INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA PÚBLICA: O USO DO RECONHECIMENTO FACIAL PARA IDENTIFICAÇÃO DE INFRATORES

Murilo Maffioletti Bada[1], Marlon Oliveira[2]

Resumo: Este artigo explora a aplicação da Inteligência Artificial (IA) na segurança pública, com foco no uso de reconhecimento facial para a identificação de infratores. A pesquisa analisa artigos e revistas científicas publicadas entre 2010 e 2023, com uma revisão integrativa da literatura para avaliar as aplicações, desafios e implicações éticas dessa tecnologia. A análise comparativa entre países desenvolvidos e o Brasil destaca os benefícios e as limitações da implementação dessa tecnologia no contexto brasileiro. Embora o reconhecimento facial ofereça vantagens substanciais, como a rápida identificação de suspeitos e a prevenção de crimes, também apresenta desafios, incluindo o potencial de vieses e erros, além das questões de invasão de privacidade. O estudo conclui que, para o Brasil avançar de maneira saudável e ética na utilização de IA na segurança pública, é essencial investir em infraestrutura tecnológica, capacitação profissional e desenvolvimento de regulamentações robustas que garantam a transparência e a proteção dos direitos individuais.

Palavras-chave: Inteligência Artificial; Segurança Pública; Reconhecimento Facial; Ética.

[1]murilomaffiolettibada@hotmail.com
[2]marlon.oliveira@unesc.net

ABSTRACT: This article explores the application of Artificial Intelligence (AI) in public security, focusing on the use of facial recognition for identifying offenders. The research analyzes articles and scientific journals published between 2010 and 2023, with an integrative literature review to evaluate the applications, challenges, and ethical implications of this technology. The comparative analysis between developed countries and Brazil highlights the benefits and limitations of implementing this technology in the Brazilian context. Although facial recognition offers substantial advantages, such as the rapid identification of suspects and crime prevention. However, it presents challenges, including the potential for biases and errors, as well as privacy invasion issues. The study concludes that for Brazil to advance healthily and ethically in the use of AI in public security, it is essential to invest in technological infrastructure, professional training, and the development of robust regulations that ensure transparency and the protection of individual rights.

Keywords: Artificial Intelligence; Public Safety; Facial Recognition; Ethics.

1 INTRODUÇÃO

Nos últimos anos, a aplicação da inteligência artificial (IA) na segurança pública tem se tornado cada vez mais prevalente, destacando-se o reconhecimento facial como uma ferramenta crucial na identificação e captura de infratores. Essa tecnologia utiliza algoritmos complexos para analisar características faciais de indivíduos em imagens e vídeos, comparando-as com bancos de dados de rostos conhecidos, com o objetivo de identificar e rastrear criminosos, melhorar a segurança em espaços públicos e auxiliar investigações criminais (Negri; Oliveira; Costa, 2020).

Em países desenvolvidos, como os europeus, os Estados Unidos e Hong Kong, o uso do reconhecimento facial na segurança pública é amplamente adotado em diversos contextos. Esta tecnologia é empregada em aeroportos, estações de trem, áreas urbanas e grandes eventos para monitorar multidões em busca de indivíduos procurados (Digital, 2023). Além disso, sistemas de IA são utilizados para analisar padrões de crime e prever áreas e momentos de maior probabilidade de ocorrência. No Brasil, o poder público vem utilizando essas informações para a solução de casos forenses mediante a identificação de suspeitos da prática de crimes (Araujo; Zullo; Torres, 2020).

Apesar dos avanços, a utilização do reconhecimento facial levanta questões éticas, legais e sociais significativas. A precisão dos algoritmos pode variar dependendo de fatores como a qualidade das imagens utilizadas e a diversidade dos rostos presentes nos bancos de dados, o que pode levar a erros de identificação e resultar na criminalização indevida de pessoas inocentes Leardini (2021). Além disso, há preocupações sobre a invasão de privacidade e a vigilância indiscriminada (Araujo; Zullo; Torres, 2020).

