



Universidade de Brasília

Faculdade UnB Planaltina – FUP

Programa de Pós-Graduação em Gestão Pública - PPGP

Simone Pereira Duarte Ferreira

**USO DE TECNOLOGIAS DE RECONHECIMENTO FACIAL PELA
SEGURANÇA PÚBLICA NO DISTRITO FEDERAL: IMPLICAÇÕES
ÉTICAS, LEGAIS E NA PROTEÇÃO DE DADOS DOS CIDADÃOS**

Brasília-DF

2025

Simone Pereira Duarte Ferreira

**USO DE TECNOLOGIAS DE RECONHECIMENTO FACIAL PELA
SEGURANÇA PÚBLICA NO DISTRITO FEDERAL: IMPLICAÇÕES
ÉTICAS, LEGAIS E NA PROTEÇÃO DE DADOS DOS CIDADÃOS.**

Dissertação defendida junto ao Programa de Pós-Graduação em Gestão Pública – PPGP/FUP, da Universidade de Brasília - UnB, Campus Planaltina, como requisito obrigatório para obtenção do título de Mestre em Gestão Pública, orientada pelo professor Dr. Luiz Honorato da Silva Junior.

Brasília-DF

2025

**USO DE TECNOLOGIAS DE RECONHECIMENTO FACIAL PELA
SEGURANÇA PÚBLICA NO DISTRITO FEDERAL: IMPLICAÇÕES
ÉTICAS, LEGAIS E NA PROTEÇÃO DE DADOS DOS CIDADÃOS.**

Comissão Examinadora constituída por:

Professor Dr. Luiz Honorato da Silva Junior
Orientador – PPGP/UnB

Professor Dr. Mauro Eduardo Del Grossi
Examinador Interno – PPGP/UnB

Professor Dr. Adriano Nascimento da Paixão
Examinador Externo – UFPB

Professor Dr. Luiz Sebastião dos Santos Júnior
Examinador Externo – UFPE

Dedico este trabalho principalmente ao meu orientador, que, com paciência e apoio inabalável, me guiou por um mestrado que se alongou além do comum, interrompido por sombras silenciosas que, como um peso escondido, visitam tantos de nós em segredo. Agradeço de coração aos poucos que nunca soltaram minha mão. À minha filha Maria Fernanda, meu amor eterno, dedico cada página com todo o meu sentimento, pedindo perdão por momentos que não estive ao seu lado, mas prometendo que este esforço é também por você, minha luz.

AGRADECIMENTOS

Antes de tudo, agradeço a Deus, minha força e refúgio, que com **S**ua infinita bondade me sustentou em cada passo desta longa jornada, iluminando meu caminho mesmo nas noites mais escuras.

Minha gratidão ao meu orientador, cuja paciência, sabedoria e confiança em mim foram faróis nos longos anos deste mestrado, marcados por pausas impostas por um vazio silencioso que, invisível, desafia tantos.

Aos poucos e seletos amigos e familiares que, com palavras e gestos simples, me lembraram que não estava sozinha.

À minha filha Maria Fernanda, minha estrela guia, agradeço por seu amor incondicional, mesmo quando o peso do caminho me afastou de você; sua luz me trouxe até aqui. À instituição e aos colegas que cruzaram esta jornada, meu reconhecimento por cada apoio, por menor que pareça. Este trabalho é fruto de todos vocês.

RESUMO

O avanço das tecnologias de inteligência artificial tem ampliado o uso do reconhecimento facial (RF) como ferramenta estratégica para a segurança pública. No Brasil, especialmente no Distrito Federal, sua implementação ocorre em um cenário marcado por lacunas normativas, desafios éticos e insegurança jurídica para os agentes públicos. Esta dissertação, vinculada ao Programa de Pós-Graduação em Gestão Pública da Universidade de Brasília (PPGP/FUP-UnB), tem como objetivo geral avaliar as implicações do uso do reconhecimento facial pela segurança pública, com foco nas dimensões éticas, legais e de proteção de dados. A pesquisa está estruturada no formato *multipaper*, composta por dois artigos científicos complementares. O primeiro artigo analisa criticamente as lacunas regulatórias e os dilemas éticos associados ao uso da tecnologia no Brasil, por meio de revisão sistemática e análise documental, com comparação a modelos normativos internacionais, como os da União Europeia e dos Estados Unidos. O estudo evidencia que a ausência de um marco regulatório nacional específico compromete a segurança jurídica das operações policiais, dificulta a transparência e limita o potencial estratégico da tecnologia. O segundo artigo apresenta uma análise empírica sobre a percepção de agentes das forças de segurança do Distrito Federal — Polícia Civil (PCDF) e Polícia Militar (PMDF) — quanto ao uso do RF em sua atuação cotidiana. Com base em 278 respostas a questionários e entrevistas semiestruturadas, os resultados indicam que, embora a maioria dos agentes reconheça a eficácia do RF para localizar suspeitos e reduzir o tempo de busca, a adoção prática ainda é rara. Fatores como a falta de regulamentação clara, de capacitação técnica e de respaldo jurídico são apontados como principais obstáculos à consolidação da tecnologia no âmbito da segurança pública. A dissertação conclui que é urgente a construção de um marco regulatório nacional que equilibre inovação tecnológica, autonomia operacional e proteção de direitos fundamentais. Propõe-se um modelo baseado em três pilares: transparência, responsabilização institucional e flexibilidade normativa, capaz de garantir governança sem comprometer a eficácia policial. A ausência de normativas específicas tem limitado o uso ético e estratégico da tecnologia e representa um risco tanto para os direitos individuais quanto para a efetividade do Estado no enfrentamento à criminalidade.

Palavras-chave: Dados pessoais; Inteligência artificial; Reconhecimento facial; Regulação; Segurança pública.

ABSTRACT

The advancement of artificial intelligence technologies has expanded the use of facial recognition (FR) as a strategic tool for public security. In Brazil, particularly in the Federal District, the implementation of such systems has occurred in a context marked by regulatory gaps, ethical challenges, and legal uncertainty for law enforcement officers. This dissertation, developed within the Graduate Program in Public Management at the University of Brasília (PPGP/FUP-UnB), aims to evaluate the implications of using facial recognition technology in public security, with a focus on ethical, legal, and data protection dimensions. The research is structured in a multipaper format, composed of two complementary scientific articles.

The first article critically analyzes the regulatory voids and ethical dilemmas associated with the use of this technology in Brazil, through systematic review and documentary analysis, with comparisons to international regulatory models, such as those adopted in the European Union and the United States. The findings show that the lack of a specific national legal framework undermines legal certainty, transparency, and the strategic potential of the technology in police operations.

The second article presents an empirical analysis of the perceptions of public security agents from the Federal District — Civil Police (PCDF) and Military Police (PMDF) — regarding the operational use of FR in their routine activities. Based on 278 responses to questionnaires and semi-structured interviews, the study reveals that, although most agents acknowledge the usefulness of the technology in suspect identification and crime reduction, its practical adoption remains limited. The main obstacles identified include lack of regulation, insufficient technical training, and lack of legal support.

The dissertation concludes that there is an urgent need for a national regulatory framework that balances technological innovation, operational autonomy, and the protection of fundamental rights. It proposes a model based on three pillars: transparency, institutional accountability, and normative flexibility. The absence of such regulation limits both the ethical application of facial recognition and the state's capacity to combat crime effectively.

Keywords: Artificial intelligence; Data protection; Facial recognition; Public security; Regulation.

LISTA DE FIGURAS

Artigo: LACUNAS REGULATÓRIAS E DESAFIOS ÉTICOS DO RECONHECIMENTO FACIAL
NA SEGURANÇA PÚBLICA BRASILEIRA

Figura 1 – Evolução do total acumulado de rostos escaneados pela tecnologia de
reconhecimento facial (RF) pela polícia metropolitana -----20

LISTA DE TABELAS

Artigo: LACUNAS REGULATÓRIAS E DESAFIOS ÉTICOS DO RECONHECIMENTO FACIAL
NA SEGURANÇA PÚBLICA BRASILEIRA

Tabela 1- Resultado Pesquisa Portal Capes-----28

Tabela 2 - Processo de seleção dos documentos pelo protocolo PRISMA-----30

Artigo: RECONHECIMENTO FACIAL: PERCEPÇÕES, DESAFIOS E IMPLICAÇÕES NA
SEGURANÇA PÚBLICA DO DISTRITO FEDERAL

Tabela ~~34~~: Distribuição dos respondentes por cargo-----
55

Tabela ~~42~~: Percepção sobre o impacto do reconhecimento facial nas investigações-----
57

Tabela ~~53~~: Preocupações dos respondentes em relação ao uso do reconhecimento facial-----
59

LISTA DE QUADROS

Artigo: LACUNAS REGULATÓRIAS E DESAFIOS ÉTICOS DO RECONHECIMENTO FACIAL
NA SEGURANÇA PÚBLICA BRASILEIRA

Quadro 1- Comparação de normativas para Reconhecimento Facial-----33

LISTA DE ABREVIATURAS E SIGLAS

AI	<i>Artificial Intelligence</i> (Inteligência Artificial)
AI ACT	<i>Artificial Intelligence Act</i> (Regulamento Europeu sobre Inteligência Artificial)
ANOVA	<i>Analysis of Variance</i> (Análise de Variância)
CNJ	Conselho Nacional de Justiça
DF	Distrito Federal
GDPR	<i>General Data Protection Regulation</i> (Regulamento Geral de Proteção de Dados da União Europeia)
GDF	Governo do Distrito Federal
IA	Inteligência Artificial
LGPD	Lei Geral de Proteção de Dados Pessoais
PCDF	Polícia Civil do Distrito Federal
PMDF	Polícia Militar do Distrito Federal
PRISMA	<i>Preferred Reporting Items for Systematic Reviews and Meta-Analyses</i>
RF	Reconhecimento Facial
RIS	<i>Research Information Systems</i> (formato de exportação bibliográfica)
UE	União Europeia
UnB	Universidade de Brasília
USA	<i>United States of America</i> (Estados Unidos da América)

SUMÁRIO

Considerações Iniciais	13
LACUNAS REGULATÓRIAS E DESAFIOS ÉTICOS DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA BRASILEIRA	15
Resumo	15
1. Introdução	16
2. Inteligência artificial (IA) e reconhecimento facial (RF): definições e seus fundamentos tecnológicos	17
3. Desafios éticos e sociais no uso de tecnologias de reconhecimento facial	18
4. O vácuo normativo no Brasil e os riscos da falta de regulamentação	21
4.1 Legislações e diretrizes.....	22
4.1.1 O Cenário Normativo Brasileiro.....	22
4.1.2 Experiências Internacionais e Lições para o Brasil	23
4.1.3 Iniciativas Legislativas no Brasil	24
4.1.4 Caminhos para um marco regulatório eficiente	25
4.1.5 Análise Crítica ao Projeto de Lei nº 1515/2022: Limitações à Ação das Forças de Segurança e Impactos na Inovação.....	26
5. Metodologia	28
6. Resultados e considerações finais.....	32
7. Conclusões	33
Referências.....	36
RECONHECIMENTO FACIAL: PERCEPÇÕES, DESAFIOS E IMPLICAÇÕES NA SEGURANÇA PÚBLICA DO DISTRITO FEDERAL	41
Resumo	41
1. Introdução	42
2. Conceito de reconhecimento facial e segurança pública	43
2.1 Conceito de segurança pública.....	43
2.2 Crescimento populacional e aumento dos riscos	45
2.3 A necessidade de tecnologia como compensação.....	45
3. Estudos e casos de aplicação no mundo e no Brasil	46
3.1 Cenário do reconhecimento facial no ambiente público do Distrito Federal: o Horus Persona	47

4. Desafios regulatórios e éticos	50
4.1 Vieses e discriminação em sistemas de reconhecimento facial	50
5. Método utilizado para pesquisa.....	51
6. Resultados e discussões	54
6.1 Perfil dos respondentes	55
6.2 Adoção do Reconhecimento Facial.....	56
6.3 Percepções sobre eficácia e impacto.....	57
6.4 Barreiras operacionais e técnicas.....	58
6.5 Acurácia, falhas e confiabilidade.....	58
6.6 Questões éticas e jurídicas	60
6.7 Necessidade de regulamentação.....	61
6.8 Integração dos dados: triangulação e síntese final dos achados	62
7. Conclusões	63
Referências.....	64
Considerações Finais	67

Contextualização

O avanço das tecnologias digitais, especialmente aquelas baseadas em inteligência artificial, tem transformado significativamente a atuação estatal no campo da segurança pública. Entre essas tecnologias, destaca-se o reconhecimento facial (RF), cuja adoção pelas forças policiais brasileiras tem se expandido em grandes centros urbanos ([Freitas, 2024](#); [Fórum Brasileiro de Segurança Pública, 2023](#)), embora essa expansão seja marcada por incertezas normativas, desafios éticos e receios jurídicos. A utilização dessa ferramenta, que visa ampliar a eficácia na identificação de suspeitos e na resolução de crimes, revela tensões relevantes entre inovação tecnológica, proteção de direitos fundamentais e a autonomia operacional dos agentes públicos.

Esta dissertação, vinculada ao Programa de Pós-Graduação em Gestão Pública (PPGP/FUP) da Universidade de Brasília (UnB), insere-se nesse contexto e propõe uma análise crítica sobre o uso do reconhecimento facial pela segurança pública no Distrito Federal. A escolha do tema decorre da constatação de que, apesar do potencial estratégico da tecnologia, sua implementação no Brasil ocorre de forma fragmentada e sem diretrizes normativas unificadas, o que acarreta insegurança jurídica tanto para os operadores quanto para os cidadãos. Tal cenário exige reflexão urgente sobre a necessidade de um marco regulatório nacional que equilibre a proteção de dados, a ética institucional e a eficiência das ações policiais.

A estrutura da dissertação adota o formato *multipaper*, contemplando dois artigos científicos independentes e complementares, que dialogam diretamente com os objetivos específicos do trabalho. O primeiro artigo investiga as lacunas regulatórias e os dilemas éticos associados ao uso do reconhecimento facial no Brasil, com base em revisão sistemática e análise documental, e realiza comparações com modelos normativos adotados nos Estados Unidos e [nos países que compõem a](#) União Europeia. O segundo artigo, de caráter empírico, analisa a percepção de policiais civis e militares do Distrito Federal quanto à aplicação prática do reconhecimento facial, seus desafios operacionais e implicações jurídicas, a partir de questionários e entrevistas com operadores da tecnologia.

Ambos os artigos convergem para o objetivo geral da pesquisa: avaliar as implicações do uso do reconhecimento facial pela segurança pública, com foco nas dimensões éticas, legais e de proteção de dados. A perspectiva adotada é aquela do agente estatal que atua diretamente com a tecnologia — uma abordagem ainda pouco explorada na literatura nacional, geralmente dominada por olhares externos voltados exclusivamente à defesa de direitos individuais. A dissertação busca, portanto, oferecer uma contribuição original ao revelar os entraves

enfrentados pelas forças de segurança e propor soluções regulatórias que não apenas protejam a privacidade, mas também garantam respaldo jurídico e operacional às instituições públicas.

A metodologia adotada combina revisão bibliográfica, análise documental e investigação empírica por meio de formulário online e entrevistas com servidores da segurança pública do Distrito Federal. A abordagem qualitativa e descritiva permitiu captar tanto os aspectos normativos quanto as percepções práticas dos operadores. Essa triangulação entre teoria, legislação e prática ampliou o rigor da análise e fortaleceu a pertinência das recomendações formuladas.

Os referenciais teóricos que embasam a dissertação incluem autores como Floridi [\(2024\)](#), Zuboff [\(2019\)](#), Lyon [\(2001\)](#) e Creswell [\(2014\)](#), cujas obras oferecem fundamentos robustos para a reflexão ética, metodológica e regulatória da inteligência artificial aplicada à segurança pública. O estudo também dialoga com experiências normativas internacionais, como o AI Act da União Europeia e diretrizes regulatórias dos Estados Unidos, evidenciando as possíveis trajetórias que o Brasil pode seguir no desenvolvimento de sua própria regulação.

A relevância da presente pesquisa reside na urgência de se estabelecer um marco normativo claro e funcional que discipline o uso do reconhecimento facial na segurança pública brasileira. Em vez de frear a inovação com regulamentações excessivamente restritivas, o Brasil deve buscar um modelo equilibrado que garanta governança, responsabilidade e proteção de dados, mas que também permita respostas ágeis e eficazes ao crime. A dissertação espera contribuir para esse debate ao apresentar diagnósticos precisos, embasados em evidência empírica, e ao propor diretrizes regulatórias compatíveis com a realidade operacional das forças de segurança do país.

LACUNAS REGULATÓRIAS E DESAFIOS ÉTICOS DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA BRASILEIRA

Resumo Este artigo analisa as lacunas regulatórias e os desafios éticos associados ao uso do reconhecimento facial (RF) na segurança pública brasileira. A partir de uma revisão sistemática e análise documental, a pesquisa examina a ausência de um marco normativo específico, evidenciando os riscos jurídicos e sociais decorrentes da falta de padronização e de mecanismos de transparência. O estudo investiga o impacto da tecnologia na privacidade e na vigilância em massa, discutindo possíveis vieses algorítmicos e suas implicações na confiança pública. Para subsidiar o debate regulatório, são analisadas experiências internacionais, com ênfase nos modelos da União Europeia e de estados norte-americanos que implementaram restrições ou auditorias obrigatórias para o uso da tecnologia. A pesquisa propõe diretrizes para a construção de um arcabouço regulatório nacional que equilibre inovação tecnológica, segurança pública e proteção dos direitos fundamentais. Conclui-se que, diante do avanço da inteligência artificial, o Brasil necessita de um modelo normativo que estabeleça transparência, supervisão independente e salvaguardas contra abusos institucionais, mas que não sejam barreiras à inovação.

Palavras-chave: Inteligência artificial, proteção de dados, reconhecimento facial, regulamentação, segurança pública, vigilância digital, viés algorítmico.

Abstract: This article analyzes the regulatory gaps and ethical challenges associated with the use of facial recognition (FR) in Brazilian public security. Based on a systematic review and documentary analysis, the research examines the absence of a specific regulatory framework, highlighting the legal and social risks arising from the lack of standardization and transparency mechanisms. The study investigates the impact of technology on privacy and mass surveillance, discussing potential algorithmic biases and their implications for public trust. To support the regulatory debate, international experiences are analyzed, with an emphasis on the models of the European Union and U.S. states that have implemented restrictions or mandatory audits for the use of this technology. The research proposes guidelines for developing a national regulatory framework that balances technological innovation, public security, and the protection of fundamental rights. The study concludes that, given the advancement of artificial intelligence, Brazil needs a regulatory model that establishes transparency, independent oversight, and safeguards against institutional abuses, while avoiding barriers to innovation.

Keywords: Algorithmic bias, artificial intelligence, data protection, digital surveillance, facial recognition, public security, regulation.

