S.l.]: Editora Dialética, 2024. Citado 2 vezes nas páginas 32 e 33.

MENEZES, G. W. A ação do uso da inteligência artificial e microfeições faciais para mitigar os riscos de deeofakes para a autenticação por biometria facial no setor financeiro brasileiro. Escola Superior de Guerra, 2024. Citado na página 40.

MONTEIRO, G. O. Instrumentos de reconhecimento facial e os contornos da lei geral de proteção de dados ante a privacidade nas cidades (in) inteligentes. *Revista de Direito e Atualidades*, n. 1, 2021. Citado 3 vezes nas páginas 18, 28 e 41.

MORAES, T. G.; ALMEIDA, E. C.; PEREIRA, J. R. L. de. Smile, you are being identified! risks and measures for the use of facial recognition in (semi-) public spaces. *AI and Ethics*, Springer, v. 1, n. 2, p. 159–172, 2021. Citado 5 vezes nas páginas 42, 45, 46, 71 e 73.

MOREIRA, A. F. S.; SALES, A. C.; MOREIRA, C. S. Aspectos da privacidade na sociedade de vigilância: proteção de dados e sistemas de videomonitoramento. *Revista da EMERJ*, v. 26, p. 1–23, 2024. Citado na página 13.

MOREIRA, J. R.; RIBEIRO, J. B. P. Letramento e competência informacional e as relações éticas na gestão da informação e do conhecimento no contexto da inteligência artificial. *Brazilian Journal of Information Science*, Universidade Estadual Paulista, n. 17, p. 46, 2023. Citado na página 40.

MOURA, E. S. et al. Agrupamento de faces em vídeos digitais. Universidade Federal de Campina Grande, 2016. Citado 2 vezes nas páginas 55 e 58.

MULHOLLAND, C. *A LGPD e o novo marco normativo no Brasil*. [S.l.]: Arquipélago Editorial, 2020. v. 6. Citado na página 17.

NEGRI, P.; HUPONT, I.; GOMEZ, E. A framework for assessing proportionate intervention with face recognition systems in real-life scenarios. *arXiv preprint arXiv:2402.05731*, 2024. Citado 3 vezes nas páginas 50, 53 e 54.

NOBRE, D. K. Direito comparado e inteligência artificial: a responsabilização civil do reconhecimento facial na lgpd. *Revista Avant-ISSN 2526-9879*, v. 4, n. 2, 2020. Citado na página 39.

NOIRET, S.; LUMETZBERGER, J.; KAMPEL, M. Bias and fairness in computer vision applications of the criminal justice system. In: IEEE. *2021 IEEE Symposium Series on Computational Intelligence (SSCI)*. [S.l.], 2021. p. 1–8. Citado 3 vezes nas páginas 43, 47 e 48.

OLIVEIRA, B. B. de; MALDONADO, G. S. A necessária regulação do reconhecimento facial no brasil diante dos riscos à intimidade e à privacidade. 2022. Citado na página 19.

OLIVEIRA, B. de. *Mulheres negras sofrem mais erros em abordagens de reconhecimento facial do que brancos*. 2024. Accessed on January 2, 2025. Disponível em: <https://expresso.estadao.com.br/naperifa/mulheres-negras-sofrem-mais-erros-em-abordagens-de-reconhecimento-facial-do-que-brancos/>. Citado na página 26.

OLIVEIRA, B. V. N. de; MELO, F. T. de. Fundamentos da visão computacional: Arcabouço teórico do reconhecimento artificial de imagens e vídeos. *Humanidades & Inovação*, v. 10, n. 17, p. 312–327, 2023. Citado na página 16.

OLIVEIRA, L. V. et al. Aspectos ético-jurídicos e tecnológicos do emprego de reconhecimento facial na segurança pública no brasil. *Revista Tecnologia e Sociedade*, v. 18, n. 50, p. 114–135, 2022. Citado 3 vezes nas páginas 38, 39 e 41.

OLIVEIRA, S. R. D. Sorria, você está sendo filmado: tecnologias de reconhecimento facial, privacidade e proteção de dados. Universidade Federal de Juiz de Fora, 2020. Citado 2 vezes nas páginas 19 e 26.

OLIVEIRA, V. W. C. d. Conformidade do metaverso da empresa meta com a lgpd: análise das práticas de coleta, tratamento e proteção de dados. 2024. Citado na página 17.

PACHECO, R. L. Estratégias integradas de segurança com inteligência artificial em eventos esportivos de grande porte: lições das olimpíadas e da copa do mundo. *Brazilian Journal of Development*, v. 11, n. 1, p. e76732–e76732, 2025. Citado na página 13.