O objetivo geral deste trabalho é analisar o uso da IA na segurança pública, com foco específico no reconhecimento facial como ferramenta de identificação de infratores, investigando os possíveis impactos decorrentes dessa tecnologia. Entre os objetivos específicos, destacam-se a definição e conceituação do uso da IA na segurança pública no Brasil, a análise do funcionamento do reconhecimento facial, a avaliação da efetividade dessa tecnologia em países desenvolvidos e a comparação com o Brasil. A justificativa para esta pesquisa reside na necessidade de compreender os benefícios e limitações do reconhecimento facial na segurança pública, bem como seus possíveis impactos negativos (Biondi; Cernev, 2023).

Portanto, este estudo visa fornecer uma análise crítica e abrangente sobre o uso da IA na segurança pública, promovendo uma discussão informada e embasada em evidências sobre os benefícios, desafios e riscos associados a essa tecnologia. Através de uma revisão bibliográfica e de uma análise ética das práticas em diferentes países, pretende-se contribuir para a formulação de políticas e práticas mais justas e equitativas nesse campo.

1.1 SEGURANÇA PÚBLICA NO BRASIL

A tecnologia tem se mostrado fundamental para aumentar a eficácia das iniciativas de segurança pública e gestão de riscos de desastres. Nos últimos anos, as transformações sociais e o avanço das tecnologias da informação e comunicação (TICs) têm redefinido os conceitos de segurança, alterando os modos de vida dos cidadãos e a forma como as instituições enfrentam o crime (Lohn, 2012). Com o desenvolvimento das TICs, avanços tecnológicos foram gradualmente aplicados como ferramentas para resolver problemas e atender às demandas de segurança das populações, visando garantir a prevenção, a tranquilidade e uma melhor qualidade de vida (Flores et al., 2021).

A participação cidadã e comunitária tem sido cada vez mais le-

vada em conta na formulação de políticas públicas de segurança, especialmente na América Latina, onde se busca novas formas de enfrentar e compreender a segurança pública (Lohn, 2012). As TICs se tornaram essenciais na formulação e desenvolvimento de políticas públicas para mitigar os níveis de criminalidade, tornando o Brasil mais técnico na prevenção e punição de crimes (Flores et al., 2021). A noção de segurança cidadã enfatiza a participação dos cidadãos como atores jurídicos e produtores de segurança, complementada por tecnologias que geram redução da incerteza e do risco social (Sela; Soares, 2014).

Entre as tecnologias aplicadas na segurança pública está o aperfeiçoamento constante dos equipamentos policiais. Dispositivos como óculos com minicâmeras acopladas permitem a identificação em tempo real de criminosos foragidos, pessoas desaparecidas ou veículos furtados, aumentando a eficiência das forças policiais (Lohn, 2012). No entanto, a implementação dessas tecnologias também apresenta desafios. A proliferação de dispositivos como caixas eletrônicos, celulares e sistemas de videovigilância adaptados inicialmente para fins militares poderão acarretar em problemas decorrentes do uso destas tecnologias caso estes sejam realizados sem levar em conta as preocupações éticas que circundam o tema (Flores et al., 2021).

A capacidade das forças de segurança pública de combater eficazmente o crime está ligada à percepção pública da legitimidade de suas ações. O uso de tecnologias como câmeras corporais e sistemas de comunicação modernos tem sido uma resposta para garantir a transparência e melhorar a aplicação da lei, prevenindo abusos verbais e agressões e garantindo a proteção dos direitos humanos (Lohn, 2012).

1.2 ATUAÇÃO DOS ÓRGÃOS DE SEGURANÇA

A organização de grandes eventos esportivos apresenta desafios significativos para a segurança pública, demandando inovações tecnológicas e a integração de diversos órgãos de segurança. O Governo Brasileiro, ao criar a Secretaria Extraordinária de Segurança para Grandes Eventos, demonstrou um compromisso em garantir a segurança dos brasileiros e turistas durante a Copa do Mundo de 2014. Uma das maiores inovações deste ministério foi a integração tecnológica de todos os órgãos policiais e de segurança, resultando na criação de uma rede de comunicação exclusiva de alta capacidade, que conectava sedes centrais, estádios, alfândega, patrulhas e a Interpol (Organização Internacional de Polícia Cri-

minal) esta que é uma organização internacional que facilita a cooperação policial mundial e o controle do crime (Sela; Soares, 2014).