1. Introdução

O desenvolvimento de tecnologias voltadas à segurança pública tem sido impulsionado pelo avanço da inteligência artificial (IA), destacando-se o reconhecimento facial (RF) nesse cenário. O uso da tecnologia por forças policiais em diferentes países tem sido defendido como uma maneira de tornar a identificação de indivíduos mais ágil, facilitar investigações criminais e aumentar a eficiência operacional. No entanto, no Brasil, essa implementação ocorre de forma descentralizada e sem um marco regulatório bem definido, o que gera insegurança jurídica, dilemas éticos e riscos à privacidade dos cidadãos onde, por um lado, os agentes públicos que utilizam a tecnologia enfrentam dúvidas jurídicas; por outro, a sociedade carece de mecanismos que garantam controle e transparência no uso desses sistemas. Enquanto países como os Estados Unidos (EUA) e [países](#) membros da União Europeia (UE) já estabeleceram regulamentações mais específicas,⁷ [o](#) Brasil ainda enfrenta um vácuo normativo e a ausência de regras bem estruturadas tem gerado debates sobre a legalidade, a proporcionalidade e a compatibilidade do RF com os princípios do ordenamento jurídico nacional.

Diante desse contexto, este artigo tem como proposta analisar as lacunas regulatórias existentes no Brasil quanto à aplicação do RF na segurança pública. Para isso, serão feitas comparações com experiências internacionais e discutidos os principais desafios éticos e operacionais envolvidos na adoção dessa tecnologia. Além disso, pretende-se sugerir diretrizes que possam contribuir para a construção de um marco regulatório capaz de equilibrar inovação tecnológica e proteção de direitos fundamentais.

A relevância desta pesquisa se justifica pela ausência de normativos e padronizações específicas para o uso destas tecnologias na segurança pública brasileira, tornando essencial um estudo aprofundado do tema. A definição de políticas públicas para inteligência artificial é uma questão essencial e urgente e se tornou um tema central nos debates sobre inovação e governança. Atrasos no processo podem colocar um país em posição desfavorável no cenário global, dificultando sua capacidade de acompanhar avanços tecnológicos possibilitando que a lacuna regulatória não apenas impacte o desenvolvimento econômico, mas também comprometa áreas estratégicas, como segurança e soberania nacional. Diretrizes bem elaboradas são essenciais para assegurar que a inteligência artificial seja implementada de maneira planejada e benéfica para a sociedade.

Para cumprir os objetivos propostos, o artigo está estruturado em seções complementares. A primeira seção apresenta um panorama das lacunas normativas existentes no Brasil, evidenciando os riscos e desafios decorrentes da falta de regulamentação específica. Em seguida, a segunda seção explora experiências internacionais na regulação do

reconhecimento facial, destacando diretrizes adotadas na União Europeia e nos Estados Unidos. A terceira seção discute as principais iniciativas legislativas no Brasil, analisando os projetos de lei em tramitação e seus impactos para o setor. A quarta seção propõe diretrizes regulatórias para a criação de um arcabouço normativo eficaz, considerando aspectos de transparência, supervisão e responsabilização. Por fim, a última seção sintetiza as principais conclusões da pesquisa, destacando os desafios e oportunidades para a regulamentação do reconhecimento facial na segurança pública brasileira.

2. Inteligência Artificial (IA) e Reconhecimento Facial (RF): Definições e seus fundamentos tecnológicos

A inteligência artificial tem se consolidado como um campo fundamental da ciência da computação, oferecendo soluções avançadas para diversas áreas do conhecimento. Sua definição pode variar conforme o contexto de aplicação, mas, de maneira geral, envolve sistemas capazes de analisar dados, tomar decisões autônomas e aprimorar seu desempenho progressivamente. A norma ABNT NBR ISO 22989:2023 descreve a IA como um conjunto de tecnologias projetadas para desempenhar funções que exigiriam inteligência humana, tais como raciocínio lógico, reconhecimento de padrões e aprendizado contínuo. Russell e Norvig (2016) reforçam essa concepção ao definir a IA como a capacidade de máquinas em imitar funções cognitivas humanas, permitindo que algoritmos sejam treinados para solucionar problemas e tomar decisões com base em grandes volumes de informações.

O uso da inteligência artificial já se encontra disseminado em múltiplos setores, como assistentes virtuais, autenticação de identidade em dispositivos móveis, análise preditiva, automação de processos nas áreas jurídica e administrativa, além de vigilância em espaços públicos e privados. No contexto da administração pública, sua adoção tem sido destacada por instituições como o Conselho Nacional de Justiça (CNJ, 2024), que aponta a utilização de IA na automatização de procedimentos jurídicos, elaboração de minutas e extração de informações de documentos processuais, o que contribui para maior eficiência dos tribunais. Além do setor judiciário, a IA tem sido aplicada na gestão pública para otimizar serviços administrativos e reduzir a sobrecarga de servidores, conforme observado pelo Conselho da União Europeia (2023). Dentre as inúmeras aplicações, uma das mais debatidas nos últimos anos tem sido o RF, tecnologia que utiliza algoritmos avançados para identificar ou verificar a identidade de indivíduos por meio de suas características faciais.

Os sistemas de monitoramento facial evoluíram significativamente desde suas primeiras pesquisas na década de 1960, tornando-se mais sofisticados e acessíveis com o avanço da visão

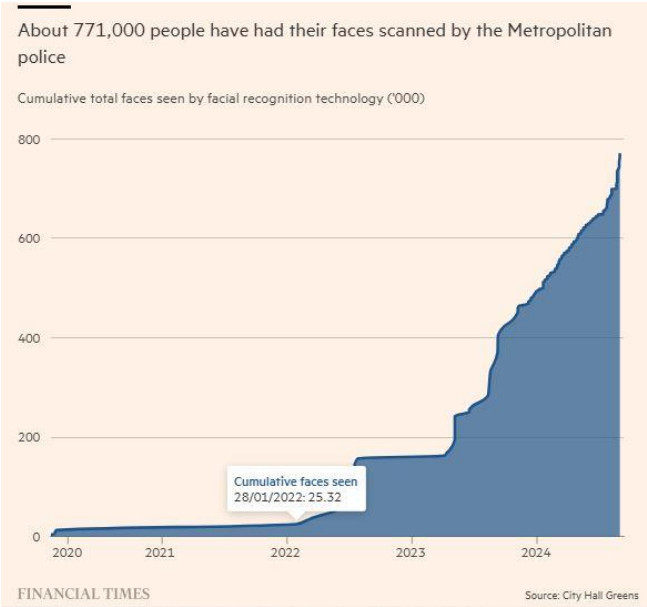
computacional e do aprendizado de máquina. De acordo com Silva e Rosa (2004), essa tecnologia funciona por meio da extração e análise de características faciais, comparando imagens captadas com registros armazenados em bancos de dados. Gargaro e Millman (2024) explicam que os algoritmos de RF operam analisando traços distintos, como a distância entre os olhos, a simetria da face e o formato do nariz e da boca, criando uma matriz de características biométricas que possibilita a identificação de indivíduos. O processamento dessas informações ocorre por meio de redes neurais convolucionais (Convolutional Neural Network - CNNs), que conseguem detectar padrões visuais complexos e extrair características essenciais das imagens analisadas. Conforme destacado por Goodfellow, Bengio e Courville (2016), as CNNs são amplamente utilizadas em aplicações de visão computacional, pois permitem que o RF ocorra mesmo sob variações de iluminação, ângulos de captura e expressões faciais, aumentando a precisão do sistema.

A eficácia dos sistemas de RF pode ser influenciada por diversos fatores, como qualidade da imagem, posicionamento do indivíduo e condições ambientais. Zhu et al. (2015) apontam que a variação desses elementos pode comprometer a precisão dos algoritmos, exigindo refinamento contínuo dos modelos utilizados. Apesar das limitações, a tecnologia tem sido amplamente adotada no setor de segurança pública, onde a necessidade de identificação rápida e precisa de indivíduos em meio a grandes multidões tornou o RF uma ferramenta estratégica para ações preventivas e investigativas.

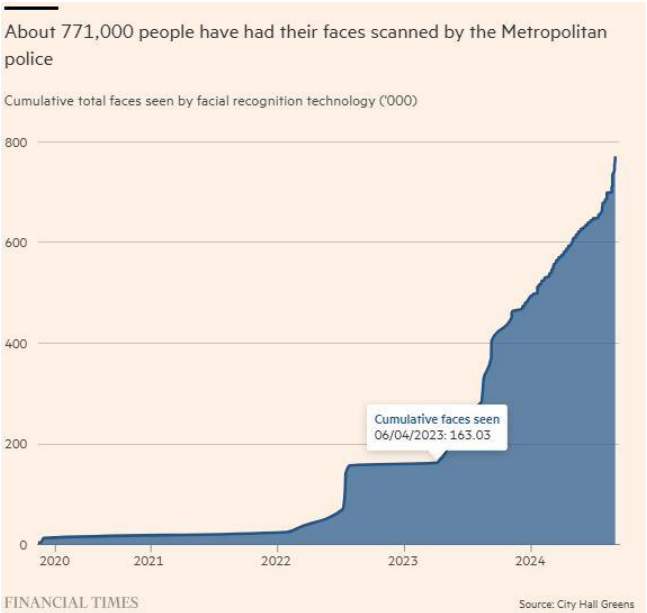
3. Desafios éticos e sociais no uso de tecnologias de reconhecimento facial

Na segurança pública, a tecnologia se destaca pelo potencial de auxiliar na identificação de suspeitos e na localização de pessoas desaparecidas, sendo utilizada em operações policiais e sistemas de monitoramento urbano-urbano. O *Financial Times* (2024) noticiou que a Polícia Metropolitana de Londres realizou mais de 117 operações utilizando RF apenas no primeiro semestre de 2024, implantações três vezes mais que nos quatro anos anteriores evidenciam o crescimento da adoção dessa ferramenta no combate ao crime (Figura 1). Além disso, a tecnologia tem sido aplicada para prevenir fraudes e aumentar a segurança em transações financeiras, como demonstrado por instituições bancárias que utilizam a biometria facial para autenticação de usuários e validação de operações (Keyless.io, 2024).

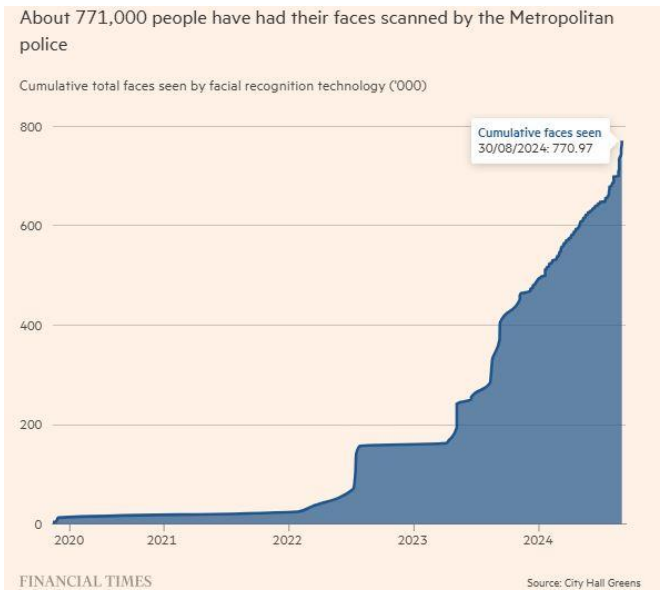
Formatado: Fonte: Itálico



(a) Janeiro de 2022



(b) Abril de 2023



(c) Agosto de 2024

Figura 1 – Evolução do total acumulado de rostos escaneados pela tecnologia de reconhecimento facial (RF) pela polícia metropolitana
Fonte: Financial Times (2024)

Embora o RF ofereça benefícios expressivos, sua implementação enfrenta desafios técnicos e éticos que precisam ser considerados. A precisão dos algoritmos pode ser comprometida por variações na qualidade das imagens e pelo próprio funcionamento dos modelos de aprendizado de máquina. Segundo Sanchez-Moreno et al. (2021), os sistemas de RF são eficientes na identificação e captura de suspeitos em cenários de vigilância, mas demandam rigorosos testes de calibração para minimizar erros de identificação e vies algorítmico. isto é, a tendência do sistema de apresentar taxas de erro desproporcionalmente maiores para determinados grupos demográficos, como mulheres e pessoas negras (Buolamwini e Gebru, 2018).

Formatado: Fonte: (Padrão) Times New Roman

O uso de tecnologias de RF levanta questionamentos éticos, especialmente em relação à privacidade e ao risco de vigilância em massa. A adoção da ferramenta sem diretrizes claras pode resultar em um ambiente de monitoramento constante, onde a população perde autonomia sobre sua própria identidade digital. Lyon (2018) alerta que a normalização de sistemas de vigilância impacta negativamente as liberdades individuais, uma vez que cidadãos podem ser rastreados sem consentimento explícito. Além disso, há preocupações sobre a transparência e o uso das bases de dados que alimentam esses sistemas, visto que, muitas vezes, a população

desconhece os critérios adotados para a coleta e o processamento das imagens. Outro problema ético relevante envolve o viés algorítmico e a possibilidade de discriminação racial. Estudos como os de Buolamwini e Gebu (2018) demonstram que sistemas de RF apresentam taxas de erro mais elevadas na identificação de indivíduos pertencentes a grupos raciais específicos, o que pode perpetuar desigualdades estruturais. No Brasil, um levantamento realizado pela Rede de Observatórios da Segurança (2019) revelou que 90% das prisões efetuadas com base em monitoramento facial entre março e outubro de 2019 envolveram pessoas negras, evidenciando a necessidade de auditorias técnicas para garantir que a tecnologia seja aplicada de maneira justa e equitativa.

4. O Vácuo Normativo no Brasil e os Riscos da Falta de Regulamentação

A aplicação de tecnologias de RF na segurança pública brasileira ocorre em um cenário de incerteza jurídica devido à ausência de um marco regulatório específico. Embora a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) estabeleça diretrizes para o tratamento de dados pessoais, sua aplicabilidade ao uso dessa tecnologia no contexto da segurança pública ainda é ambígua. Segundo Melo e Serra (2023), a falta de regulamentação clara gera riscos operacionais e desafios éticos significativos, permitindo interpretações diversas sobre a legalidade da ferramenta e abrindo espaço para práticas discriminatórias. Buiten (2019) e Barroso (2024) também ressaltam que a lacuna normativa compromete a previsibilidade das ações do Estado e levanta preocupações sobre possíveis abusos e violações de direitos fundamentais.

A regulamentação do RF no Brasil enfrenta o desafio da fragmentação legislativa. Sem uma estrutura nacional uniforme, estados e municípios têm adotado normativas próprias, muitas vezes sem critérios padronizados de transparência, auditoria e supervisão independente. O Regulamento Europeu de Inteligência Artificial (AI ACT, 2024) demonstra a importância de um conjunto normativo estruturado para garantir um uso mais seguro e justo dessas ferramentas, destacando a necessidade de um modelo semelhante no Brasil. Conforme Veale e Borgesius (2021), tal disparidade compromete a segurança jurídica dos agentes públicos e dificulta a definição de diretrizes mínimas que garantam o uso responsável da tecnologia. Além disso, Brundage et al. (2020) enfatizam que a ausência de exigências normativas para auditorias contínuas compromete a confiabilidade dos sistemas, tornando-os suscetíveis a falhas e vieses. Um estudo do Observatório da Segurança (2019) mostra que a falta de padrões regulatórios pode levar a erros sistemáticos na aplicação da tecnologia, prejudicando principalmente grupos

historicamente marginalizados, o que reforça a necessidade de medidas eficazes para evitar discriminação.

Diante do cenário discutido, a criação de um marco regulatório federal se apresenta como uma necessidade urgente. Buiten (2019) destaca que um modelo regulatório robusto deve assegurar transparência, equidade e previsibilidade na aplicação da tecnologia de RF. Experiências internacionais, como as estabelecidas pelo AI ACT da União Europeia, demonstram que a implementação de normas claras reduz os riscos associados ao uso indiscriminado da tecnologia e melhora sua confiabilidade. No entanto, enquanto essa regulamentação não for implementada no Brasil, as tecnologias continuarão a ser aplicadas sem um controle efetivo. Brundage et al. (2020) alertam que, sem auditorias e supervisão adequadas, cidadãos permanecerão vulneráveis a possíveis abusos e erros, o que pode comprometer a legitimidade e a eficácia do uso dessa tecnologia no país.

4.1. Legislações e diretrizes

4.1.1. O Cenário Normativo Brasileiro

O Brasil ainda não conta com uma legislação federal específica para regulamentar o uso do reconhecimento facial na segurança pública. Embora a LGPD estabeleça diretrizes para o tratamento de dados pessoais, sua aplicação ao uso de inteligência artificial nesse setor permanece indefinida. Segundo Azevedo et al. (2022), essa lacuna impede que agentes públicos tenham parâmetros claros para operar a tecnologia, o que pode resultar tanto em insegurança jurídica quanto na aplicação inconsistente das ferramentas de captura e monitoramento facial. A falta de normatização não apenas compromete a previsibilidade legal, mas também gera desafios operacionais diretos para os profissionais de segurança pública, que precisam lidar com a incerteza sobre a legalidade de suas ações. Conforme aponta Gargaro e Millman (2024), a ausência de regulamentação nacional uniforme faz com que cada estado ou município defina seus próprios critérios para o uso da tecnologia, sem necessariamente seguir padrões mínimos de transparência ou governança. Como consequência, um mesmo sistema pode ser aplicado de maneiras diferentes em diferentes localidades, criando distorções e insegurança para os operadores da tecnologia.

Além da falta de padronização, a ausência de auditorias técnicas obrigatórias e de supervisão independente amplia o risco de monitoramento indevido e abordagens seletivas, conforme alerta Cavoukian e Jonas (2012). Sem mecanismos de fiscalização eficazes, não há garantias de que os sistemas utilizados estejam sendo revisados regularmente para evitar vieses

ou falhas operacionais. Esse problema é especialmente preocupante em um cenário onde, de acordo com o relatório do Conselho Nacional de Justiça (2024), não há diretrizes nacionais que exijam auditorias recorrentes ou relatórios de impacto para esses sistemas, o que pode comprometer sua confiabilidade e aumentar o risco de uso indevido da tecnologia. Diante desse cenário, Freitas (2024) observa que a ausência de regulamentação não impediu a ampliação do uso do monitoramento em cidades como São Paulo, onde a implementação ocorre sem garantias formais de governança. Essa situação reforça a necessidade de um arcabouço regulatório federal capaz de garantir não apenas um uso transparente e previsível, mas também de estabelecer mecanismos que assegurem a proteção de direitos fundamentais. Como destaca Cavoukian (2012), qualquer sistema de inteligência artificial aplicado a políticas públicas deve incorporar princípios de governança desde sua concepção, garantindo que a proteção da privacidade e dos direitos civis seja uma prioridade e não uma preocupação secundária.

A insegurança jurídica afeta diretamente os profissionais da segurança pública, que podem ser responsabilizados por eventuais violações de privacidade sem que existam parâmetros claros para a operação da tecnologia. A falta de padronização na implementação dos sistemas de RF acentua desigualdades entre estados e municípios, permitindo que cada localidade estabeleça critérios próprios, muitas vezes sem garantias mínimas de governança e transparência. ~~Além disso, sem auditorias técnicas obrigatórias e supervisão independente, cresce o risco de monitoramento indevido e de perseguições seletivas, tornando urgente a criação de um arcabouço regulatório que estabeleça regras claras para a utilização dessa tecnologia.~~

4.1.2. Experiências Internacionais e Lições para o Brasil

A experiência internacional demonstra que países que estabeleceram marcos regulatórios específicos para o RF apresentam maior controle sobre seu uso e mitigam riscos relacionados à privacidade e discriminação. A distinção entre os modelos regulatórios dos EUA e da EU na IA é amplamente discutida na literatura acadêmica. Buiten (2019) e Veale & Zuiderveen Borgesius, (2021) apontam que os EUA adotam uma postura de regulação mínima, incentivando a inovação e permitindo que o mercado se autorregule, enquanto a União Europeia opta por uma abordagem mais prescritiva, baseada na avaliação de riscos e na proteção de direitos fundamentais.