PARK, S.; NA, H.; CHOI, D. Verifiable facial de-identification in video surveillance. *IEEE Access*, IEEE, 2024. Citado na página 70.

PEREIRA, D. F. M. O uso de câmeras de reconhecimento facial em contexto de pós democracia–uma ferramenta contra o inimigo no direito penal. *https://bit. ly/3gXu51f]. Acesso em*, v. 28, p. 12, 2022. Citado na página 35.

QUEIROLO, C. C.; SILVA, L.; BELLON, O. R. Reconhecimento facial 3d usando simulated annealing e a medida de interpenetraçao de superficies. 2009. Citado 2 vezes nas páginas 54 e 56.

RAMOS, L. F. M. Biometric technologies and the law: Developing a taxonomy for guiding policymakers. *arXiv preprint arXiv:2312.00013*, 2023. Citado 3 vezes nas páginas 50, 53 e 73.

REIS, A. *Sociedade. com: como as tecnologias digitais afetam quem somos e como vivemos*. [S.l.]: Arquipélago editorial, 2018. Citado na página 37.

RESENDE, C. A. de P.; PEREIRA, M. H. R. Visão computacional aplicada em reconhecimento facial na busca por pessoas desaparecidas. *e-xacta*, v. 8, n. 2, p. 95–107, 2015. Citado na página 35.

RIBEIRO, L. G. T. Sistema de presença por reconhecimento facial. Universidade Federal do Rio de Janeiro, 2022. Citado na página 28.

RODRIGUES, E. C. Reconhecimento facial na vigilância pública. 2023. Citado na página 35.

ROSSI, E. *Reconhecimento facial erra mais rosto feminino*. 2019. Accessed on January 02, 2025. Disponível em: <https://istoedinheiro.com.br/reconhecimento-facial-erra-mais-rosto-feminino/>. Citado na página 26.

SANNON, S.; FORTE, A. Privacy research with marginalized groups: what we know, what's needed, and what's next. *Proceedings of the ACM on Human-Computer Interaction*, ACM New York, NY, USA, v. 6, n. CSCW2, p. 1–33, 2022. Citado 2 vezes nas páginas 66 e 67.

SANTAELLA, L. *A inteligência artificial é inteligente?* [S.l.]: Almedina Brasil, 2023. Citado na página 25.

SANTOS, É. L. d. et al. Cidades inteligentes e sustentáveis: percepções sobre a cidade de curitiba/pr a partir dos planos plurianuais de 2014 a 2021. *urbe. Revista Brasileira de Gestão Urbana*, SciELO Brasil, v. 14, p. e20210299, 2022. Citado na página 35.

SANTOS, G. A. d. S. Face recognition: o rosto da insatisfação contra vigilante. 2018. Citado 3 vezes nas páginas 63, 64 e 65.

SANTOS, J. G. Reconhecimento facial entre a criminologia, a mídia e a lgpd penal. *Internet & Sociedade*, v. 2, n. 1, p. 219, 2021. Citado na página 36.

SANTOS, L. R. dos; PRADO, V. J. do; RODRIGUEZ, V. B. C. Os reflexos de uma abolição mal-acabada no brasil: Da coroa ao algoritmo. *Revista de Direito, Governança e Novas Tecnologias*, v. 9, n. 1, p. 74–91, 2023. Citado na página 39.

SARABDEEN, J. Protection of the rights of the individual when using facial recognition technology. *Heliyon*, Elsevier, v. 8, n. 3, 2022. Citado 2 vezes nas páginas 60 e 62.

SCOPEL, B. G.; PUHL, E. A tecnologia de reconhecimento facial e sua utilização como prova no processo penal. *Academia de Direito*, v. 6, p. 3678–3700, 2024. Citado 3 vezes nas páginas 13, 36 e 37.

SILVA, B. de L.; LIMEIRA, M. L. da C. As novas tecnologias e a segurança pública: um casamento complexo e promissor. *Pro Lege Vigilanda*, v. 2, n. 2, 2023. Citado na página 13.

SILVA, G. B. A. d. Aplicabilidade das tecnologias disruptivas de reconhecimento facial em sistemas de vigilância pública no brasil: implicações da efetividade do direito constitucional à privacidade. Pontifícia Universidade Católica de Goiás, 2022. Citado 3 vezes nas páginas 20, 31 e 38.

SILVA, K. P. d. Análise de aplicação de visão computacional e redes neurais, em conjunto com o uso de técnicas de aumento de dados, na tradução automática de libras. 2023. Citado na página 40.

SILVA, M.; OLIVEIRA, D. Brazilian favela women: How your standard solutions for technology abuse might actually harm them. *arXiv preprint arXiv:2101.09257*, 2021. Citado 2 vezes nas páginas 60 e 61.