Essa integração permitiu que os bancos de dados das forças de segurança brasileiras fossem unificados com os da Interpol, facilitando o compartilhamento de informações críticas. Além disso, o governo brasileiro solicitou dados sobre terroristas ou pessoas que já possuíam certo histórico de comportamento em diversos outros países, como Estados Unidos, Alemanha e Inglaterra, visando prevenir possíveis ameaças (Brasília, 2017).

Um dos principais desafios enfrentados foi a renovação do sistema de telecomunicações e infraestrutura de TIC, essencial para proporcionar comunicação de qualidade e melhorar a gestão dos 12 estádios que sediaram os jogos da copa do mundo de 2014 (Biondi; Cernev, 2023).

A implementação das redes 4G, lançadas comercialmente nas cidades-sede da Copa das Confederações em 2013, foi um passo crucial. Este investimento, que atingiu US$ 111 milhões, visava aumentar a velocidade e a capacidade de resposta das comunicações, permitindo a utilização de aplicações existentes com maior desempenho e a proliferação de novas aplicações (Sela; Soares, 2014). A tecnologia 4G permitiu a consulta rápida a bancos de dados, retornando relatórios abrangentes com imagens e videoclipes, essenciais para a segurança pública (Brasília, 2017).

Além das redes 4G, a comunicação por radiofrequência (RF) foi utilizada prioritariamente dentro das arenas, facilitando a coordenação entre guardas, agentes e cinegrafistas sem sobrecarregar a rede 4G (Brasília, 2017). A empresa Radio Frequency Systems (RFS) forneceu esse serviço, garantindo conectividade estável. Durante a Copa do Mundo de 2014, drones também foram empregados para garantir a segurança dos estádios. A Elbit Systems forneceu drones Hermes 900, operados pela Força Aérea Brasileira, complementando as aeronaves Hermes 450 já em uso para controle aéreo (Sela; Soares, 2014).

A experiência adquirida com a utilização de tecnologia avançada em segurança durante a Copa do Mundo permitiu ao Brasil planejar futuros eventos massivos com maior eficiência. Empresas como o Grupo Risco implementaram sistemas de segurança no estádio Arena Pantanal, em Cuiabá, capazes de identificar tentativas de entrada com ingressos falsos e monitorar áreas internas e externas do estádio Goncalves e Varella (2018). Assim, a visibilidade e a aplicabilidade das inovações tecnológicas reforçaram a capacidade das instituições responsáveis pela segurança no país (Brasília, 2017).

1.3 INTELIGÊNCIA ARTIFICIAL

A inteligência artificial (IA) tem se consolidado como uma ferramenta poderosa e versátil, capaz de executar processos cognitivos de maneira próxima ao raciocínio humano, abrangendo aprendizagem, interação, resolução de problemas e até criatividade (Rai; Constantinides; Sarker, 2019). A aplicação da IA oferece inúmeras possibilidades para melhorar a vida das pessoas em diversos setores, como emprego, educação, saúde e qualidade de vida (Stone et al., 2022).

No contexto da segurança pública, a IA e o *machine learning* têm desempenhado papéis cruciais na compreensão e enfrentamento de crises, identificando padrões e aprimorando a coleta e tratamento de dados (Araujo; Zullo; Torres, 2020). Esses aplicativos mostram o potencial do aprendizado de máquina para prever a evolução dos acontecimentos e contribuir para uma segurança mais eficaz, apesar das restrições e desafios que acompanham sua implementação.

Fundamentalmente, a eficácia da IA na segurança pública está ligada à infraestrutura de dados digitalizados e interoperáveis, que permitem a integração de bancos de dados e a utilização de software baseado em conhecimento (Sela; Soares, 2014). No entanto, a metodologia de treinamento dos sistemas de IA muitas vezes carece de explicação adequada, e a insuficiência de dados pode comprometer a precisão dos modelos, introduzindo vieses que dificultam previsões e detecções precisas (Araujo; Zullo; Torres, 2020).