A União Europeia, por meio do *Artificial Intelligence Act* (AI Act, 2024), classificou o RF como uma tecnologia de alto risco, impondo restrições rigorosas à sua implementação exigindo transparência, auditorias frequentes e avaliações de impacto antes do uso.

Complementarmente, o Regulamento Geral de Proteção de Dados (GDPR, 2018) estabelece exigências rigorosas de consentimento e proteção de dados pessoais, garantindo que as aplicações dessa tecnologia respeitem princípios fundamentais de privacidade e equidade. De acordo com Floridi et al. (2018) o modelo europeu é baseado na ideia de que a IA deve respeitar princípios éticos e legais preexistentes, garantindo transparência, responsabilidade e supervisão humana. Por outro lado, a *Executive Order 13859*, promulgada nos EUA, que é um marco da estratégia do governo americano, estabelece diretrizes para o desenvolvimento da IA sem impor barreiras regulatórias significativas (*US Government, 2019*). Segundo Bryson (2019) tal visão é sustentada pelo argumento de que regulamentações excessivas podem inibir o avanço tecnológico e comprometer a competitividade americana no cenário global

Nos EUA, a regulação da IA está fortemente atrelada à segurança nacional e à manutenção da liderança global no setor. Conforme apontam Allen & Chan (2019), a estratégia americana busca impedir que adversários geopolíticos, como a China, dominem o desenvolvimento da IA, o que justifica a ênfase na proteção de propriedade intelectual e na segurança cibernética. Em contraste, a União Europeia preocupa-se mais com os impactos sociais e éticos da IA. Estudos como os de Wachter, Mittelstadt & Floridi (2017) ressaltam a necessidade de supervisão regulatória para evitar discriminação algorítmica e violações de privacidade. Para Veale (2021) a abordagem europeia se baseia nos princípios da regulamentação baseada em risco, que busca equilibrar inovação e proteção de direitos fundamentais.

A China, por sua vez, adota uma abordagem vertical de regulação de IA, com leis específicas para questões como reconhecimento facial e vigilância, integradas a um sistema de controle estatal voltado para segurança pública e estabilidade social (Taeihagh, 2021). Características centrais incluem o registro público de sistemas de IA, avaliações éticas obrigatórias, e supervisão rigorosa, frequentemente associada a tecnologias de vigilância em massa, como o Sistema de Crédito Social. Diferentemente da UE, que prioriza direitos fundamentais, e dos EUA, que enfatizam inovação, o modelo chinês levanta preocupações éticas sobre privacidade e liberdades individuais, mas demonstra a eficácia de regulamentações específicas para mitigar riscos técnicos e operacionais.

A escolha entre um modelo mais flexível e voltado à inovação, como o dos EUA, um modelo mais regulado e orientado à segurança jurídica, como o europeu, ou um modelo de controle estatal, como o chinês, tem implicações diretas para o Brasil. Segundo Carini (2020), o país deve adotar um modelo híbrido, considerando a necessidade de fomentar inovação sem

Formatado: Justificado, Recuo: Primeira linha: 1,25 cm, Espaço Antes: 0 pt, Depois de: 6 pt, Espaçamento entre linhas: 1,5 linhas

negligenciar aspectos éticos e legais, e aprendendo com as experiências internacionais para estabelecer regulamentações específicas que equilibrem eficiência tecnológica e proteção de direitos fundamentais.

~~A escolha entre um modelo mais flexível e voltado à inovação, como o dos EUA, ou um modelo mais regulado e orientado à segurança jurídica, como o europeu, tem implicações diretas para o Brasil. Segundo Carini (2020), o país deve adotar um modelo híbrido, considerando a necessidade de fomentar inovação sem negligenciar aspectos éticos e legais.~~

4.1.3. Iniciativas Legislativas no Brasil

A regulação da IA no Brasil tem sido objeto de discussões diferentes frentes e esferas, porém ainda carece de normativas detalhadas para aplicações de alto impacto, como o RF na segurança pública. O país conta com um conjunto de leis e políticas voltadas à inovação digital, mas sem diretrizes específicas que orientem a aplicação dessas tecnologias em operações policiais e vigilância pública.

Entre os principais normativos existentes, destaca-se a Lei de Inovação (Lei nº 10.973/2004), que incentiva a pesquisa científica e tecnológica, mas não aborda questões éticas e operacionais do uso da IA para segurança pública. De forma semelhante, o Marco Civil da Internet (Lei nº 12.965/2014) estabelece princípios gerais de proteção de dados e privacidade.

A Estratégia Brasileira para a Transformação Digital (E-Digital), instituída em 2018, também buscou fomentar o avanço das tecnologias digitais, incluindo a inteligência artificial, mas não contemplou um marco regulatório específico para sua aplicação em segurança pública. A Estratégia Brasileira de Inteligência Artificial (EBIA), lançada posteriormente, representou um passo à frente ao reconhecer a necessidade de regulamentação, mas ainda não estabeleceu diretrizes claras para o reconhecimento facial, demonstrando que o Brasil segue atrasado na estruturação de normativas que garantam governança e transparência na aplicação dessa tecnologia.

Dentre as iniciativas mais recentes, destaca-se o Projeto de Lei nº 1515/2022, que propõe a criação de uma Lei Geral de Proteção de Dados Pessoais para fins de segurança pública, defesa nacional e persecução penal. O projeto busca preencher lacunas deixadas pela LGPD, estabelecendo parâmetros específicos para o uso de dados biométricos e decisões automatizadas no setor público. No entanto, ainda há pontos críticos a serem aprimorados, especialmente no que diz respeito à exigência de autorização judicial para o tratamento de dados

sensíveis e à proibição de decisões exclusivamente automatizadas, que podem comprometer a eficiência da tecnologia em operações de segurança.

4.1.4. Caminhos para um marco regulatório eficiente

A inexistência de um marco regulatório específico para o reconhecimento facial compromete a confiança pública e aumenta o risco de uso indevido da tecnologia. A criação de uma legislação federal que estabeleça diretrizes padronizadas para a aplicação desse recurso na segurança pública é essencial para mitigar riscos e assegurar a proteção dos direitos fundamentais. Conforme destacado por Araújo, Cardoso e Paula (2020), a falta de regulamentação específica no âmbito federal potencializa o desrespeito à igualdade e coloca em risco garantias e direitos constitucionalmente previstos.

A regulação do uso dos dados biométricos no Brasil deve seguir três pilares fundamentais: transparência, supervisão e responsabilização. A exigência de auditorias periódicas e testes de viés algorítmico permitiria um monitoramento contínuo da eficácia dos sistemas, reduzindo falhas e prevenindo impactos discriminatórios. A criação de uma autoridade reguladora independente, responsável por fiscalizar o uso da tecnologia e garantir que as normas sejam seguidas, fortaleceria o controle social sobre sua implementação. Além disso, a definição de penalidades para o uso indevido da ferramenta contribuiria para a responsabilização de órgãos públicos e privados, garantindo que a tecnologia seja empregada dentro de parâmetros éticos e legais. Melo e Serra (2022) apontam que, em um país marcado pelo racismo estrutural, é crucial que as tecnologias digitais aplicadas à segurança pública considerem as possíveis implicações éticas, sociais, políticas e culturais, evitando a perpetuação de violências contra grupos historicamente discriminados.

Araújo, Cardoso e Paula (2020) também ressaltam que a ausência de legislação específica, aliada à utilização de algoritmos suscetíveis a erros, potencializa o desrespeito à igualdade e coloca em risco garantias e direitos fundamentais constitucionalmente previstos. Referências estrangeiras reforçam que a adoção de um marco regulatório equilibrado é essencial para permitir que a inovação tecnológica avance sem comprometer os direitos fundamentais dos cidadãos. O Brasil, ao estruturar sua legislação sobre RF, pode se beneficiar das diretrizes já estabelecidas por países como os Estados Unidos e a União Europeia, garantindo que sua implementação ocorra de maneira ética, segura e socialmente responsável.

4.1.5. Análise Crítica ao Projeto de Lei nº 1515/2022: Limitações à Ação das Forças de Segurança e Impactos na Inovação

Conforme análise do Laboratório de Políticas Públicas e Internet (LAPIN), o Projeto de Lei nº 1515/2022 surge como uma tentativa de suprir a lacuna deixada pela LGPD, propondo diretrizes específicas para o tratamento de dados pessoais no contexto da segurança pública, defesa nacional e persecução penal. No entanto, embora represente um avanço na regulamentação dessas tecnologias, o projeto apresenta pontos críticos que podem limitar tanto a atuação das forças de segurança quanto a inovação tecnológica no setor.

A mesma Nota Técnica do LAPIN destaca um dos aspectos mais debatidos que é a exigência de autorização judicial para o tratamento de dados sensíveis, incluindo biometria facial. Embora essa medida busque garantir maior controle e proteção à privacidade, sua aplicação rígida pode comprometer a eficiência das operações de segurança pública, especialmente em situações emergenciais que demandam respostas rápidas. O tempo necessário para obtenção de autorizações judiciais pode se tornar um entrave operacional, reduzindo a eficácia de investigações e ações policiais baseadas em tecnologia.

Além disso, o projeto proíbe decisões exclusivamente automatizadas, exigindo que qualquer análise realizada por inteligência artificial passe por validação humana. Essa restrição impacta diretamente a utilização de sistemas de reconhecimento facial em tempo real, pois impede que a tecnologia opere de maneira autônoma para identificar suspeitos ou padrões criminosos em grandes volumes de dados. Embora a supervisão humana seja fundamental para evitar vieses algorítmicos e garantir maior confiabilidade, a exigência absoluta de intervenção humana pode sobrecarregar as forças de segurança e reduzir a agilidade nas operações.

Outro ponto que merece atenção é a rigidez nas regras de compartilhamento de dados entre órgãos públicos e entidades privadas. O projeto estabelece que qualquer transferência de informações entre diferentes instituições exige justificativa detalhada e, em alguns casos, autorização judicial. Essa burocratização pode dificultar a cooperação entre diferentes forças de segurança, limitando a integração de bancos de dados e a interoperabilidade entre sistemas de inteligência. Como consequência, a falta de um fluxo eficiente de informações pode comprometer investigações criminais e ações conjuntas que dependem da troca de dados entre diferentes instituições.

A regulamentação proposta também estabelece limites para o armazenamento de dados biométricos, exigindo sua eliminação após o cumprimento da finalidade para a qual foram

coletados. Castro e Paula (2021) apontam que a referida exigência pode ser problemática em casos de investigações de longo prazo, onde a preservação de registros históricos é essencial para a análise de padrões criminais e a identificação de indivíduos reincidentes. A inexistência de uma cláusula que permita o armazenamento estendido de dados para fins estratégicos de segurança pode prejudicar a continuidade e eficácia das investigações, além de dificultar a criação de bases de dados nacionais integradas.

Outro aspecto relevante do projeto é a exigência de relatórios de impacto à proteção de dados para qualquer operação que envolva o uso de tecnologias sensíveis, como o monitoramento biométrico facial. Embora essa medida tenha como objetivo garantir maior transparência e controle sobre o uso da tecnologia, sua aplicação indiscriminada pode gerar um excesso de burocracia, dificultando a adoção e implementação de novas soluções tecnológicas. A ausência de critérios claros sobre quando e como esses relatórios devem ser exigidos pode aumentar a carga administrativa das forças de segurança, sem necessariamente melhorar a proteção dos direitos fundamentais.

Diante desses desafios, o Projeto de Lei nº 1515/2022 necessita de ajustes para equilibrar segurança pública, inovação tecnológica e proteção de direitos fundamentais. A inclusão de mecanismos mais flexíveis para o tratamento de dados em situações emergenciais, aliada à definição de critérios mais objetivos para o uso de decisões automatizadas, pode garantir maior eficiência operacional sem comprometer a proteção da privacidade. Além disso, a criação de exceções para o compartilhamento de dados entre órgãos de segurança e a possibilidade de armazenamento prolongado de informações essenciais são aspectos que merecem ser revisados para tornar a regulamentação mais funcional e alinhada às necessidades do setor.

Práticas adotadas globalmente demonstram que a regulação do reconhecimento facial deve ser baseada em princípios de transparência, auditoria contínua e governança responsável, sem impedir o avanço da inovação ou limitar a capacidade operacional das forças de segurança. Para que o Brasil desenvolva um marco regulatório eficaz e equilibrado, é fundamental que a legislação adote uma abordagem pragmática, assegurando que a tecnologia seja utilizada de forma ética, mas sem comprometer sua aplicabilidade prática na segurança pública.

5. Metodologia

O presente estudo adota uma abordagem qualitativa e exploratória, baseada na análise documental e na revisão sistemática da literatura, seguindo os protocolos PRISMA (*Preferred*

Reporting Items for Systematic Reviews and Meta-Analyses). A escolha dessa metodologia justifica-se pela necessidade de compreender as lacunas regulatórias e os desafios éticos do reconhecimento facial na segurança pública brasileira, estabelecendo conexões entre normativas nacionais e internacionais e a produção acadêmica sobre o tema.

A abordagem qualitativa permite explorar aspectos normativos, jurídicos e sociais do uso da tecnologia, enquanto a análise documental possibilita uma avaliação crítica das diretrizes regulatórias e normativas aplicáveis. A revisão sistemática foi utilizada para garantir a abrangência e rigor científico da pesquisa, identificando padrões e tendências nos estudos existentes.

5.1. Processo de Levantamento do Referencial Teórico

O levantamento bibliográfico foi conduzido no Portal de Periódicos da CAPES, utilizando descritores selecionados conforme a Tabela 1. Foram empregados critério de inclusão e exclusão rigorosos, considerando artigos revisados por pares e documentos publicados em português e inglês visando garantir a qualidade acadêmica do material analisado.

A busca inicial retornou 15.431 resultados, que foram refinados por meio de filtros de relevância, idioma (português e inglês) e revisão por pares, resultando em 5.458 documentos válidos conforme demonstrado na Tabela 1.

Tabela 64- Resultado Pesquisa Portal Capes

ID_RIS	PARÂMETRO (descritores e palavras-chave)	RESULTADOS	APÓS FILTRO (Revisado por pares e Português e Inglês)
A	inteligência artificial	7.080	
B	reconhecimento Facial	308	188
C	inteligência artificial and reconhecimento Facial	8	3
I	artificial intelligence and facial recognition	7.648	4.996
F	artificial intelligence and facial recognition and public safety	27	16
D	reconhecimento Facial and segurança pública	5	5
E	reconhecimento Facial and política pública	5	5
G	facial recognition and public safety	166	101
H	facial recognition and public policy	184	144
TOTAL		15.431	5.458

Fonte: Elaborado pelo autor

5.2. Processo de seleção e refinamento das fontes

As linhas A e I da Tabela 1 foram excluídas, pois tratavam de aspectos gerais da inteligência artificial, sem conexão direta com aplicação específica do RF na segurança pública. Após essa etapa, 462 artigos foram exportados no formato RIS e importados para o software *Mendeley* Desktop, onde foi realizada a eliminação de duplicatas. Esse processo resultou em 200 artigos únicos, que foram analisados por título e resumo, culminando na seleção final de 158 documentos para análise detalhada.

Além da pesquisa acadêmica, a metodologia incluiu documentos técnicos, normativos e governamentais de relevância nacional e internacional, ampliando o escopo da investigação. Foram analisados, entre outros: o Decreto nº 63.552/2024 (*Smart Sampa*), que regulamenta o uso de câmeras de monitoramento em São Paulo, estabelecendo diretrizes para a implementação ética e transparente dessa tecnologia; a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), que serve como referência para o tratamento de dados pessoais no Brasil, embora exclua explicitamente questões de segurança pública; e as Diretrizes da União Europeia (*Artificial Intelligence Act*). A análise documental permitiu construir um marco comparativo entre as regulamentações vigente no Brasil e as diretrizes internacionais, possibilitando um diagnóstico crítico sobre os desafios regulatórios e éticos do uso da tecnologia na segurança pública.

Formatado: Fonte: (Padrão) Arial, 12 pt, Itálico

Formatado: Normal

5.3. Aplicação do Protocolo PRISMA

Para assegurar a transparência e o rigor no processo de seleção dos documentos, foram seguidas as etapas do protocolo PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*) amplamente utilizado para as revisões sistemáticas e meta-análises. O PRISMA proporciona um método estruturado e replicável, garantindo a seleção criteriosa de fontes acadêmicas e documentais. A Tabela 2 descreve as etapas do protocolo aplicadas no estudo, evidenciando o processo de refinamento da literatura analisada.

Tabela 72 - Processo de seleção dos documentos pelo protocolo PRISMA

Etapa PRISMA	Descrição	Número de Documentos
1. Identificação	Busca inicial nas bases de dados utilizando os descritores e palavras-chave.	15.431
2. Triagem	Remoção de duplicatas e documentos irrelevantes com base no título e resumo.	5.458
3. Elegibilidade	Aplicação de critérios de inclusão e exclusão: - Revisão por pares - Idioma: Português e Inglês - Relevância temática (IA, reconhecimento facial, segurança pública).	-
4. Inclusão	Documentos selecionados para análise detalhada.	462
5. Exclusão de duplicados	Remoção de documentos duplicados após a triagem.	200
6. Análise de Títulos	Exclusão de documentos com títulos fora do escopo.	158
7. Análise de Resumos	-	158
8. Documentos Finais	-	158

Fonte: Elaborada pelo autor

Esse processo metodológico garantiu a adequação e relevância dos materiais analisados, permitindo uma investigação aprofundada e fundamentada sobre as normativas e os desafios regulatório do RF na segurança pública.

5.4. Seleção e Critérios dos Documentos Analisados

A seleção dos documentos seguiu um modelo de amostragem intencional, conforme descrito por Patton (2015), priorizando fontes diretamente relacionadas ao tema central do estudo. O modelo foi adotado para garantir a inclusão de materiais com profundidade analítica, evitando generalizações estatísticas irrelevantes ao contexto regulatório e jurídico.

Critérios de seleção adotados

Relevância temática: Documentos que abordassem reconhecimento facial, segurança pública ou regulação de inteligência artificial.

Confiabilidade da fonte: Apenas artigos revisados por pares, normativas oficiais e relatórios técnicos de órgãos governamentais foram considerados.

Atualidade: Foram priorizadas publicações dos últimos 10 anos (2014-2024), garantindo a pertinência dos dados analisados.

Triangulação de dados: O estudo cruzou informações de bases acadêmicas, normativas governamentais e documentos institucionais, garantindo uma abordagem metodológica mais robusta possibilitando uma análise mais completa, evidenciando pontos de convergência e divergência entre a teoria acadêmica, a legislação vigente e as recomendações internacionais.

Conforme Creswell (2014), a amostragem intencional é particularmente útil em estudos exploratórios, pois permite a inclusão contínua de novas fontes à medida que a pesquisa avança, garantindo flexibilidade e profundidade analítica.