SILVA, M. L. S. *As tecnologias de reconhecimento facial para Segurança Pública no Brasil: perspectivas regulatórias e a garantia de Direitos Fundamentais*. Dissertação (B.S. thesis) — Universidade Federal do Rio Grande do Norte, 2022. Citado na página 40.

SILVA, M. T. D. d. Vieses em algoritmos de reconhecimento facial: um mapeamento sistemático da literatura. Universidade Federal de Campina Grande, 2024. Citado na página 27.

SILVA, P. H. M. d. Desenvolvimento tecnológico da segurança pública do ceará por meio da inteligência artificial:"olhos"e"cérebros"operando a vigilância de arrasto. 2023. Citado na página 35.

SILVA, R. L. d.; SILVA, F. d. S. R. d. Reconhecimento facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro. In: *Congresso Internacional de Direito e Contemporaneidade, Santa Maria, RS, Brasil*. [S.l.: s.n.], 2019. v. 5. Citado na página 26.

SOLAROVA, S. et al. Reconsidering the regulation of facial recognition in public spaces. *AI and Ethics*, Springer, v. 3, n. 2, p. 625–635, 2023. Citado 6 vezes nas páginas 43, 47, 49, 51, 52 e 73.

SOUZA, C. V. d. et al. Compliance digital: privacidade e proteção de dados à luz da lei geral de proteção de dados (lgpd) e os desafios de implementação. Universidade Federal de Uberlândia, 2022. Citado 2 vezes nas páginas 17 e 18.

SOUZA, D. C.; FERREIRA, V. H.; NETO, C. A. Aplicação de redes neurais artificiais para estimação de indicadores de segurança estática e dinâmica de sistemas elétricos de potência. *Simpósio Brasileiro de Sistemas Elétricos-SBSE*, v. 2, n. 1, 2022. Citado na página 39.

STEFFEN, C. A inteligência artificial e o processo penal: a utilização da técnica na violação de direitos. *Revista da EMERJ*, v. 25, n. 1, p. 105–129, 2023. Citado na página 32.

TEIXEIRA, R. F. d. S.; JANUZI, R. B.; FARIA, F. A. The brazilian data at risk in the age of ai? *arXiv preprint arXiv:2205.01772*, 2022. Citado 10 vezes nas páginas 49, 51, 55, 59, 60, 61, 62, 63, 71 e 73.

TERRA, A. L. d. A. Reconhecimento facial e surveillance: desafios à proteção de direitos fundamentais ante à coleta indiscriminada de dados pessoais biométricos. *Trabalho de Conclusão de Curso (Bacharelado em Direito)-Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro*, 2021. Citado na página 36.

VALMORBIDA, W.; ETGETON, K. F. Controle de dispositivos em casas inteligentes por meio do reconhecimento de gestos e biometria facial com uso de deep learning. *Revista Destaques Acadêmicos*, v. 12, n. 4, 2020. Citado na página 29.

VANZ, S. A. d. S. et al. Gestão de dados de pesquisa: questões éticas e legais. UFRGS, 2023. Citado na página 17.

VARGAS, É. N. P. O uso da tecnologia de reconhecimento facial como política de segurança pública no estado da bahia. Universidade Salvador, 2022. Citado na página 32.

VECCI, A. F. A. Estudo da capacidade humana de reconhecimento facial: revisão de literatura. Universidade Federal de Uberlândia, 2023. Citado na página 29.

VERISSIMO, G. H. G.; NOVAIS, T. G. O (im) procedimento no reconhecimento pessoal como fator primordial de prisões indevidas. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, v. 10, n. 5, p. 5313–5333, 2024. Citado na página 14.

VIEIRA, F. da S. et al. Aplicabilidade da inteligência artificial nas polícias militares brasileiras: Vantagens, desvantagens e/ou limitações. In: *Anais do Congresso Internacional de Conhecimento e Inovação–ciki*. [S.l.: s.n.], 2024. Citado na página 31.

WALLACE, B. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. 2019. Citado na página 19.

WANG, M. et al. Racial faces in the wild: Reducing racial bias by information maximization adaptation network. In: *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV)*. [S.l.: s.n.], 2019. Citado 3 vezes nas páginas 7, 27 e 71.

ZENG, J.; QIU, X.; SHI, S. Image processing effects on the deep face recognition system. *Math. Biosci. Eng*, v. 18, n. 2, p. 1187–1200, 2021. Citado 2 vezes nas páginas 25 e 29.

ZOGAHIB, A. L. N. et al. *Segurança Pública, Cidadania e Direitos Humanos: pesquisas, relatos e reflexões–Vol. 9*. [S.l.]: AYA Editora, 2024. Citado na página 39.