Machine learning, como subcampo da IA, baseia-se em algoritmos que aprendem com dados para fazer previsões ou tomar decisões, sendo uma ferramenta transformadora em setores como saúde, finanças e segurança pública (Bonaccorso, 2017). Contudo, enfrenta desafios significativos, como vieses nos dados de treinamento e preocupações com a privacidade e a transparência dos algortmos (Biondi; Cernev, 2023).

Entre as aplicações específicas da IA, o reconhecimento facial destaca-se por sua utilização em monitoramento de segurança e identificação de indivíduos, embora enfrente limitações relacionadas à variabilidade populacional e condições de leitura Leardini (2021). A implementação eficaz dessas tecnologias exige uma infraestrutura robusta e processos rigorosos para testar e validar a precisão e a viabilidade das soluções de IA, especialmente no contexto de segurança pública, onde as consequências de falhas podem ser graves (Leardini, 2021).

A capacitação profissional é essencial para garantir o uso res-

ponsável e ético da IA na segurança pública, abordando tanto as competências técnicas quanto as éticas e sociais necessárias para operar essas tecnologias Brigade (2016). Esta capacitação pode trazer benefícios significativos, como melhoria da eficiência dos serviços de segurança e promoção dos direitos humanos, mas também implica desafios como garantir a confiabilidade dos sistemas e evitar discriminações (Biondi; Cernev, 2023).

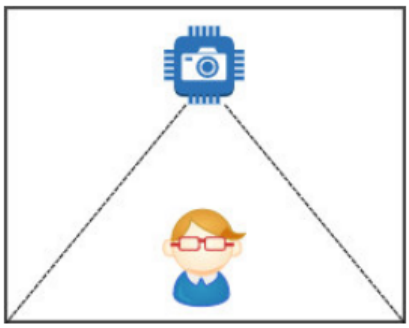
Dessa forma, a presente discussão visa explorar como a IA pode ser utilizada de forma ética e eficaz na segurança pública, destacando tanto as oportunidades quanto os desafios que essa tecnologia apresenta. A IA pode ser uma aliada poderosa na busca por uma segurança mais efetiva e democrática, mas deve ser empregada com critério e responsabilidade para garantir que os direitos e a dignidade das pessoas sejam sempre protegidos (Araujo; Zullo; Torres, 2020).

1.4 PROBLEMAS E DIFICULDADES NO USO DO RECONHECIMENTO FACIAL

Uma das dificuldades da implementação deste tipo de tecnologia, é a necessidade do agente que terá seu rosto lido estar bem posicionado em relação ao leitor como exemplifica o problema a Figura 1, com poucos ou nenhum objeto em seu rosto que dificultem a sua identificação como bonés, óculos, máscaras e etc como exemplifica a Figura 2 (Neto, 2019).

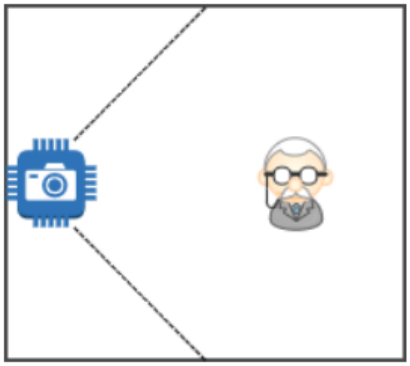
Embora se tenha a consciência que este problema exemplificado pela Figura 2 esteja cada vez menos recorrente devido a melhora da tecnologia com o passar dos anos.

Figura 1 - Um dos exemplos é a posição desfavorável do agente em relação ao leitor.



Fonte: Neto (2019).

Figura 2 - Um segundo exemplo é a presença de objetos no rosto que dificultem a leitura.



Fonte: Neto (2019).

1.5 ÉTICA DA INFORMAÇÃO E INVASÃO DE PRIVACIDADE

Os avanços tecnológicos, especialmente no campo da inteligência artificial (IA), têm levantado importantes questões sobre ética da informação e privacidade. Tais preocupações abrangem diversas áreas, incluindo propriedade intelectual, cibersegurança, liberdade de expressão, privacidade digital, proteção de dados pessoais, desconexão digital, comportamento nas redes sociais e regulação de grandes empresas (Biondi; Cernev, 2023). À medida que tecnologias como IA, Internet das Coisas, realidade virtual e robótica continuam a evoluir, surgem novas oportunidades de negócios e, simultaneamente, dilemas éticos e perigos associados ao uso dessas tecnologias (Goncalves; Varella, 2018).