5.5. Análise dos Dados

A análise dos dados foi conduzida em duas etapas complementares, combinando Revisão Sistemática da Literatura e Análise Documental, conforme detalhado a seguir.

✓ Primeira etapa: Revisão Sistemática da Literatura

A revisão da literatura seguiu as diretrizes do protocolo PRISMA, priorizando estudos que abordassem:

- Regulamentação do reconhecimento facial em diferentes contextos.
- Impactos éticos e sociais da tecnologia.
- Experiências internacionais de governança regulatória.

A primeira etapa possibilitou um mapeamento abrangente do debate acadêmico e normativo, fornecendo subsídios para a análise comparativa entre o Brasil e outros países.

✓ Segunda etapa: Análise Documental

Os documentos jurídicos e normativos foram interpretados utilizando a técnica de análise de conteúdo categorial, conforme Bardin (2011). Foram identificados três eixos principais para a categorização das informações:

- Compatibilidade entre reconhecimento facial e LGPD: Análise das disposições legais que regulamentam o uso de dados biométricos no Brasil e suas implicações para a segurança pública.
- Lacunas regulatórias no Brasil: Avaliação de como a ausência de normas específicas impacta a adoção da tecnologia pelas forças de segurança.
- Modelos de regulamentação internacional: Comparação com legislações de países como Estados Unidos e União Europeia, identificando pontos de convergência e divergência.

A triangulação dos dados permitiu uma visão crítica e aprofundada sobre a regulamentação da tecnologia, evidenciando desafios e oportunidades para a governança digital no Brasil.

5.6. Limitações da Metodologia

Apesar do rigor metodológico adotado, a pesquisa apresenta algumas limitações que precisam ser consideradas:

- Dependência de fontes públicas e acadêmicas: A ausência de dados internos das forças de segurança limita a análise prática do uso da tecnologia.
- Evolução rápida da tecnologia: O campo do reconhecimento facial está em constante transformação, exigindo atualizações contínuas da análise regulatória.
- Variedade normativa no Brasil: As disparidades entre normas federais, estaduais e municipais dificultam a criação de um panorama regulatório unificado.

Mesmo com essas limitações, a metodologia adotada assegura transparência e robustez científica. A aplicação do protocolo PRISMA, aliada à utilização de critérios rigorosos de seleção e análise, fortalece a qualidade e confiabilidade das conclusões apresentadas no estudo.

6. Resultados e discussões finais

A pesquisa investigou a existência de um arcabouço regulatório adequado para garantir o uso eficaz e juridicamente seguro do RF na segurança pública brasileira. A análise demonstrou que o Brasil ainda carece de um marco regulatório consolidado, o que gera insegurança jurídica para os operadores da tecnologia e limitações práticas para sua aplicação no combate ao crime. A ausência de uma regulação federal unificada favorece um cenário fragmentado, permitindo que cada estado e município estabeleça normas próprias, sem garantir

Comentado [MD1]: Tímido e faltou referenciar com autores revisados

um mínimo de segurança operacional para as forças de segurança. Além disso, a comparação internacional evidenciou que os Estados Unidos adotam uma abordagem mais pragmática, permitindo flexibilidade regulatória e garantindo que a segurança pública possa fazer uso da tecnologia sem entraves excessivos. Enquanto a União Europeia classifica o reconhecimento facial como tecnologia de alto risco e impõe restrições rigorosas, nos EUA não há uma legislação federal única, permitindo que estados e municípios desenvolvam normas adaptadas à sua realidade. O modelo norte-americano prioriza a segurança pública e a inovação, evitando exigências excessivas que possam comprometer a agilidade das operações policiais.

Quadro 21- Comparação de normativas para Reconhecimento Facial

Critério	Brasil (LGPD e normativas estaduais)	União Europeia (AI Act)	Estados Unidos (Regulações estaduais)
Base legal	LGPD (sem cobertura para segurança pública)	AI Act	Normas estaduais/localizadas
Risco associado	Indefinido	Tecnologia de alto risco	Variável por estado
Regulação específica	Ausente no nível federal	Estrutura normativa detalhada	Depende da legislação estadual
Proibição parcial?	Não	Sim, em determinados contextos	Sim, em alguns estados

Fonte: Elaborado pelo autor.

6.1. Impactos na segurança pública e na atuação policial

O uso do reconhecimento facial é uma ferramenta estratégica para o combate ao crime, permitindo a rápida identificação de suspeitos, monitoramento de atividades criminosas e otimização de investigações. Contudo, a ausência de um marco regulatório claro tem limitado o seu uso, gerando receios entre agentes da segurança pública sobre possíveis violações legais e insegurança na tomada de decisões operacionais.

Nos EUA, a regulamentação permite que a tecnologia seja usada sem necessidade de autorização judicial em diversos contextos, desde que sejam observadas diretrizes mínimas de transparência e prestação de contas. Já no Brasil, a atual abordagem prioriza excessivamente o direito individual, sem considerar que a criminalidade não obedece a regras. A implementação de um modelo flexível permitiria uma resposta mais ágil e eficaz, garantindo a segurança da população sem comprometer a governança da tecnologia.

7. Conclusões

Dessa forma, este estudo aponta que o Brasil deve buscar um modelo regulatório mais flexível, alinhado às necessidades dos agentes de segurança pública, assegurando transparência e governança, mas sem criar entraves burocráticos que favoreçam a criminalidade. O excesso de regulação pode dificultar o uso da tecnologia e restringir a atuação policial, beneficiando aqueles que não seguem as regras legais. Assim, propõe-se diretrizes regulatórias que equilibrem segurança jurídica, inovação tecnológica e eficácia operacional.

7.1. Diretrizes para um modelo regulatória mais ágil e efetivo

Para que o reconhecimento facial seja utilizado de forma eficiente e juridicamente segura na segurança pública brasileira, torna-se essencial a adoção de um marco regulatório nacional que garanta autonomia operacional às forças de segurança, reduza entraves burocráticos e fortaleça a segurança jurídica dos agentes. A atual ausência de uma legislação unificada resulta em interpretações divergentes e cria um ambiente de incerteza normativa, o que, por sua vez, compromete a previsibilidade e a confiabilidade da tecnologia no combate ao crime.

A experiência internacional demonstra que um modelo regulatório mais flexível e voltado à inovação, como o dos Estados Unidos, oferece maior agilidade às operações de segurança pública sem comprometer a governança da tecnologia. Diferentemente da abordagem europeia, que impõe camadas extensivas de supervisão e auditorias obrigatórias, o modelo norte-americano prioriza a autonomia dos agentes e a eficiência operacional, eliminando barreiras excessivas que possam dificultar o uso estratégico da tecnologia. Dessa forma, o Brasil deve considerar a flexibilização de exigências burocráticas, como a dispensa da necessidade de autorização judicial prévia para o uso da tecnologia em investigações e operações em tempo real. Ao garantir acesso imediato a bases de dados nacionais de identificação e eliminar entraves na integração de informações entre órgãos públicos e privados, seria possível viabilizar um fluxo operacional mais dinâmico e eficaz, permitindo que a tecnologia atue como um diferencial estratégico no combate à criminalidade organizada.

Além disso, a necessidade de auditorias recorrentes e regulação externa deve ser reavaliada para evitar o engessamento da atuação policial. Um modelo mais eficiente poderia prever auditorias apenas em casos de suspeita de uso indevido da tecnologia, garantindo que a fiscalização ocorra de forma direcionada e não represente um entrave à atuação das forças de segurança. A descentralização desse controle para órgãos internos de supervisão contribuiria para um equilíbrio entre governança e eficiência operacional.

Outra medida fundamental para o aprimoramento da regulação do reconhecimento facial é a ampliação do tempo de retenção de dados biométricos. Diferentemente do que ocorre em alguns países europeus, onde há exigências rígidas de eliminação rápida das informações coletadas, uma abordagem mais flexível permitiria que esses dados fossem armazenados por períodos mais longos, garantindo suporte contínuo a investigações criminais e ao rastreamento de suspeitos reincidentes. A criação de um banco de dados centralizado voltado a crimes violentos e organizações criminosas poderia aumentar significativamente a eficácia na identificação de padrões criminosos e na prevenção de novos delitos.

Por fim, a regulamentação deve priorizar a segurança coletiva sem comprometer a liberdade operacional das forças de segurança. O direito à privacidade, embora essencial, não pode ser tratado de forma isolada, sobrepondo-se ao direito fundamental da sociedade à segurança pública. O Brasil deve adotar um modelo regulatório que assegure transparência e governança, mas que, ao mesmo tempo, garanta que a aplicação da tecnologia ocorra sem burocracias excessivas que possam limitar sua eficácia no enfrentamento do crime organizado. Ao seguir um modelo baseado na inovação e responsabilidade, como o dos Estados Unidos, é possível estruturar um marco regulatório que equilibre direitos individuais e a necessidade de atuação eficiente das forças de segurança, garantindo que o reconhecimento facial seja uma ferramenta de apoio e não um obstáculo à proteção da sociedade.

7.2. Reflexão sobre governança digital e a segurança pública

O reconhecimento facial não deve ser tratado como uma ameaça aos direitos fundamentais, mas sim como um instrumento essencial para aprimorar a segurança pública. Ao contrário do modelo europeu, que impõe limites rigorosos ao uso da tecnologia, o Brasil deve seguir um modelo regulatório voltado à proteção da sociedade como um todo, garantindo que a criminalidade não se beneficie de um excesso de restrições legais.

Nos EUA, a regulação da inteligência artificial tem sido guiada pelo princípio da inovação com responsabilidade, assegurando que a tecnologia seja usada com transparência, mas sem limitar a liberdade operacional dos órgãos de segurança. O Brasil deve adotar uma abordagem semelhante, garantindo que o reconhecimento facial seja um aliado da segurança pública, e não um obstáculo burocrático.

7.3. Limitações do trabalho

Apesar de seu rigor metodológico, esta pesquisa não teve acesso a bases de dados operacionais do governo, limitando-se a fontes acadêmicas e documentais. Além disso, a constante evolução da tecnologia de IA exige que a regulamentação seja dinâmica e acompanhe

os avanços do setor. A principal contribuição deste estudo está na defesa de um modelo regulatório que assegure segurança jurídica para as forças de segurança, evitando um arcabouço normativo excessivamente restritivo que possa inviabilizar o uso da tecnologia. Ao invés de um controle baseado na limitação operacional, propõe-se um modelo voltado à liberdade de atuação, eficiência na prevenção ao crime e fortalecimento da segurança pública. Dessa forma, o reconhecimento facial pode ser amplamente utilizado sem comprometer direitos fundamentais, mas garantindo que a tecnologia seja empregada de forma ética e transparente, fortalecendo a segurança coletiva e conferindo autonomia ao trabalho das forças policiais.

Apesar dessas limitações, a pesquisa abre caminho para novas investigações sobre a aplicação do reconhecimento facial na segurança pública brasileira. Um aspecto relevante a ser explorado em estudos futuros é a avaliação de programas já em operação no país, como os implantados na Bahia, em São Paulo ou Distrito Federal, onde a tecnologia tem sido utilizada na identificação de suspeitos em grandes eventos e vias públicas ou em soluções de resolução de crime. A análise desses casos pode fornecer indicadores concretos sobre a eficácia da ferramenta, os desafios enfrentados na sua implementação e os impactos na redução da criminalidade. Além disso, a percepção do Estado sobre a regulamentação da tecnologia, sob a ótica da segurança jurídica e da eficiência operacional das forças de segurança, deve ser aprofundada para alinhar a normatização do reconhecimento facial às necessidades práticas do combate ao crime no Brasil.

REFERÊNCIAS

- AI ACT, Artificial Intelligence Act. Regulamento da União Europeia (UE), v. 1689, 2024.
- ALLEN, G.; CHAN, T. Artificial intelligence and national security. Cambridge, MA: Belfer Center for Science and International Affairs, 2017. Disponível em: <https://csdsafica.org/wp-content/uploads/2020/06/AI-NatSec-final.pdf>. Acesso em: 19 out. 2024.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). Inteligência artificial: conceitos e terminologia. NBR ISO 22989. Rio de Janeiro: ABNT, 2023.
- AZEVEDO, C. P. G. de; LIMA, E. M. B. de; SILVA, F. R. da; et al. Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), novembro de 2022. Disponível em: <https://lapin.org.br>. Acesso em: 18/10/2024.
- BAUER, Martin W.; GASKELL, George. Pesquisa qualitativa com texto, imagem e som: um manual prático. Petrópolis: Vozes, 2002.

Código de campo alterado

BARROSO, L.R. Inteligência Artificial, plataformas digitais e democracia: direito e tecnologia no mundo atual. Belo Horizonte: Fórum, 2024.

Formatado: Inglês (Estados Unidos)

BINNS, R. "Fairness in Machine Learning: Lessons from Political Philosophy." Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency (FAT), 2018.

Formatado: Inglês (Estados Unidos)

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Brasília, DF, 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018.

BRASIL. Câmara dos Deputados. Projeto de Lei n. 4.612/2019. Disponível em: <https://www.camara.leg.br>. Acesso em: 10/11/2025.

BRASIL. Câmara dos Deputados. Projeto de Lei n. 1515/2022. Disponível em: <https://www.camara.leg.br>. Acesso em: 12/2024.

Formatado: Inglês (Estados Unidos)

BRUNDAGE, M.; AVIN, S.; WANG, J.; et al. "Toward trustworthy AI development: mechanisms for supporting verifiable claims." arXiv preprint, 2020. Disponível em: <https://arxiv.org/abs/2004.07213>. Acesso em 12/12/2024.

Código de campo alterado

BUITEN, M. C. Towards intelligent regulation of artificial intelligence. European Journal of Risk Regulation, v. 10, n. 1, 2019. Disponível em: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/AF1AD1940B70DB88D2B24202EE933F1B/S1867299X19000084a.pdf/towards_intelligent_regulation_of_artificial_intelligence.pdf. Acesso em: 15/02/2025.

Código de campo alterado

BUOLAMWINI, J.; GEBRU, T. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." Proceedings of the 1st Conference on Fairness, Accountability and Transparency (FAT), 2018.

BRYSON, J. J. The ethics of artificial intelligence. In: DUBBER, Markus D.; PASQUALE, Frank; DAS, Sunit (Ed.). *The Oxford Handbook of Ethics of AI*. Oxford: Oxford University Press, 2019.

Formatado: Alemão (Alemanha)

CAVOUKIAN, A.; JONAS, J. Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, Canada, 2012.

Formatado: Português (Brasil)

CONSELHO DA UNIÃO EUROPEIA. "ChatGPT in the Public Sector: Overhyped or Overlooked?", European Union, 2023.

Formatado: Inglês (Estados Unidos)

CONSELHO NACIONAL DE JUSTIÇA. O uso da inteligência artificial generativa no Poder Judiciário brasileiro: relatório de pesquisa. CNJ, 2024. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2024/09/cnj-relatorio-de-pesquisa-iag-pj.pdf>. Acesso em: 19/10/2024.

CÓBE, R. M. O. "Rumo a uma política de Estado para inteligência artificial." Revista USP, São Paulo, n. 124. 2020. DOI: <http://dx.doi.org/10.11606/issn.2316-9036.v124i0p37-48>.

CRESWELL, J. W. Projeto de pesquisa: métodos qualitativo, quantitativo e misto. Porto Alegre: Penso, 2014.

CRESWELL, J. W.; CLARK, V. L.P. Designing and conducting mixed methods research. Thousand Oaks, CA: SAGE, 2017.

ESTADOS UNIDOS. Executive Order 13859: Maintaining American Leadership in Artificial Intelligence. 2019. Disponível em: <https://www.presidency.ucsb.edu/documents/executive-order-13859-maintaining-american-leadership-artificial-intelligence>. Acesso em: 15/02/2025.

FINANCIAL TIMES. "Met police use of facial recognition in London surges". Financial Times, 19/10/2024. Disponível em: <https://www.ft.com/content/c33322a7-eba7-4299-8172-4ce1d4e88908>

FLORIDI, L. "Information Ethics: Its Nature and Scope." SIGCAS Computers and Society, v. 36, n. 3, set. 2006. DOI: <https://doi.org/10.1145/1167344.1167352>.

FLORIDI, L. The Ethics of Information. Oxford: Oxford University Press, 2013.

FLORIDI, L. The Fourth Revolution: How the Infosphere is Reshaping Human Reality. Oxford: Oxford University Press, 2014.

FLORIDI, L.; COWLS, J.; BELTRAMETTI, M.; CHATILA, R.; CHAZERAND, P.; DIGNUM, V.; SCHAFER, B. AI4People—An ethical framework for a good AI society. *Minds & Machines*, v. 28, n. 4, 2018. Disponível em: <https://link.springer.com/content/pdf/10.1007/s11023-018-9482-5.pdf>. Acesso em: 15/02/2025.

FREITAS, H. "Câmeras de reconhecimento facial se multiplicam em São Paulo: medida é aposta do governo estadual e da prefeitura para a área da segurança pública." *Veja São Paulo*, São Paulo, 27 maio 2024. Disponível em: <https://vejasp.abril.com.br/cidades/cameras-reconhecimento-facial-sp/>. Acesso em: 02 fev. 2025.

GANDY, O. H. The Panoptic Sort: A Political Economy of Personal Information. Boulder: Westview Press, 1993.

GARGARO, D.; MILLMAN, R. "The pros and cons of facial recognition technology." *ITPro*, 23 jul. 2024. Disponível em: <https://www.itpro.com/security/privacy/356882/the-pros-and-cons-of-facial-recognition-technology>. Acesso em: 19 out. 2024.

GOVERNO DO DISTRITO FEDERAL. Plano de Governo do GDF 2023-2026. Brasília, DF: Governo do Distrito Federal, 2023.

GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. Deep Learning. MIT Press, 2016.

JOHNSON, D. G. "Ethics Online." *Communications of the ACM*, v. 40, n. 1, 1997. DOI: <https://doi.org/10.1145/242857.242867>.

JOHNSON, D. G.; MILLER, K.W. Computer Ethics: Analyzing Information Technology. Upper Saddle River, NJ: Prentice Hall, 2009.

Formatado: Fonte: Português (Brasil), Não Todas em Maiúsculas, Não Expandido por / Condensado por

Formatado: Inglês (Estados Unidos)

Formatado: Português (Brasil)

KEYLESS.IO. "Facial Recognition Applications: Benefits and Challenges." Keyless, 19 out. 2024. Disponível em: <https://keyless.io/blog/post/facial-recognition-applications-benefits-and-challenges>. Acesso em: 19 out. 2024.

Formatado: Inglês (Estados Unidos)

KRIZHEVSKY, A.; SUTSKEVER, I.; HINTON, G. E. "ImageNet classification with deep convolutional neural networks." *Communications of the ACM*, v. 60, n. 6, p. 84-90, 2012.

LAKATOS, E. M.; MARCONI, M. A. *Metodologia do trabalho científico*. São Paulo: Atlas, 1991.

LECUN, Y.; BOTTOU, L.; BENGIO, Y.; HAFFNER, P. "Gradient-based learning applied to document recognition." *Proceedings of the IEEE*, v. 86, n. 11, 1998.

LYON, D. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press, 2001.

MAYER-SCHÖNBERGER, V.; CUKIER, K. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Houghton Mifflin Harcourt, 2013.

MELO, P.; SERRA, P. "Tecnologia de Reconhecimento Facial e Segurança Pública nas Capitais Brasileiras: Apontamentos e Problematisações." *Revista de Estudos de Segurança Pública*, v. 12, n. 3, 2023.