A sociedade atual está passando por uma revolução digital comparável à revolução industrial, mas com mudanças muito mais rápidas, o que dificulta a assimilação dos riscos e perigos inerentes a essas transformações (Sela; Soares, 2014). Nesse cenário, a ética digital desempenha um papel fundamental na busca por soluções para problemas já existentes e futuros causados pela utilização da Internet e das novas tecnologias. A criação de leis de proteção de dados, por exemplo, tem sido crucial para garantir maior controle e transparência sobre o uso dos dados dos cidadãos (Sela; Soares, 2014).

As leis de proteção de dados, fundamentadas na ética e no respeito à privacidade, buscam garantir que as empresas sejam mais responsáveis e transparentes no processamento de dados pessoais, evitando a invasão de privacidade que antes era comum (Biondi; Cernev, 2023). A ética digital visa assegurar que os dados gerados pelos usuários não sejam explorados indiscriminadamente, prevenindo usos questionáveis que

podem afetar direitos e liberdades fundamentais (Biondi; Cernev, 2023).

Além de cumprir as regulamentações, as organizações devem adotar uma abordagem ética em seus negócios e no impacto que causam na sociedade, antecipando os riscos associados aos novos avanços tecnológicos (Campbell, 2023). A proatividade na proteção de dados e a adoção de medidas de segurança eficazes são essenciais para garantir a privacidade e a segurança no ambiente digital (Sela; Soares, 2014).

A aplicação ética das novas tecnologias é um tema recorrente, especialmente porque o desenvolvimento tecnológico supera a velocidade de criação de leis específicas para sua regulamentação. Portanto, estabelecer princípios éticos para a utilização de tecnologias avançadas é crucial para evitar problemas como os observados no caso da Cambridge Analytica, onde a análise de dados foi utilizada para influenciar eleições e disseminar desinformação (Biondi; Cernev, 2023). A ética digital, portanto, não só protege a privacidade dos usuários, mas também assegura que os benefícios das novas tecnologias sejam plenamente aproveitados de maneira responsável e justa (Sela; Soares, 2014).

Este artigo está organizado em 10 seções, sendo que na Seção 1 está contida a introdução, em suas Subseções constam as seguintes 1.1 Segurança pública no Brasil, 1.2 Atuação dos órgãos de segurança, 1.3 Inteligência Artificial, 1.4 Problemas e Dificuldades no Uso do reconhecimento Facial, 1.5 Ética da informação e invasão de privacidade. Na Seção 2 está contido os trabalhos correlatos, por sua vez na Seção 3 constam os Materiais e Métodos. Logo na Seção 4 os Resultados seguidos pela última e final Seção 5 a Conclusão.

2 TRABALHOS CORRELATOS

Conforme Alexandre (2022) no artigo ”Novos Desafios da Administração Pública: Inteligência Artificial e Ética nos Sistemas Inteligentes com Autonomia”. A União Europeia (UE) tem produzido bastante documentação neste domínio com preocupações centradas na dignidade da pessoa humana e nos direitos fundamentais.

Como cita Flores et al. (2021) no artigo ”A segurança Pública Brasileira no Paradigma do Sistema de Informação”. As questões de segurança pública mudaram o modo de vida dos brasileiros. A história mostra que estes problemas têm raízes antigas e relacionadas ao transferir a família real portuguesa para o nosso país. Na verdade, essas questões são sempre consideradas pela maioria das pessoas, não é preocupação exclu-

siva das agências municipais, estaduais e políticas Federais.

De acordo com Henman (2020) no artigo ”Melhorando os serviços públicos usando inteligência artificial: possibilidades, armadilhas e governança”. Os governos estão a implementar cada vez mais a IA para melhorar a governança pública e a segurança pública. Uma maior utilização de serviços públicos online acarreta maiores riscos de dados violações de proteção e privacidade, bem como desafios mais amplos de segurança cibernética. A IA vem sendo usada para identificar padrões emergentes em tempo real para permitir respostas governamentais e avaliar ataques cibernéticos de negação de serviço ou outras atividades maliciosas de guerra cibernética.