MITCHELL, T. M. *Machine Learning*. McGraw-Hill, 1997.

MITTELSTADT, B.; ALLO, P.; TADDEO, M.; WACHTER, S.; FLORIDI, L. "The ethics of algorithms: Mapping the debate." *Big Data & Society*, v. 3, n. 2, 2016.

O'NEIL, C. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown, 2016.

PATTON, M. Q. *Qualitative research & evaluation methods: integrating theory and practice*. Thousand Oaks, CA: SAGE, 2015.

REDE DE OBSERVATÓRIOS DA SEGURANÇA. "90% das pessoas presas por reconhecimento facial são negras, diz estudo". Centro de Estudos de Segurança e Cidadania (CESeC), 2019. Disponível em: <https://cesecseguranca.com.br/reportagens/90-das-pessoas-presas-por-reconhecimento-facial-sao-negras-diz-estudo/>. Acesso em: 14 fev. 2025.

REDMON, J.; FARHADI, A. "YOLOv3: An Incremental Improvement." arXiv preprint, 2018. Disponível em: <https://arxiv.org/abs/1804.02767>.

RUSSELL, S.; NORVIG, P. *Artificial Intelligence: A Modern Approach*. Prentice Hall, 2016.

Formatado: Inglês (Estados Unidos)

RUSSELL, S. J.; NORVIG, P. *Inteligência Artificial*. Trad. Regina Céilia Simille. Rio de Janeiro: Elsevier, 2013.

SANCHEZ-MORENO, A.; OLIVARES-MERCADO, J.; HERNANDEZ-SUAREZ, A.;

TOSCANO-MEDINA, K.; SÁNCHEZ-PÉREZ, G.; BENITEZ-GARCIA, G. "Efficient Face Recognition System for Operating in Unconstrained Environments." *Journal of Imaging*, v. 7, 2021. DOI: <https://doi.org/10.3390/jimaging7090161>.

Formatado: Inglês (Estados Unidos)

SANTIN, V. F. Controle judicial da segurança pública: eficiência do serviço na prevenção e repressão ao crime. São Paulo: Revista dos Tribunais, 2004.

SÃO PAULO (Prefeitura). Decreto nº 63.552, de 4 de julho de 2024. Cria o Programa Smart Sampa, destinado a promover a adoção de soluções tecnológicas inovadoras e avançadas para a melhoria da gestão pública e o aprimoramento da segurança pública. Disponível em: <https://www.sinesp.org.br/legislacao>. Acesso em: 02 fev. 2025.

SILVA, P. Q. da; ROSA, A. N. de C. S. Reconhecimento Facial Aplicado à Perícia Criminal. ICCyber, 2004.

TAEIHAGH, Araz. "Governance of Artificial Intelligence". *Policy and Society*, v. 40, n. 2, 2021.

Formatado: Inglês (Estados Unidos)

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Regulamento Geral sobre a Proteção de Dados (GDPR). Relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *Jornal Oficial da União Europeia*, L 119, 4 mai. 2016.

VEALE, M.; ZUIDERVEEN BORGESIU, F. Demystifying the draft EU artificial intelligence act — analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, v. 22, n. 4, 2021. Disponível em: <https://arxiv.org/pdf/2107.03721>. Acesso em: 15 fev.2025.

Formatado: Português (Brasil)

WACHTER, S.; MITTELSTADT, B.; FLORIDI, L. Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, v. 7, n. 2, 2017. Disponível em: <https://doi.org/10.1093/idpl/ix005>. Acesso em: 15 fev. 2025.

Formatado: Português (Brasil)

ZHU, X.; RAMANAN, D.; ZHANG, H. "Face Detection, Pose Estimation, and Landmark Localization in the Wild." *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2015.

ZUBOFF, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs, 2019.

RECONHECIMENTO FACIAL: PERCEPÇÕES, DESAFIOS E IMPLICAÇÕES NA SEGURANÇA PÚBLICA DO DISTRITO FEDERAL

Resumo: Este estudo analisa a percepção, os desafios e implicações sobre o uso do reconhecimento facial (RF) pelas forças de segurança pública do Distrito Federal (DF), investigando como a ausência de regulamentação específica e as restrições de proteção de dados impactam suas operações. Com uma abordagem metodológica mista, combinando métodos quantitativos e qualitativos foram coletadas 278 respostas de servidores da Polícia Civil (PCDF) e Militar (PMDF) por meio de questionários, complementadas por entrevistas semiestruturadas com operadores do sistema Horus Persona e análise documental de relatórios técnicos. Os resultados indicam que 69,1% dos respondentes percebem o RF como de "grande impacto" na resolução de casos, com eficácia operacional corroborada por relatos de localização de desaparecidos e pela redução do tempo de busca de um dia para cinco minutos. Contudo, os respondentes percebem que a tecnologia é utilizada apenas esporadicamente (66,1% raramente ou nunca), limitada pela falta de treinamento formal (86%) e preocupações com acurácia (74,8%) e privacidade (18,7%). A triangulação dos dados revelou convergências na eficácia do RF e discrepâncias éticas não captadas quantitativamente, sugerindo tensões entre inovação e direitos fundamentais. A média de 14,3 anos de serviço dos respondentes reflete uma força experiente, enriquecendo as perspectivas. Assim, pode-se concluir que, embora o RF potencialize investigações, a ausência de marco regulatório claro compromete sua adoção por motivos éticos, comprometendo assim, sua eficiência. Tais resultados apontam para a necessidade de consecução de políticas públicas que conciliem privacidade, proteção de dados e respaldo jurídico para os agentes que utilizam essa tecnologia.

Palavras-chave: Distrito Federal, reconhecimento facial, segurança pública, regulamentação, privacidade.

Abstract: This study analyzes the perceptions, challenges, and implications of facial recognition (FR) use by public security forces in the Federal District (DF), Brazil, investigating how the absence of specific regulations and data protection constraints impact their operations. Using a mixed-methods approach, combining quantitative and qualitative methods, 278 responses were collected from Civil Police (PCDF) and Military Police (PMDF) officers through questionnaires, complemented by semi-structured interviews with Horus Persona system operators and documentary analysis of technical reports. Results indicate that 69.1% of respondents perceive FR as having a "high impact" on case resolution, with operational efficacy supported by reports of locating missing persons and reducing search times from one day to five minutes. However, ~~the~~ technology is used sporadically (66.1% rarely or never), limited by a lack of formal training (86%) and concerns over accuracy (74.8%) and privacy (18.7%). Data triangulation revealed convergences in FR efficacy and ethical discrepancies not captured quantitatively, suggesting tensions between innovation and fundamental rights. The respondents' average of 14.3 years of service reflects an experienced workforce, enriching the perspectives. Thus, while FR enhances investigations, the lack of a clear regulatory framework compromises its ethical adoption and efficiency. These findings underscore the need for public policies that reconcile privacy, data protection, and legal support for officers using this technology.

Keywords: Facial recognition, Federal District, public security, privacy, regulation.

1. Introdução

As forças de segurança pública enfrentam o desafio constante de equilibrar eficiência operacional e respeito aos direitos individuais em um cenário de criminalidade cada vez mais complexo. Nesse contexto, o reconhecimento facial (RF) surge como uma ferramenta promissora, ampliando a capacidade investigativa e de monitoramento das polícias. No Distrito Federal (DF), essa prática já é realidade com o sistema Horus Persona, desenvolvido pela Polícia Civil do Distrito Federal (PCDF), que tem contribuído para a redução significativa do tempo de buscas em investigações. Todavia, sua adoção ocorre em um ambiente permeado por incertezas regulatórias, o que levanta questões relevantes sobre privacidade e proteção de dados para o cidadão e respaldo jurídico para os agentes públicos que utilizam essa tecnologia.

O presente trabalho se dedica a compreender como os agentes de segurança pública percebem e utilizam essa tecnologia em seu cotidiano. A partir dessa perspectiva, busca-se responder à seguinte questão: de que forma a ausência de regulamentação específica e as restrições relacionadas à proteção de dados pessoais impactam as operações das forças de segurança no DF? Além disso, pretende-se analisar aspectos como acurácia da tecnologia, eficácia operacional, impacto nas investigações e preocupações regulatórias emergentes.

A relevância deste estudo reside na tentativa de compreender os desafios práticos enfrentados pelos agentes de segurança pública, contribuindo para o desenvolvimento de políticas públicas que conciliem inovação tecnológica e a salvaguarda de direitos fundamentais. Busca-se também oferecer uma visão sobre o perfil dos profissionais que interagem com o RF, o tipo de operações em que a tecnologia é aplicada, as percepções acerca de seu desempenho, confiabilidade, além das preocupações ética e regulatórias associadas. Ademais, o estudo visa captar opiniões e recomendações dos agentes, de modo a subsidiar ajustes e aprimoramentos no uso dessa tecnologia. Ao destacar a perspectiva dos profissionais diretamente envolvidos, busca-se enriquecer o debate acadêmico e oferecer subsídios para o aperfeiçoamento da regulamentação e do uso ético do reconhecimento facial no DF.

O artigo está estruturado em quatro seções principais. Após esta introdução, a revisão de literatura aborda conceitos essenciais sobre reconhecimento facial e segurança pública, estudos de casos no Brasil e em outros países, bem como os desafios regulatórios e éticos relacionados. Em seguida, a seção de metodologia detalha os procedimentos de coleta e análise de dados. A seção de resultados e discussão apresenta e analisa criticamente os dados obtidos. Por fim, a conclusão sintetiza as principais descobertas e propõe recomendações para o aprimoramento da tecnologia e sua regulamentação.

2. Conceito de reconhecimento facial e segurança pública

O avanço da tecnologia digital, especialmente no campo da inteligência artificial (IA), tem provocado transformações significativas nas esferas sociais e institucionais. Entre essas inovações, o reconhecimento facial (RF) desponta como uma das mais debatidas, dada sua relevância para a segurança pública e suas implicações em termos de privacidade e direitos fundamentais. Esta ~~breve revisão teórica~~ ~~referencial teórico~~ visa compreender os conceitos centrais de RF e segurança pública, explorando suas intersecções e desafios no contexto do Distrito Federal.

Historicamente, o RF evoluiu de métodos geométricos simples para sofisticadas redes neurais convolucionais, ~~o que permitiu~~ ~~Parkhi, Vedaldi e Zisserman (2015) destacam que tais avanços ampliaram~~ na precisão das identificações em ambientes complexos ~~(Parkhi, Vedaldi e Zisserman, 2015), e a~~. Atualmente, seu uso se estende desde o desbloqueio de dispositivos móveis até sistemas de vigilância em espaços públicos (MELO; SERRA, 2023). Goodfellow, Bengio e Courville (2016) enfatizam que os avanços em aprendizado profundo (*deep learning*) foram determinantes para elevar a eficácia de tais tecnologias, tornando-se valiosas para a segurança pública. No Brasil iniciativas como o Programa *Smart Sampa*, em São Paulo (Decreto nº 63.552/2024), que integra câmeras inteligentes para monitoramento em tempo real, e o sistema Horus Persona da PCDF, que agiliza investigações ao reduzir significativamente o tempo de buscas (Governo do Distrito Federal, 2023), exemplificam essa tendência.

Entretanto, o uso do RF em segurança pública é permeado por controvérsias. Lyon (2021) discute como a vigilância, por meio da tecnologia como RF, influencia não apenas a segurança, mas também ~~uma~~ as interações sociais e a experiência cotidiana. No contexto do DF, tal análise é pertinente, uma vez que a vigilância tecnológica tem o potencial de redefinir a relação entre Estado e os cidadãos. Complementarmente, Gandy (1993) introduz o conceito de "*Panoptic Sort*", um processo de categorização de indivíduos com base em dados pessoais, o que pode gerar práticas discriminatórias. ~~O conceito é central~~ ~~para~~ o debate, pois destaca riscos relacionados à perpetuação de desigualdades sociais.

2.1. Conceito de Segurança Pública

A segurança pública, de acordo com o artigo 144 da Constituição Federal de 1988, é um dever do Estado, direito e responsabilidade de todos, exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio. A Carta Magna define que a segurança pública deve ser realizada por meio dos órgãos de segurança, como as polícias federal,

rodoviária, civil, militar, corpo de bombeiros, entre outros (BRASIL, 1988). Segundo Santin (2004), a eficácia das políticas de segurança depende da capacidade do Estado em prevenir e reprimir crimes, preservando os direitos fundamentais. Para Barroso (2024), a segurança pública deve ser analisada sob uma perspectiva de direitos humanos, garantindo não apenas a ausência de violência, mas também a proteção da liberdade individual e da dignidade humana.

Além disso, a doutrina clássica do direito entende que a segurança pública não se limita à prevenção do crime, mas também à promoção de um ambiente em que os direitos civis sejam efetivamente garantidos. Para Bitencourt (2001), o conceito de segurança pública deve ser amplamente interpretado, abrangendo a segurança social e institucional.

A segurança pública constitui um pilar essencial para a estruturação das relações sociais e a garantia do bem-estar coletivo, sendo contemporaneamente reconhecida como um direito fundamental nas sociedades democráticas. No contexto brasileiro, esse direito é assegurado pela Constituição Federal, mas sua efetivação enfrenta desafios significativos diante dos elevados índices de violência que posicionam o país entre os mais violentos do mundo (Pereira & Santos, 2023, p. 1). Para compreender esse conceito, é necessário explorar suas dimensões teóricas e práticas, considerando tanto a ausência objetiva de ameaças quanto a percepção subjetiva de segurança entre os cidadãos.

De acordo com Wolfers (1952), a segurança pode ser analisada em duas dimensões complementares: a primeira, de caráter objetivo, refere-se à "ausência de ameaças aos valores adquiridos", enquanto a segunda, subjetiva, está associada à "ausência de medo quanto ao ataque a estes valores". Essa dualidade é particularmente relevante no contexto abordado, que transcende a mera proteção física para abarcar também o sentimento de segurança da população. Segundo Pereira e Santos (2023), no Brasil, essa percepção é constantemente desafiada pela escalada da violência urbana, promovida, em grande medida, pela atuação de facções criminosas que expandiram suas operações para além das fronteiras estaduais e nacionais.

A esse respeito, Costa e Lima (2014), argumentam que segurança pública é "menos um conceito teórico e mais um campo empírico e organizacional que estrutura as instituições e relações sociais em torno da forma como o Estado administra ordem e conflitos sociais". Essa definição destaca a complexidade do tema nas Ciências Sociais, sugerindo que a segurança pública não se limita à repressão do crime, mas envolve a gestão de riscos e a manutenção da ordem em um contexto de diversidade social e territorial. No caso brasileiro, com uma extensão territorial de 8,51 milhões de quilômetros quadrados (Instituto Brasileiro de Geografia e Estatística, 2021), essa gestão torna-se ainda mais desafiadora, especialmente em áreas urbanas onde a violência se intensifica.

2.2. Crescimento Populacional e Aumento dos Riscos

O crescimento populacional no Brasil tem sido um fator agravante no cenário da violência urbana, ampliando os riscos. ~~es~~ Segundo dados apresentados por Pereira e Santos (2023), entre 1996 e 2018, a população brasileira aumentou 32,7%, passando de 157,1 milhões para 208,59 milhões de habitantes, e registrado em 2024 com 212,6 milhões conforme estimativas do IBGE. No mesmo período, o número de homicídios cresceu 43,7%, de 38.894 para 55.914, o que representa uma taxa de aumento 33,64% superior à do crescimento populacional. Esse descompasso evidencia que o incremento demográfico não é acompanhado por uma proporcional capacidade de controle da criminalidade, resultando em uma sobrecarga das instituições responsáveis pela segurança.

A violência urbana, mensurada por indicadores como o número de homicídios, reflete não apenas o crescimento populacional, mas também a sofisticação do crime organizado. Pereira e Santos (2023) apontam ainda que facções ~~como o PCC e o CV~~, ao estruturarem-se com base em hierarquia, controle territorial e práticas de uso da violência, representam uma ameaça crescente à sociedade brasileira. Esse cenário é agravado pela percepção de risco entre os cidadãos, que, conforme Elias (2012), veem a segurança como "um direito e um dever inalienável", constantemente ameaçado em um mundo globalizado.

2.3. A Necessidade de Tecnologia como Compensação

Diante desse contexto de crescimento populacional e elevação dos riscos, o uso de tecnologias surge como uma estratégia indispensável para compensar as limitações da Administração Pública no enfrentamento à criminalidade. Pereira e Santos (2023) destacam que "a utilização de tecnologia e inovação em seus processos e procedimentos tem papel fundamental" para que o Estado combata de forma eficiente as ações do crime organizado. Equipamentos como drones, satélites, câmeras e ferramentas de monitoramento permitem a geração e integração de dados, possibilitando a criação de núcleos de inteligência capazes de articular respostas mais eficazes.

O conceito de cidades inteligentes, abordado por Lacinák e Ristvej (2017), exemplifica essa integração tecnológica, propondo o uso de sistemas interligados para garantir o desenvolvimento sustentável e a segurança urbana. Nesse modelo, a tecnologia não apenas otimiza recursos, mas também fortalece a capacidade do Estado em monitorar e prevenir riscos. Santos, Silveira e Silva (2021) reforçam essa perspectiva ao afirmar que "as novas tecnologias

adotadas contribuem para o aumento da produtividade e, com isso, podem aumentar significativamente a eficiência da atuação policial no enfrentamento ao crime organizado".

Portanto, a incorporação de soluções tecnológicas na segurança pública não se limita a uma resposta reativa à violência, mas constitui uma abordagem proativa para mitigar os efeitos do crescimento populacional, da sofisticação criminal, da globalização do crime e da desigualdade social (Costa & Lima, 2014). A inovação tecnológica, nesse sentido, emerge como um instrumento essencial para equilibrar as demandas de uma sociedade em expansão com a necessidade de proteger seus cidadãos e agentes públicos, promovendo uma gestão mais transparente e eficaz da ordem social.

3. Estudos e casos de aplicação no mundo e no Brasil

No cenário internacional, o uso do RF na segurança pública é amplamente documentado. No Reino Unido, a polícia de Londres realizou 117 operações com essa tecnologia em 2024, segundo o *Financial Times* (2024), gerando debates sobre o *trade off* entre eficácia e privacidade. Nos Estados Unidos, Garrett e Jain (2020) destacam o dilema entre segurança e direitos individuais, com casos de falsos positivos levando a prisões injustas.

Na China, o RF integra um amplo sistema de vigilância pública, considerado o mais avançado e expansivo do mundo. Segundo Batista (2019), o país tem investido massivamente em tecnologias digitais para garantir maior controle e segurança, em especial nas chamadas *smart cities*, onde câmeras inteligentes são instaladas estrategicamente para monitorar o fluxo de pessoas. De acordo com a pesquisa, o sistema de reconhecimento facial na China é projetado para criar uma identidade digital de cada indivíduo. O processo inclui a captura da imagem, o processamento por algoritmos para identificação de características faciais (como distâncias entre olhos, nariz e boca) e o armazenamento dessas informações em bancos de dados para futuras consultas (Batista, 2019).

Um exemplo emblemático é o Sistema de Crédito Social Chinês, que utiliza dados de vigilância para avaliar o comportamento dos cidadãos, premiando boas condutas e penalizando infrações. Embora eficaz na redução de crimes em áreas urbanas densamente povoadas, o sistema levanta preocupações quanto à privacidade e à potencial discriminação de grupos vulneráveis. Além disso, Batista (2019) destaca que o controle massivo pode acarretar efeitos colaterais, como o aumento da desigualdade e o cerceamento das liberdades individuais. Por isso, há críticas internacionais sobre o risco de exportação desse modelo para outros países, o que poderia comprometer princípios democráticos e de direitos humanos.

No Brasil, a adoção pelo setor público, em especial para segurança pública, tem avançado rapidamente, mas ainda carece de regulamentação específica. Um dos estados que mais têm investido na aplicação dessa tecnologia é São Paulo, onde a Polícia Militar iniciou um projeto piloto com câmeras inteligentes equipadas com reconhecimento facial em grandes centros urbanos.

O Decreto nº 63.552, de 4 de julho de 2024 (São Paulo), institui o Programa *Smart Sampa*, destinado a promover a adoção de soluções tecnológicas inovadoras para a melhoria da gestão pública e o aprimoramento da segurança na cidade de São Paulo.

O experimento, implementado no sistema de videomonitoramento do Metrô e em áreas de grande fluxo, busca identificar foragidos da Justiça e prevenir crimes em tempo real. Segundo estudos recentes conduzidos por institutos de pesquisa em segurança pública (Fórum Brasileiro de Segurança Pública, 2023), o uso do RF em São Paulo tem gerado debates sobre eficiência e privacidade, uma vez que a tecnologia ainda apresenta desafios relacionados a vieses algorítmicos e risco de falsos positivos. Além disso, uma lacuna regulatória reforça a importância de se estabelecer diretrizes normativas para garantir o uso ético e eficiente dessas tecnologias, alinhando inovação e direitos fundamentais (Freitas, 2024).

~~O Decreto nº 63.552, de 4 de julho de 2024 (São Paulo), institui o Programa *Smart Sampa*, destinado a promover a adoção de soluções tecnológicas inovadoras para a melhoria da gestão pública e o aprimoramento da segurança na cidade de São Paulo.~~

3.1. Cenário do reconhecimento facial no ambiente público do Distrito Federal: o Horus Persona

No Distrito Federal não é diferente, pode ser identificado como projeto de governo por meio do Plano de Governo do GDF (2023-2026) ~~por meio do~~ qual enfatiza a modernização tecnológica como prioridade, buscando melhorar a segurança pública ampliando o videomonitoramento com câmeras e criação de centros de monitoramento remoto (Governo do Distrito Federal, 2023).

Segundo PCDF (2025), a Polícia Civil do Distrito Federal (PCDF) tem investido, desde o início de 2022, em pesquisas e no desenvolvimento de ações voltadas para o uso de IA. Essa tecnologia está revolucionando a forma como crimes são desvendados no Distrito Federal o que levou à criação do Núcleo de Inteligência Artificial do Instituto de Criminalística (IC) na PCDF. Esse núcleo é composto por peritos criminais especialistas que desenvolvem soluções periciais utilizando IA.

Além do núcleo, a instituição possui outras áreas voltadas para tecnologia que desenvolvem ferramentas avançadas. Um exemplo é a solução Horus Persona, utilizada como referência nesta pesquisa. Trata-se de um sistema que aplica tecnologia avançada de RF para melhorar a eficiência das operações investigativas. Seu grande banco de dados vetorial armazena uma enorme quantidade de dados (6 *terabytes* inicialmente) e já processou mais de 1 milhão de buscas apenas nos primeiros três meses de uso, auxiliando em investigações, buscas por pessoas desaparecidas e identificação de vítimas, ou seja, aplica-se além dos casos criminais (PCDF, 2025).

O Distrito Federal (DF), área territorial de atuação ~~de onde~~ a PCDF ~~atua~~, possui mais de 3 milhões de habitantes e abriga Brasília, a capital política do país. Assim como muitas forças policiais urbanas modernas, a PCDF utiliza tecnologias avançadas para garantir a segurança dos cidadãos e investigar crimes. Entre as inovações adotadas, destacam-se as buscas com IA em vastos bancos de dados policiais, que contêm bilhões de registros, incluindo documentos, fotos, vídeos e outros arquivos digitais. Atualmente, os policiais podem utilizar smartphones oficiais para capturar imagens e realizar buscas instantâneas no banco de dados otimizando a tomada de decisões no local de um evento (PCDF, 2025).

Antes da implementação da solução de RF Horus Persona, a investigação policial enfrentava desafios significativos na identificação de pessoas. A ausência de ferramentas tecnológicas avançadas obrigava a realização manual das operações, demandando elevado tempo e recursos humanos. Esse modo de trabalho apresentava limitações em termos de eficácia e precisão, já que os policiais dependiam de um sistema rudimentar digital e de arquivos físicos, compostos por milhares de fotografias (PCDF, 2025).

A variabilidade natural das características físicas, como alterações no corte de cabelo ou na barba, diminuía as chances de uma verificação precisa. Além disso, a ausência de um dispositivo centralizado, que pudesse organizar e armazenar fotos, características e dados pessoais dos suspeitos, representava uma barreira significativa para a eficiência das operações policiais. A falta de estrutura tecnológica limitava severamente a capacidade dos investigadores de realizarem cruzamentos de dados e análises profundas, essenciais para o avanço das investigações e do reconhecimento de pessoas (PCDF, 2025).

O projeto Horus Persona contou com uma colaboração interdepartamental, envolvendo áreas especialistas em tecnologia e em algoritmos de identificação de pessoas, focado na aplicação de conhecimentos técnicos específicos para a biometria e análise de dados. De um modo geral, a solução envolve a integração de cinco camadas tecnológicas:

1. Desenvolvimento web avançado – utilização de modelo *Single Page Application* (SPA) e *Progressive Web App* (PWA), desenvolvida com *Blazor* e *.NET* da Microsoft permitindo uma experiência de usuário fluida e responsiva e utilizando de tecnologia mobile, possibilitando que as informações ou serviços sejam acessados de qualquer localização acessível em qualquer dispositivo com internet, sem a necessidade de instalação de software adicional;

2. Plataforma e linguagens de programação - a base do desenvolvimento está na plataforma da Microsoft, utilizando *C#* (CSharp) com *.NET Core* e *Blazor WebAssembly*, que ofereceu um ambiente de desenvolvimento robusto, seguro e altamente performático;

3. Técnicas de reconhecimento facial e *machine learning* – emprego de tecnologias avançadas, apoiadas por modelos de aprendizado de máquina e algoritmos de vetorização elaborados em *Python* e cruciais para a análise de imagens, permitindo a identificação precisa de indivíduos, mesmo diante de mudanças nas características físicas;

4. *ElasticSearch* – utilizado como motor para indexação e a busca eficiente dos vetores gerados pelos algoritmos de reconhecimento facial facilitando a rápida recuperação de informações a partir de um vasto banco de fotografias, melhorando significativamente a velocidade e a precisão do processo;

5. Modelos de RF específicos: a aplicação integra representações específicas de identificação, como as bibliotecas *Dlib* e *OpenCV*, que são referências no campo da visão computacional. Os moldes são empregados para otimizar a detecção de faces em diferentes condições de iluminação, expressões faciais e ângulos.

Esses avanços representam, segundo a PCDF (2025), uma transformação significativa no trabalho investigativo ~~da PCDF~~, garantindo mais agilidade e precisão na identificação de suspeitos e na resolução de casos complexos.

A PCDF aproveita, além de seus próprios modelos de *machine learning*, modelos de terceiros para transformar os dados em um formato especial chamado “*embedding*”, conceito este usado pela Elastic (2024) para definir uma forma de converter palavras, frases e outros dados em números que capturam seus significados e relações. Eles representam diferentes tipos de dados como pontos em um espaço multidimensional, onde pontos de dados semelhantes são agrupados mais próximos. Essas representações numéricas ajudam as máquinas a compreenderem e processar esses dados de maneira mais eficaz em que capturam as relações entre diferentes pontos de dados que são armazenados de forma eficiente em grande escala, permitindo buscas nesses dados com extrema rapidez e em tempo real.

Embora o estudo enfatize a importância de explorar o uso destas novas tecnologias assim como de mitigar vieses algorítmicos, a implementação prática da mitigação no sistema Horus Persona ainda não foi avaliada em profundidade, o que pode comprometer a consistência entre a discussão teórica e as conclusões operacionais. Além de tudo, a ausência de regulamentação específica, como observado por Freitas (2024), expõe fragilidades éticas e legais nesse uso.

4. Desafios Regulatórios e Éticos

No Brasil, a Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/2018) classifica dados biométricos como sensíveis, mas não oferece diretrizes específicas para seu uso em segurança pública. Isso cria um vácuo jurídico, como apontado por Doneda (2018), que impacta a segurança dos agentes e dos cidadãos. Floridi (2013) defende que a ética da informação exige uma reavaliação constante das práticas diante de novas tecnologias, especialmente quando envolvem vigilância. Buolamwini e Gebru (2018) demonstraram que sistemas de RF têm taxas de erro mais altas para mulheres e pessoas negras, o que pode ampliar discriminações em contextos policiais. No DF, onde a diversidade populacional é expressiva, esse risco é relevante, mas ainda não foi avaliado. Mittelstadt et al. (2016) reforçam que a opacidade dos algoritmos dificulta a *accountability*, um problema agravado pela falta de auditoria pública sobre sistemas.

Zuboff (2019) introduz o conceito de "capitalismo de vigilância", alertando para o uso comercial e político de dados biométricos, um risco potencial no Brasil diante da ausência de normas claras.

4.1. Vieses e discriminação em sistemas de reconhecimento facial

Vieses em sistemas de inteligência artificial, como os de reconhecimento facial (RF), referem-se a distorções sistemáticas nos resultados dos algoritmos, frequentemente causadas por dados de treinamento enviesados ou decisões de design inadequadas, que podem levar a discriminações contra grupos específicos. No contexto do RF, esses vieses manifestam-se em taxas de erro desproporcionalmente altas para certas populações, como mulheres e pessoas negras, ampliando desigualdades sociais (Buolamwini & Gebru, 2018).

Floridi (2024) argumenta que é imperativo que as soluções de IA sejam desenvolvidas e implementadas com um forte compromisso ético, garantindo que beneficiem toda a sociedade de maneira justa e equitativa.

Formatado: Normal (Web), Justificado, Recuo: Primeira linha: 1,27 cm, Espaço Antes: 0 pt, Depois de: 0 pt, Espaçamento entre linhas: 1,5 linhas, Sem marcadores ou numeração

Mittelstadt et al. (2016) destacam que opacidade dos algoritmos de IA representa um desafio significativo para a responsabilidade e transparência e quando os algoritmos operam como "caixas-pretas", torna-se difícil escrutinar suas decisões e identificar as causas dos vieses. Isso se torna especialmente crítico em aplicações de segurança pública. Assim, é essencial que os desenvolvedores de IA adotem práticas de design transparente e explicável para mitigar os riscos de discriminação e assegurar que as tecnologias sejam utilizadas de forma ética e responsável. A combinação das preocupações levantadas por Buolamwini e Gebru (2018) com os princípios éticos de Floridi (2013) e as recomendações de transparência de Mittelstadt et al (2016) oferece uma base sólida para o desenvolvimento de políticas públicas que promovam o uso justo e ético das tecnologias de RF.

4.2. Síntese e Lacunas no uso ético e regulatório do Reconhecimento Facial

A literatura evidencia que o RF oferece benefícios operacionais, mas sua adoção sem regulamentação robusta gera riscos éticos e legais. No DF, o Horus Persona exemplifica essa dualidade: eficiência investigativa versus incerteza jurídica. Estudos como os de Ferrari (2020) e Taeihagh (2021) sugerem a necessidade de marcos regulatórios que incluam transparência, auditoria e conformidade com normas de proteção de dados, alinhando inovação e direitos fundamentais – uma lacuna que esta pesquisa busca preencher a partir da perspectiva dos agentes. Além das questões legais, a implementação do RF levanta debates éticos complexos, como risco de vigilância em massa em que o uso indiscriminado da tecnologia pode criar um ambiente de monitoramento constante, afetando liberdades individuais e a privacidade dos cidadãos, vies algorítmico e discriminação; ~~possibilitando que p~~ Pesquisas indicam que erros na identificação são mais comuns em determinados grupos, podendo reforçar práticas discriminatórias e abordagens policiais injustas e a falta de transparência e controle público visto que sem um sistema de fiscalização adequado, há risco de uso político da tecnologia ou monitoramento de cidadãos sem justificativa legal.

A adoção de novas tecnologias exemplifica esses desafios transformadores, onde práticas tradicionais de segurança e vigilância são reavaliadas sob a luz de novas capacidades tecnológicas. A ética da informação considera a produção, organização, distribuição e uso da informação como questões morais fundamentais, que requerem atenção crítica e soluções responsáveis (Floridi, 2006). Estamos vivenciando a chamada quarta revolução, em que um complexo ambiente informacional está reformulando nossa realidade, levantando questões éticas e filosóficas fundamentais sobre nossa existência e o mundo que habitamos

Comentado [LJ2]: Não é explicativo. Síntese de qu-é? Lacuna regulatória?

Comentado [SF3R2]: O conteúdo do item sintetiza:

- Benefícios operacionais do RF (ex.: eficiência do Horus Persona).
- Riscos éticos e legais (ex.: vigilância em massa, vieses, falta de transparência).
- Lacunas específicas: ausência de marcos regulatórios (transparência, auditoria, conformidade com proteção de dados) e desafios éticos (discriminação, controle público).

O que acha da nova proposta?

(Floridi,2014). O uso de IA na segurança pública, especialmente no RF, reflete essa nova realidade, e a análise ética desses sistemas exige uma compreensão profunda das novas questões que surgem.

Complementarmente, sistemas como o Horus Persona, que potencializam a segurança pública no DF, enfrentam riscos de cibersegurança devido à ausência de regulamentações específicas. A interconexão de redes e o armazenamento de dados biométricos sensíveis criam vulnerabilidades a ataques, como vazamentos de dados ou *ransomware*, que podem comprometer a privacidade e a confiança pública (Carvalho et al., 2024; Chouraik et al., 2024). A adoção de medidas como criptografia, autenticação robusta e auditorias regulares, previstas em frameworks de cibersegurança, seria essencial para mitigar esses riscos, reforçando a necessidade de um marco regulatório que alinhe inovação, segurança digital e proteção de direitos.

Cyber segurança

5. Método utilizado para a pesquisa

O estudo concentrou-se nos servidores ativos da Polícia Civil do Distrito Federal (PCDF) e da Polícia Militar do Distrito Federal (PMDF), que possuem contato direto ou indireto com tecnologias de RF. Segundo dados do portal de transparência do Governo do Distrito Federal, consultados em janeiro de 2025, e critérios adicionais de seleção, a população de estudo é estimada em cerca de 3.500 profissionais, ativos da Polícia Civil do Distrito Federal (PCDF), da Polícia Militar do Distrito Federal (PMDF) e da Secretaria de Segurança Pública do DF (SSP-DF). O filtro no portal considerou cargos com potencial contato com tecnologias de reconhecimento facial, como agentes, delegados, peritos, e militares em funções operacionais ou de inteligência, enquanto a familiaridade com RF foi inferida com base nas atividades e locais de atuação das unidades pesquisadas. Esse grupo é heterogêneo em termos de cargos, tempo de serviço e familiaridade com a tecnologia, refletindo a ausência de categorização específica para interação com RF no portal.

Optou-se por uma amostragem não probabilística por conveniência, justificada pela facilidade de acesso via e-mails institucionais e pela necessidade de maximizar a participação em prazo restrito. O convite para o questionário foi enviado a todos os servidores da PCDF e a policiais militares e a SSP-DF.

Formatado: Normal (Web), Justificado, Recuo: Primeira linha: 1,27 cm, Espaço Antes: 0 pt, Depois de: 0 pt, Espaçamento entre linhas: 1,5 linhas

Formatado: Fonte: Itálico

Comentado [LJ4]: Se pudesse apresentar um número exato seria melhor. Como foi filtrado no portal? Uma breve explicação seria necessária.

Comentado [SF5R4]: Considerando que número exato extraído do portal não é possível, mas estou reformulando o texto para descrever a forma real que cheguei nesta estimativa, veja se atende ou se deseja outra forma.

Para as entrevistas, utilizou-se uma amostragem intencional, selecionando 4 a 6 participantes com base em critérios de relevância: experiência direta com o Horus Persona e participação na gestão ou desenvolvimento do sistema. Essa escolha assegura uma visão abrangente, contemplando tanto a prática operacional quanto as dimensões técnica e administrativa. A participação foi voluntária, com todos os envolvidos assinando o Termo de Consentimento Livre e Esclarecido (TCLE), em conformidade com a Resolução CNS nº 510/2016 (Brasil, 2016).

Adotou-se uma abordagem metodológica mista, combinando técnicas quantitativas e qualitativas (Creswell & Plano Clark, 2018). O questionário estruturado, distribuído eletronicamente captou percepções sobre uso cotidiano, eficácia operacional e preocupações éticas relacionadas ao RF. ~~Embora-Foi realizada uma~~ amostragem por conveniência ~~cuja de~~ taxa de reposta ~~foi~~ de 7,94%, ~~pela qual~~ buscou-se mitigar vieses diversificando os perfis dos participantes. As entrevistas semiestruturadas aprofundaram aspectos práticos e éticos, e a análise documental forneceu dados técnicos sobre desempenho e conformidade com a LGPD. Tal integração assegurou uma análise robusta e fundamentou recomendações para políticas públicas que conciliem inovação tecnológica e proteção de direitos fundamentais

5.1. Instrumentos de Coleta de Dados

Três instrumentos foram utilizados, complementando-se para atender aos objetivos do estudo:

1. **Questionário Estruturado:** Intitulado "Uso de Tecnologias de Reconhecimento Facial pela Segurança Pública no Distrito Federal", composto por 17 perguntas divididas em seis seções: perfil demográfico, uso do RF, treinamento, percepções sobre eficácia, implicações éticas e sugestões de aprimoramento. Predominaram questões de múltipla escolha com escalas *Likert*, além de duas perguntas abertas. Distribuído via *LimeSurvey* entre fevereiro e março de 2025, com um lembrete após a primeira semana, o instrumento passou por piloto na PCDF.
2. **Entrevistas Semiestruturadas:** Realizadas com 4 participantes, exploraram impacto do RF nas investigações, desafios operacionais e preocupações éticas/regulatórias. Conduzidas virtualmente entre fevereiro e março de 2025, com duração de 30 a 60 minutos.
3. **Análise Documental:** Incluiu registros de atividades e relatórios internos da PCDF e documentos públicos, como o Plano de Governo do GDF 2023-2026. Avaliou-se o

desempenho técnico, práticas de armazenamento de dados e conformidade com a LGPD.

5.2. Procedimentos de Análise de Dados

- **Análise Quantitativa:** Dados do questionário foram processados com estatística descritiva para identificar padrões em variáveis como frequência de uso e percepção de eficácia e testes inferenciais Chi-quadrado, para explorar relações entre variáveis e Análise de Variância – ANOVA (*Analysis of Variance*), para comparar percepções de acurácia entre cargos. Softwares como Excel e *PowerBi* foram utilizados para tabulação e visualização gráfica, assegurando rigor na interpretação.
- **Análise Qualitativa:** As entrevistas foram analisadas por meio da análise de conteúdo categorial (Bardin, 2011), em três etapas: (i) pré-análise; (ii) exploração, com codificação; e (iii) interpretação, com validação por triangulação.

A abordagem mista permitiu complementar os dados do questionário com entrevistas, enriquecendo a compreensão dos impactos, desafios e percepções do uso do RF na segurança pública.

5.3. Indicadores de avaliação

O estudo buscou adotar um conjunto de indicadores de desempenho, divididos em três dimensões principais:

- **Técnica:** analisadas métricas como taxa de acurácia, falsos positivos e falsos negativos, fundamentais para compreender a confiabilidade do sistema. Além disso, o tempo médio de resposta foi avaliado para verificar a rapidez com que a tecnologia processa e fornece informações relevantes para a atividade policial.
- **Operacional:** a análise se concentrou na frequência de uso da tecnologia pelos agentes de segurança, no número de casos solucionados com base na ferramenta e na percepção dos profissionais sobre sua eficácia.
- **Social e ética:** avaliado impacto na privacidade, conformidade com a LGPD e percepções sobre aceitação pública e a necessidade de regulamentação mais detalhada.

A avaliação abrangente garantiu resultados descritivos e comparáveis, contribuindo para formulação de políticas públicas.

5.4. Triangulação dos Dados

A triangulação integrou dados quantitativos, qualitativos e documentais na fase final de interpretação validando achados convergentes e explorando discrepâncias, o que enriqueceu a análise e respondeu à questão central do estudo.

5.5. Limitações Metodológicas

O estudo enfrentou limitações, como taxa de resposta de 7,94%, possivelmente devido à resistência dos servidores, desconhecimento ou sobrecarga operacional, logo a amostragem por conveniência pode ter privilegiado participantes mais familiarizados com o RF. A ausência de dados longitudinais limita a análise de tendências ao longo do tempo. Essas limitações sugerem cautela na extrapolação dos resultados, reforçando a necessidade de estudos futuros com amostras maiores e métodos probabilísticos.

6. Resultados e discussões

Esta seção apresenta os achados da pesquisa para responder à questão central do estudo: de que forma a ausência de regulamentação específica e as restrições de proteção de dados impactam as operações policiais? A análise baseia-se em 278 respostas coletadas até março de 2025, complementadas por entrevistas com operadores de sistemas, incluindo usuários do Horus Persona, e pela análise de relatórios técnicos. Os resultados evidenciam as percepções, experiências e desafios enfrentados pelos servidores na utilização dessa tecnologia, destacando lacunas normativas, implicações operacionais e dilemas éticos.

A discussão que segue não apenas descreve o panorama atual do RF, mas também interpreta seus impactos sobre a eficiência policial, a segurança jurídica e a privacidade dos cidadãos.

6.1. Perfil dos respondentes

A amostra da pesquisa foi composta por 278 profissionais da segurança pública do Distrito Federal, pertencentes a diferentes carreiras da Polícia Civil do Distrito Federal (PCDF) e da Polícia Militar do Distrito Federal (PMDF). O maior grupo de respondentes é formado por Agentes de Polícia (67,63%), seguido por Delegados de Polícia (6,47%), Papiloscopistas (5,40%), Escrivães (3,60%) e Peritos Criminais (3,60%). Também participaram da pesquisa profissionais de patentes militares, como Sargentos, Capitães, Tenentes e Major, conforme apresentado na Tabela 1.

Tabela 84: Distribuição dos respondentes por cargo

Cargo	Frequência	Percentual
Agente de Polícia	188	67,63%
Delegado de Polícia	18	6,47%
Escrivão	10	3,60%
Papiloscopista	15	5,40%
Perito Criminal	10	3,60%
Sargento	12	4,32%
Capitão	4	1,44%
2º Tenente ou 1º Tenente	3	1,08%
Major	7	2,52%
Subtenente	1	0,36%
Tenente-Coronel	1	0,36%
Chefe de Gabinete	1	0,36%
Assessorias Especializadas (jurídica, inteligência etc.)	1	0,36%
Outros	7	2,52%

Fonte: Elaborado pelo autor (Dados da pesquisa 2025)

Além da diversidade de cargos, a amostra apresenta variação importante de faixa etária e tempo de serviço, elementos que enriquecem a análise por influenciarem diretamente a relação dos profissionais com o uso e a aceitação de novas tecnologias, como o reconhecimento facial.

Com relação à faixa etária:

- A maior parte dos respondentes (44,6%) está entre 41 e 50 anos;
- 28,8% têm entre 31 e 40 anos;
- 18,7% têm mais de 50 anos;
- Apenas 7,9% possuem menos de 30 anos.

Já quanto ao tempo de atuação na segurança pública:

- A maior parte dos respondentes (38,8%) atua há até 10 anos;
- 33,8% têm entre 11 e 20 anos de serviço;
- 27,3% têm mais de 20 anos de experiência institucional.

Essas informações indicam que a amostra é formada predominantemente por profissionais com trajetória consolidada, mas com grande proporção de agentes em fase intermediária de carreira, que compõem a linha de frente das operações. Isso é relevante para os objetivos da pesquisa, pois indica que a percepção sobre o uso do reconhecimento facial é formada tanto por experiências acumuladas ao longo dos anos, quanto por contato mais recente

com inovações tecnológicas e normativas, o que pode influenciar a visão crítica — e por vezes ambígua — sobre regulamentação, eficiência e riscos do uso de IA na segurança pública.

6.2. Adoção do Reconhecimento Facial

Os dados coletados revelam um quadro de disseminação parcial da tecnologia de reconhecimento facial no cotidiano operacional das forças de segurança. Embora o tema seja conhecido por grande parte dos profissionais, o uso prático ainda não é plenamente difundido.

Apenas 13,3% dos respondentes afirmaram utilizar a tecnologia regularmente em suas atividades, enquanto 43,5% já fizeram uso ocasional. Um total de 62 participantes (22,3%) nunca teve qualquer contato com o sistema, e 58 (20,9%) declararam ter conhecimento teórico, mas sem uso efetivo.

Esse cenário evidencia que menos de um quarto dos profissionais entrevistados teve contato direto e sistemático com a ferramenta, o que pode estar relacionado à ausência de padronização institucional no uso da tecnologia, além de limitações de acesso e capacitação. Essa hipótese é reforçada por outro dado da pesquisa: apenas 14% dos participantes receberam treinamento formal para operar ou interpretar sistemas de reconhecimento facial.

A entrevista com um agente da PCDF ilustra um caso em que o uso está mais disseminado: ele destaca o sistema Horus Persona, adotado pela PCDF, como “um divisor de águas por ‘descentralizar o acesso à tecnologia’, permitindo sua utilização em diversas frentes — da identificação de suspeitos à localização de pessoas desaparecidas”. Ainda assim, mesmo neste cenário otimista, o entrevistado ressalta a importância da validação humana, apontando que o sucesso da ferramenta depende do “olhar atento dos agentes”. Por outro lado, um perito da PCDF indica um uso mais restrito e técnico da IA, aplicada à análise comparativa de imagens e vídeos, sem integrar bases de dados externas. A experiência dele revela uma adoção especializada, limitada ao contexto pericial, com menor capilaridade nas operações em campo.

6.3. Percepções sobre eficácia e impacto

Apesar da adoção limitada, os profissionais da segurança pública demonstram percepções ~~fortemente~~ positivas quanto à eficácia do reconhecimento facial nas investigações criminais. A maioria dos respondentes, 192 (69,1%), considera que a tecnologia tem grande impacto nas atividades de segurança. Outros 61 participantes (21,9%) enxergam um impacto moderado, enquanto apenas 9% declaram pouco ou nenhum impacto. A Tabela 2 apresenta esta distribuição da percepção.

Tabela 92: Percepção sobre o impacto do reconhecimento facial nas investigações

Opinião declarada sobre o impacto	Frequência	Percentual (%)
Grande impacto	192	69,1
Impacto moderado	61	21,9
Pouco impacto	14	5,0
Nenhum impacto	11	4,0
Total	278	100

Fonte: Dados da pesquisa (2025).

As entrevistas aprofundam essa percepção. Um agente da PCDF relata experiências concretas em que a tecnologia foi decisiva para a solução de casos, como na identificação de um corpo em uma ocorrência sem testemunhas, ou na localização de um idoso desaparecido, cuja identidade foi confirmada rapidamente pelo sistema. Para ele, a tecnologia representa uma ferramenta “indispensável, desde que aliada ao conhecimento dos policiais”.

Do ponto de vista pericial, um perito da PCDF destaca que a IA acelera o processo investigativo, especialmente na análise de imagens e vídeos, mas reforça que seu uso deve ser sempre acompanhado de interpretação técnica fundamentada. Para ele, “o resultado do sistema precisa ser analisado por um perito experiente, pois a prova produzida deve resistir ao contraditório”.

Esses relatos demonstram que, quando empregada de forma crítica e supervisionada, a tecnologia de reconhecimento facial contribui para aumentar a eficiência investigativa, sem substituir o papel fundamental da análise humana e técnica.

6.4. Barreiras operacionais e técnicas

Apesar da alta percepção de impacto do reconhecimento facial nas atividades de segurança pública, os dados revelam uma série de barreiras que limitam a efetiva adoção da tecnologia pelas corporações. Dentre os obstáculos mais significativos, destaca-se a ausência de treinamento institucionalizado: apenas 14% dos respondentes relataram ter recebido capacitação formal para utilizar ou interpretar sistemas baseados em inteligência artificial voltados à identificação facial.

Esse dado é relevante quando cruzado com o fato de que 43,5% dos profissionais já utilizaram a tecnologia ocasionalmente: a exposição sem preparação técnica pode acarretar interpretações imprecisas, uso inadequado e até riscos jurídicos no uso da prova digital. A falta de formação adequada compromete não apenas a operacionalização da ferramenta, mas também sua legitimidade como meio de prova no processo penal.

Nas entrevistas, os dois profissionais consultados reforçam essa preocupação. Um perito da PCDF pontua que, embora o sistema *Peritus* utilizado pela Seção de Perícias de Biometria Forense tenha boa aplicação técnica, ele exige conhecimento especializado:

“A ferramenta é um auxiliar. Os resultados só ganham valor quando analisados por peritos capacitados em técnicas com fundamentação acadêmica e base estatística robusta.” (ENTREVISTADO 1, 2025)

Já um agente da PCDF reconhece o valor do sistema Horus Persona, mas alerta para os limites operacionais impostos por questões técnicas, como qualidade de imagem, condições ambientais e atualização de bases de dados. Ele afirma que, em situações adversas, como baixa iluminação ou ângulos desfavoráveis, a precisão do sistema pode ser comprometida:

“Numa operação com imagens comprometidas, o sistema apresentou dificuldades e a identificação foi feita por métodos tradicionais.” (ENTREVISTADO 2, 2025)

Outro fator que aparece de forma transversal nas falas e nas respostas do questionário é a ausência de fluxos padronizados dentro das instituições. A inexistência de protocolos claros sobre coleta, armazenamento, acesso e uso dos dados produz insegurança jurídica e operacional, além de fragilizar a governança da tecnologia.

6.5. Acurácia, falhas e confiabilidade

A percepção sobre a confiabilidade da tecnologia apresenta nuances importantes. Embora os entrevistados relatem confiança na ferramenta, a maioria dos profissionais expressa preocupações quanto à acurácia e à possibilidade de erros, especialmente falsos positivos. Esse dado é sensível, pois indica que, mesmo havendo reconhecimento da utilidade do sistema, a confiança plena ainda não está consolidada.

As respostas da pesquisa representadas na Tabela 3 indicam que 74,8% dos respondentes identificam a precisão e a acurácia como uma preocupação relevante. Quando questionados diretamente sobre falhas, 43,2% relataram já ter vivenciado ou tomado conhecimento de erros ocasionais em sistemas de reconhecimento facial. Outros 33,4% afirmaram não saber avaliar o nível de acurácia dos sistemas — o que reforça a conclusão anterior sobre a lacuna de formação técnica.

Tabela 103: Preocupações dos respondentes em relação ao uso do reconhecimento facial

Tipo de preocupação mencionada	Frequência	Percentual (%)
Precisão e acurácia do sistema	208	74,8
Implicações legais	88	31,7
Privacidade de dados dos cidadãos	52	18,7
Reação pública negativa (opinião pública)	26	9,4

Fonte: Elaborado pelo autor

A preocupação com a acurácia é majoritária, acima inclusive de temas jurídicos e de privacidade. E a percepção sobre a confiabilidade do sistema é fragmentada: apenas 28% (alta ou muito alta) avaliam positivamente; enquanto 33,4% não sabem opinar o que aponta para um grau elevado de incerteza e possível desconhecimento técnico. O cruzamento com a baixa taxa de treinamento formal (14%) sugere que há uma carência de capacitação técnica que afeta a percepção e o uso consciente da tecnologia.

Nas entrevistas, essa ambivalência também está presente. Um perito da PCDF reconhece que, embora os sistemas com IA sejam úteis para acelerar a análise de vídeos e imagens, não são autossuficientes:

“O sistema tem nível razoável de acurácia, mas não substitui o exame técnico. A validação por um perito é indispensável.” (ENTREVISTADO 1, 2025)

Já um agente da PCDF destaca que, apesar da base de dados do sistema Horus contar com aproximadamente 16 milhões de imagens, o risco de falsos positivos persiste, exigindo validação por parte dos operadores:

“O papel do policial é essencial para validar e interpretar os resultados, garantindo que apenas informações precisas sejam utilizadas.” (ENTREVISTADO 2, 2025)

Ambas as falas convergem na ideia de que, sem supervisão qualificada, o reconhecimento facial pode gerar decisões equivocadas, potencializando riscos éticos, jurídicos e operacionais. Essa constatação reforça a importância da triagem humana especializada, tanto para preservar os direitos fundamentais dos cidadãos quanto para assegurar a credibilidade institucional da tecnologia empregada.

6.6. Questões éticas e jurídicas

A introdução de tecnologias de reconhecimento facial no contexto da segurança pública levanta preocupações éticas e jurídicas relevantes, especialmente quanto à proteção de dados pessoais, à privacidade dos cidadãos, e à legalidade do uso de imagens faciais para fins de identificação criminal, em um país que historicamente convive com desafios estruturais relacionados à seletividade penal.

Os dados da pesquisa indicam que 31,7% dos respondentes demonstraram preocupação com as implicações legais do uso da tecnologia, enquanto 18,7% mencionaram diretamente a questão da privacidade. Ainda que essas proporções sejam inferiores à preocupação técnica

com acurácia (74,8%), elas não devem ser minimizadas, especialmente por estarem presentes no discurso de profissionais com experiência prática consolidada.

Nas entrevistas, as visões se complementam. O agente da PCDF acredita que a aplicação utilizada pela PCDF está plenamente em conformidade com a LGPD, e menciona a existência de protocolos internos rigorosos de acesso e armazenamento de dados, baseados em:

- Acesso restrito a pessoal autorizado;
- Armazenamento criptografado;
- Auditorias periódicas de controle.

Por outro lado, o perito apresenta uma percepção distinta. Para ele, não há protocolos específicos e bem definidos sobre o uso de dados no âmbito da perícia. Ele também aponta que a LGPD não se aplica diretamente ao setor de segurança pública, conforme disposto no art. 4º, inciso III da lei. No entanto, reconhece que a ausência de regulamentação complementar provoca insegurança quanto aos fluxos de trabalho e à responsabilidade pelo tratamento de dados sensíveis:

“Como não há regulamentação clara sobre o tema, os fluxos de trabalho não são bem estabelecidos.” (ENTREVISTADO 1, 2025)

Esse descompasso entre a percepção jurídica e a realidade institucional pode refletir uma lacuna normativa e administrativa, que reforça a necessidade de diretrizes específicas para o uso ético, seguro e juridicamente sustentável da tecnologia.

6.7. Necessidade de regulamentação

A ausência de normativas claras e específicas para o uso de tecnologias de reconhecimento facial na segurança pública foi um dos pontos mais mencionados ao longo da pesquisa. Os dados do questionário revelam que:

- 66,5% dos participantes defendem a criação de novas regulamentações, desde que elas não comprometam a eficiência das operações;
- 13,1% acreditam que a regulamentação atual é suficiente;
- Outros 20,4% afirmaram não saber opinar ou demonstraram incerteza quanto ao tema.

Essa ambivalência é reforçada pelo tom das entrevistas. Ambos os participantes consideraram urgente a regulamentação específica da tecnologia, mas com enfoques distintos.

O agente da PCDF entrevistado sugere a adoção de frameworks robustos de governança algorítmica, inspirados em legislações internacionais, como o GDPR (Regulamento Geral de Proteção de Dados da União Europeia) e o EU AI Act, que estabelecem regras sobre:

- Prestação de contas e transparência;
- Auditoria independente de sistemas automatizados;
- Protocolos rígidos de acesso;
- Participação da sociedade civil no processo regulatório.

Ele ainda defende que a atualização do banco de dados facial deve ser realizada com o apoio de convênios institucionais e que o sistema deva incorporar mecanismos de atualização contínua, diante da constante evolução tecnológica.

Já o perito propõe uma regulamentação focada nas especificidades do processo criminal, com ênfase na preservação da cadeia de custódia dos dados, na definição de critérios objetivos para o uso da IA pericial e na previsibilidade legal quanto ao armazenamento e persistência das informações:

“A regulamentação deve prever a aquisição, a manutenção e o uso dos dados conforme a realidade da segurança pública e do processo penal, que muitas vezes tem prazos longos.” (ENTREVISTADO 1, 2025)

Essas contribuições revelam um consenso quanto à importância da regulação, mas também apontam para a necessidade de que ela seja contextualizada, flexível e construída com participação técnica e interinstitucional.

6.8. Integração dos dados: triangulação e síntese final dos achados

A análise conjunta dos dados quantitativos e qualitativos permite afirmar que a incorporação de tecnologias de reconhecimento facial na segurança pública do Distrito Federal ocorre de maneira fragmentada, seletiva e sem uma regulamentação robusta que dê sustentação jurídica e operacional ao seu uso. Essa constatação responde diretamente à questão-problema da pesquisa, que indaga sobre os impactos da ausência de normativas específicas e de diretrizes para proteção de dados pessoais nas práticas institucionais.

Do ponto de vista operacional, observa-se que, embora haja alta percepção de eficácia da tecnologia — com 69,1% dos respondentes considerando seu impacto como grande —, sua adoção prática ainda é limitada: apenas 13,3% afirmam utilizar o sistema regularmente. Essa contradição revela que o reconhecimento facial, apesar de presente institucionalmente, não está plenamente incorporado às rotinas da maioria dos agentes.

Entre as barreiras mais citadas estão a falta de treinamento (86%), a ausência de protocolos claros, e as dificuldades técnicas relacionadas à qualidade das imagens, ângulos desfavoráveis e falsos positivos — elementos que afetam diretamente a confiança dos usuários na ferramenta. Ao mesmo tempo, 74,8% dos participantes demonstram preocupação com a acurácia e confiabilidade do sistema, reforçando a ideia de que não basta a existência da tecnologia; é preciso que ela seja compreendida, testada e validada por profissionais capacitados.

Do ponto de vista ético e jurídico, a pesquisa evidencia um cenário ambíguo: enquanto 31,7% mencionam implicações legais como preocupação e 18,7% apontam questões de privacidade, muitos profissionais (inclusive entrevistados) demonstram desconhecimento quanto à aplicabilidade da LGPD ao setor de segurança pública. A maioria dos respondentes (66,5%) reconhece a necessidade de novas regulamentações, mas teme que essas possam comprometer a eficiência operacional, revelando uma tensão entre efetividade policial e garantias fundamentais.

A triangulação também evidencia disparidades institucionais internas. Enquanto algumas áreas, como a perícia criminal, operam com ferramentas especializadas (caso do *Peritus*), com foco na robustez técnica e na validação humana, outras frentes de atuação, como a investigação de campo, demonstram maior fluidez de uso e protagonismo operacional (como relatado no uso do sistema *Horus Persona*). Em ambas as frentes, contudo, há reconhecimento unânime de que a tecnologia é uma ferramenta auxiliar, que não substitui a análise humana crítica e que exige supervisão contínua, protocolos bem definidos e mecanismos de controle externo.

Em síntese, os dados confirmam que a ausência de regulamentação específica sobre o uso do reconhecimento facial, combinada à carência de formação técnica e de normas internas sobre proteção de dados, gera insegurança operacional e institucional, limitando o uso responsável e ético da tecnologia. A pesquisa indica, portanto, a urgência da construção de diretrizes normativas contextualizadas à realidade da segurança pública brasileira, que equilibrem o avanço tecnológico com o respeito aos direitos fundamentais.

[Discussão: comparar os achados e conclusões com a literatura](#)

7. Conclusões

A presente pesquisa teve como objetivo central analisar como a ausência de regulamentação específica e as restrições relacionadas à proteção de dados pessoais impactam as operações das forças de segurança pública no Distrito Federal, com foco no uso da tecnologia de reconhecimento facial. A partir de uma abordagem método-quantitativa e qualitativa, combinando aplicação de questionário estruturado e entrevistas semiestruturadas, foi possível realizar uma leitura crítica do cenário atual e das percepções dos operadores diretamente envolvidos com essa tecnologia.

Os resultados evidenciam que, embora haja amplo reconhecimento do potencial da tecnologia – com 69,1% dos respondentes apontando impacto positivo na resolução de casos –, o uso prático ainda é limitado: apenas 13,3% afirmam utilizar o sistema regularmente, enquanto a maioria o utiliza de forma ocasional, pontual ou sequer teve contato direto com a ferramenta. Essa dissociação entre expectativa e prática parece diretamente associada a barreiras estruturais como a falta de treinamento (86% dos respondentes), a ausência de protocolos operacionais claros, e a insegurança jurídica decorrente da indefinição normativa.

Adicionalmente, os dados indicam uma preocupação significativa com a acurácia dos sistemas (74,8%), refletindo incertezas sobre a confiabilidade da tecnologia em diferentes condições operacionais. As entrevistas aprofundaram esse ponto ao mostrar que a tecnologia é vista como ferramenta auxiliar, e não como substituta da análise humana, sendo indispensável a validação técnica por peritos ou operadores experientes.

Do ponto de vista jurídico e ético, a pesquisa confirma que há lacunas normativas que dificultam a governança institucional do uso do reconhecimento facial, sobretudo no que diz respeito à proteção de dados pessoais. Ainda que parte dos profissionais entenda que a LGPD não se aplica diretamente à segurança pública (conforme previsto em seu art. 4º), a ausência de normativas complementares específicas gera insegurança, assimetria de práticas e risco de violações de direitos fundamentais.

Diante disso, a pesquisa aponta para a necessidade urgente de construção de marcos normativos próprios, adaptados à realidade operacional das polícias, mas fundamentados em princípios democráticos, respeito à privacidade e controle público. Entre as recomendações destacam-se: a criação de regulamentação específica para uso de reconhecimento facial na segurança pública, com diretrizes claras sobre coleta, armazenamento, acesso e persistência de dados; estabelecimento de protocolos padronizados de uso e validação da tecnologia, compatíveis com o devido processo legal; capacitação contínua e especializada dos

profissionais que operam os sistemas ou lidam com os dados gerados; e, implementação de mecanismos de auditoria e governança, com participação de órgãos independentes e da sociedade civil.

A principal limitação deste estudo reside no recorte geográfico (Distrito Federal), o que restringe a generalização dos achados para outros contextos estaduais. Além disso, a análise qualitativa foi baseada em apenas duas entrevistas, o que limita a variedade de experiências e opiniões coletadas. Entretanto, esses elementos foram compensados por uma amostra quantitativa robusta e pela integração analítica entre os dados.

Para pesquisas futuras, recomenda-se a expansão do estudo para outros entes federativos, com diferentes níveis de adoção tecnológica e de regulamentação vigente, bem como o aprofundamento do debate sobre os impactos sociais e raciais da aplicação do reconhecimento facial no Brasil, dada sua interface direta com temas como discriminação algorítmica, seletividade penal e desigualdades institucionais.

Conclui-se, portanto, que o reconhecimento facial não pode ser tratado apenas como uma inovação técnica, mas como uma ferramenta cujo uso demanda respaldo jurídico, capacitação técnica e controle democrático, sob pena de comprometer não apenas a eficácia das ações policiais, mas a confiança pública no sistema de justiça e na proteção dos direitos fundamentais.

REFERÊNCIAS

BATISTA, Rafael. O uso de tecnologias de reconhecimento facial na segurança pública: desafios e perspectivas. *Revista Brasileira de Segurança Pública*, v. 13, n. 2, p. 45-67, 2019.

BAUER, Martin W.; GASKELL, George. *Pesquisa qualitativa com texto, imagem e som: um manual prático*. Petrópolis: Vozes, 2002.

BARROSO, Luís Roberto. *Inteligência Artificial, plataformas digitais e democracia: direito e tecnologia no mundo atual*. Belo Horizonte: Fórum, 2024. 256p. ISBN 978-65-5518-836-3.

BITENCOURT, Cezar Roberto. *Falência da pena de prisão: causas e alternativas*. 3. ed. São Paulo: Editora Revista dos Tribunais, 2001.

BRASIL. Câmara dos Deputados. *Projeto de Lei n. 4.612/2019*. Dispõe sobre o desenvolvimento, aplicação e uso de tecnologias de reconhecimento facial e emocional, bem como outras tecnologias digitais voltadas à identificação de indivíduos e à predição ou análise de comportamentos. Disponível em:

<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2216455>.

Acesso em: 02 fev. 2025.

BRASIL. Ministério da Saúde. Conselho Nacional de Saúde. Resolução nº 510, de 07 de abril de 2016. Dispõe sobre as normas aplicáveis a pesquisas em Ciências Humanas e Sociais. *Diário Oficial da União*, Brasília, DF, 24 maio 2016. Seção 1, p. 44-46.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17 mar. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*, seção 1, Brasília, DF, 24 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 2014. *Diário Oficial da União*, seção 1, Brasília, DF, 15 ago. 2018.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, v. 81, p. 77-91, 2018.

CARVALHO, L. P. M. A.; SILVA, R. B. Segurança pública, vigilantismo e novas tecnologias: o reconhecimento facial como ferramenta de garantia de direitos. *Ciências Humanas*, [S. l.], v. 29, n. 140, nov. 2024. DOI: 10.69849/revistaft/fa10202411101449. Disponível em: <https://revistaft.com.br/seguranca-publica-vigilantismo-e-novas-tecnologias-o-reconhecimento-facial-como-ferramenta-de-garantia-de-direitos/>. Acesso em: 24 jun. 2025.

CHOURAIK, C.; EL-FOUNIR, R.; TAYBI, K. *Comprehensive review of smart city cybersecurity strategies. International Journal of Applied Research in Social Sciences*, [S. l.], v. 6, n. 9, p. 2112-2120, set. 2024. DOI: 10.51594/ijarss.v6i9.1560. Disponível em: www.fepbl.com/index.php/ijarss. Acesso em: 24 jun. 2025.

Formatado: Fonte: Itálico

COSTA, A. T. M.; LIMA, R. S. Segurança pública. In: COSTA, A. T. M.; LIMA, R. S. (org.). *Crime, polícia e justiça no Brasil*. São Paulo: Contexto, 2014. p. 482-489.

CRESWELL, John W. *Projeto de pesquisa: métodos qualitativo, quantitativo e misto*. 4. ed. Porto Alegre: Penso, 2014.

CRESWELL, John W.; PLANO CLARK, Vicki L. *Designing and conducting mixed methods research*. 3. ed. Thousand Oaks, CA: SAGE, 2018.

DONEDA, Danilo. Lei Geral de Proteção de Dados e o Desafio da Inteligência Artificial. *Revista de Direito do Consumidor*, v. 27, n. 1, p. 11-25, 2018.

ELASTIC. O que são embeddings vetoriais? Disponível em: <https://www.elastic.co/pt/what-is/vector-embedding>. Acesso em: 19 out. 2024.

Formatado: Inglês (Estados Unidos)

ELIAS, L. Desafios da segurança na sociedade globalizada. *Observatório Político*, São Paulo, n. 11, maio 2012.

FERRARI, Valentino. Legal challenges of facial recognition technology in the EU. *Computer Law & Security Review*, v. 36, p. 105394, 2020.

FINANCIAL TIMES. Facial Recognition used in 117 London police operations this year so far. Disponível em: <https://www.ft.com/content/c33322a7-eba7-4299-8172-4ce1d4e88908>. Acesso em: 19 out. 2024.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. *17º Anuário Brasileiro de Segurança Pública*. São Paulo: FBSP, 2023. Disponível em: <https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf>. Acesso em: 17 mar. 2025.

FLORIDI, Luciano. *Information Ethics: Its Nature and Scope*. *SIGCAS Computers and Society*, v. 36, n. 3, p. 21-36, set. 2006. DOI: 10.1145/1167344.1167352.

FLORIDI, Luciano. *The Ethics of Information*. Oxford: Oxford University Press, 2013.

FLORIDI, Luciano. *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford: Oxford University Press, 2014.

FLORIDI, Luciano. A ética da inteligência artificial: princípios, desafios e oportunidades. Curitiba: PUCPress, 2024.

FRANCO, A. S.; SILVA, M. C. Internet das Coisas e Inteligência Artificial: Desafios Éticos e Legais. *Revista de Direito, Tecnologia e Internet*, v. 8, n. 2, p. 77-94, 2020.

FREITAS, Hyndara. Câmeras de reconhecimento facial se multiplicam em São Paulo. *Veja São Paulo*, São Paulo, 27 maio 2024. Disponível em: <https://vejasp.abril.com.br/cidades/cameras-reconhecimento-facial-sp/>. Acesso em: 02 fev. 2025.

GANDY, Oscar H. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder: Westview Press, 1993.

GARRETT, P. M.; JAIN, A. Facial Recognition Technology: Balancing Security and Privacy in the United States. *Journal of Technology Law & Policy*, v. 25, n. 2, p. 123-145, 2020.

GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. *Deep Learning*. Cambridge: MIT Press, 2016.

GOVERNO DO DISTRITO FEDERAL. *Plano de Governo do GDF 2023-2026*. Brasília, DF: Governo do Distrito Federal, 2023.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. Áreas territoriais. Rio de Janeiro: IBGE, 2021. Disponível em: <https://www.ibge.gov.br/geociencias/organizacao-do-territorio/estrutura-territorial/15761-areas-dos-municipios.html>. Acesso em: 31 jul. 2021.

Formatado: Português (Brasil)

LACINÁK, M.; RISTVEJ, J. Smart city, safety and security. *Procedia Engineering*, [S.l.], v. 192, p. 522-527, 2017. DOI: 10.1016/j.proeng.2017.06.090.

LYON, David. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press, 2001.

MELO, P.; SERRA, P. Tecnologia de Reconhecimento Facial e Segurança Pública nas Capitais Brasileiras: Apontamentos e Problematisações. *Revista de Estudos de Segurança Pública*, v. 12, n. 3, p. 45-68, 2023.

MITTELSTADT, Brent; ALLO, Patrick; TADDEO, Mariarosaria; WACHTER, Sandra;

FLORIDI, Luciano. The ethics of algorithms: Mapping the debate. *Big Data & Society*, v. 3, n. 2, p. 1-21, 2016.

Formatado: Inglês (Estados Unidos)

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Agenda 2030*. [S.l.]: ONU, 2015. Disponível em: <https://nacoesunidas.org/pos2015/agenda2030/>. Acesso em: 12 ago. 2021.

Formatado: Inglês (Estados Unidos)

PARKHI, O. M.; VEDALDI, A.; ZISSERMAN, A. Deep Face Recognition. In: *British Machine Vision Conference (BMVC)*, 2015.

Formatado: Inglês (Estados Unidos)

PEREIRA, F. T.; SANTOS, I. C. Tecnologia e inovação na segurança pública: uma lacuna no debate acadêmico. *Revista Ciências Exatas*, Taubaté, v. 29, n. 2, p. 1-21, 2023.

POLÍCIA CIVIL DO DISTRITO FEDERAL. Relatório de gestão interno. Informação sobre o sistema Horus Persona. Brasília, 2025.

SAMPIERI, Hernández Roberto; COLLADO, Carlos Fernández; LUCIO, María del Pilar Baptista. *Metodologia de pesquisa*. Tradução: Daisy Vaz de Moraes. 5. ed. Porto Alegre: Penso, 2013.

SANTIN, Valter Foletto. *Controle judicial da segurança pública: eficiência do serviço na prevenção e repressão ao crime*. São Paulo: Revista dos Tribunais, 2004.

SANTOS, I. C.; SILVEIRA, G. B.; SILVA, R. E. G. Análise da produção científica em tecnologia e inovação no agronegócio. *Research, Society and Development*, [S.l.], v. 10, n. 5, e59210515933, 2021. DOI: 10.33448/rsd-v10i5.15933.

Formatado: Inglês (Estados Unidos)

SANTOS, P. H.; ALMEIDA, J. R. IA no Poder Judiciário e Segurança Pública: Uma Análise Crítica. *Revista de Estudos Judiciários*, v. 19, n. 1, p. 45-68, 2021.

SÃO PAULO (Prefeitura). *Decreto nº 63.552, de 4 de julho de 2024*. Cria o Programa Smart Sampa, destinado a promover a adoção de soluções tecnológicas inovadoras e avançadas para a melhoria da gestão pública e o aprimoramento da segurança pública. Disponível em: <https://www.sinesp.org.br/legislacao>. Acesso em: 02 fev. 2025.

SILVA, Paulo Quintiliano da; ROSA, Antônio Nuno de Castro Santa. Reconhecimento Facial Aplicado à Perícia Criminal. 2004. Disponível em: <http://santacruzadv.com/artigos/anais-iccyber-dpf-2004.pdf#page=176>. Acesso em: 22 dez. 2019.

TAEIHAGH, Araz. Governance of Artificial Intelligence. *Policy and Society*, v. 40, n. 2, p. 205-223, 2021.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016*. Regulamento Geral sobre a Proteção de Dados (GDPR). Relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *Jornal Oficial da União Europeia*, L 119, 4 mai. 2016.

VIEIRA, M. L.; TAKASE, E.; OLIVEIRA, A. M. F. Estratégia Nacional de Inteligência Artificial: O Caminho para a Inovação Responsável. *Revista Brasileira de Inovação*, v. 19, n. 3, p. 123-145, 2020.

WOLFERS, A. National security as an ambiguous symbol. *Political Science Quarterly*, [S.l.], v. 67, n. 4, p. 481-502, 1952. DOI: 10.2307/2145138.

ZUBOFF, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs, 2019.

Considerações Finais

As transformações tecnológicas impulsionadas pela inteligência artificial, especialmente no campo do reconhecimento facial (RF), têm desafiado paradigmas clássicos da segurança pública e do direito à privacidade. A presente dissertação, estruturada no formato *multipaper*, buscou examinar essas transformações sob duas perspectivas complementares: a análise normativa e ética da tecnologia e a percepção prática de seus operadores no contexto da segurança pública do Distrito Federal.

O primeiro artigo evidenciou lacunas regulatórias significativas no Brasil, com destaque para a ausência de um marco legal específico que discipline o uso do reconhecimento facial pelas forças de segurança. Essa carência normativa compromete a previsibilidade jurídica, fragiliza os princípios de governança e gera insegurança para os agentes públicos quanto à legalidade de suas ações. A comparação com experiências internacionais revelou que a União Europeia opta por uma abordagem restritiva e pautada na avaliação de riscos, enquanto os Estados Unidos adotam um modelo mais flexível, voltado à inovação e à autonomia operacional dos estados. A análise crítica desses modelos permitiu propor diretrizes que conciliem eficiência operacional, proteção de dados e respeito aos direitos fundamentais.

O segundo artigo, por sua vez, trouxe uma importante contribuição empírica ao dar voz aos profissionais da Polícia Civil e Militar do Distrito Federal. A pesquisa revelou que, embora os agentes reconheçam o potencial do RF na resolução de crimes e na otimização de investigações — com destaque para a redução do tempo de buscas e localização de pessoas desaparecidas —, sua aplicação prática ainda é esporádica. Fatores como a falta de treinamento, limitações técnicas e, sobretudo, a insegurança jurídica decorrente da ausência de regulamentação foram apontados como principais entraves. A pesquisa revelou ainda uma percepção de que as normas existentes, voltadas prioritariamente à proteção individual, muitas vezes dificultam a adoção de soluções tecnológicas capazes de potencializar a atuação estatal no enfrentamento à criminalidade.

Como síntese dos achados, constata-se que o reconhecimento facial é uma tecnologia estratégica para a segurança pública, mas que sua efetividade está diretamente condicionada à existência de um arcabouço normativo claro, equilibrado e funcional. O Brasil se encontra em um ponto de inflexão: ou avança na criação de diretrizes jurídicas que proporcionem segurança aos operadores e proteção aos cidadãos, ou continuará permitindo que essa lacuna regulatória comprometa tanto a governança quanto a eficácia das ações policiais.

Essa dissertação propõe, portanto, um modelo regulatório que valorize três pilares centrais: transparência, autonomia operacional e responsabilização institucional. Tais diretrizes são fundamentais para garantir que o uso da tecnologia ocorra de forma ética, eficiente e juridicamente segura. A experiência brasileira, particularmente no Distrito Federal, demonstra que é possível combinar inovação tecnológica com respeito às liberdades civis, desde que haja respaldo legal claro e políticas públicas orientadas à qualificação dos agentes e à governança dos sistemas utilizados.

Embora os resultados aqui apresentados representem uma contribuição relevante ao debate público e acadêmico, reconhece-se que o estudo apresenta limitações, especialmente pela indisponibilidade de dados operacionais internos das forças policiais e pela constante evolução tecnológica, que impõe desafios à permanência das conclusões. Ainda assim, os achados desta dissertação oferecem subsídios concretos para o aperfeiçoamento da regulamentação do reconhecimento facial no Brasil e indicam caminhos para futuras pesquisas, incluindo a avaliação de políticas já em curso em estados como São Paulo, Bahia e Distrito Federal.

Conclui-se, portanto, que a construção de um marco normativo brasileiro para o reconhecimento facial não pode prescindir da escuta ativa dos profissionais de segurança pública, tampouco ignorar as boas práticas internacionais. A tecnologia, quando bem regulada, pode se tornar uma aliada poderosa na promoção da segurança coletiva, sem renunciar aos princípios constitucionais que sustentam o Estado Democrático de Direito.