3 MATERIAIS E MÉTODOS

A pesquisa metodológica adota uma abordagem abrangente, focalizando o uso de Inteligência Artificial (IA) na segurança pública, especialmente o reconhecimento facial, tanto em países desenvolvidos quanto no Brasil. Apesar do potencial benefício, limitações financeiras e lacunas regulatórias no Brasil levantam preocupações éticas. O estudo realiza uma revisão integrativa para analisar aplicações práticas, desafios e implicações éticas da IA na segurança, contrastando práticas globais e a realidade brasileira. O objetivo é identificar áreas de investimento e aprimoramento, promovendo o avanço ético e responsável da IA na segurança pública, visando maximizar benefícios e minimizar riscos para a sociedade.

Para a realização da pesquisa metodológica, adotou-se a seleção de artigos e revistas científicas publicados entre 2010 e 2023, foram utilizadas as palavras-chaves: ”segurança pública”, ”inteligência artificial”, ”reconhecimento facial”, ”ética”, ”Brasil”, ”países desenvolvidos”, ”Europa” e ”China” para encontrar os artigos relevantes para escrita deste artigo, foram encontrados e analisados 30 materiais dos quais foram selecionados 23 desses para compor essa pesquisa, entre eles artigos, teses e notícias. A análise destes materiais teve como foco principal o uso de Inteligência Artificial (IA) em países desenvolvidos e no Brasil, com especial ênfase no emprego do reconhecimento facial em investigações criminais e na segurança de grandes eventos.

É importante destacar que, apesar do potencial benefício que o uso de tecnologias de IA pode trazer para a segurança pública, o Brasil pode enfrentar limitações financeiras significativas na implementação dessas tecnologias. Além disso, a regulamentação no país ainda não atingiu

o mesmo nível de maturidade observado em países desenvolvidos, o que levanta preocupações éticas relevantes.

Diante desse contexto, este trabalho analisa criticamente a literatura existente sobre o tema. O objetivo é destacar as aplicações práticas da IA na segurança pública, os desafios enfrentados e as implicações éticas decorrentes do seu uso, tanto em nível nacional quanto internacional.

Os pontos mencionados acima são os objetos de estudo desta pesquisa, que inclui uma análise minuciosa dos dados coletados. Será realizado um contraste entre as práticas adotadas em países desenvolvidos e a realidade brasileira, visando identificar áreas em que o Brasil pode investir, melhorar ou desenvolver suas políticas e tecnologias relacionadas à IA na segurança pública.

É fundamental que o avanço nesta área seja promovido de forma saudável e coesa, respeitando os limites éticos de sua aplicação. Assim, este trabalho busca contribuir para o debate sobre o uso responsável e ético da IA na segurança pública, com o intuito de garantir que seus benefícios sejam maximizados e seus riscos minimizados para toda a sociedade.

4 RESULTADOS

Nos Estados Unidos, o caso de Nijeer Parks, preso injustamente devido a um erro de reconhecimento facial, ilustra as falhas dessa tecnologia. Parks foi detido por crimes graves com base em uma correspondência facial errada, resultante da análise de uma imagem de carteira de motorista falsa. Este incidente destaca as preocupações sobre a precisão da tecnologia, especialmente em relação a pessoas de pele mais escura. Em resposta, alguns estados e cidades dos EUA estão restringindo o uso do reconhecimento facial pela polícia. No Brasil, a situação pode ser diferente, e a comparação dessas práticas é crucial para entender o uso da tecnologia em diferentes contextos jurídicos e sociais (Sarlin, 2021).

Na Europa, há um avanço legislativo significativo em relação ao reconhecimento facial em espaços públicos. Os legisladores europeus aprovaram uma proibição geral da identificação biométrica remota, tanto em tempo real quanto após a captura das imagens, refletindo preocupações crescentes com a privacidade e os direitos individuais (Digital, 2023).

Em Hong Kong, o governo planeja instalar cerca de duas mil novas câmeras de vigilância equipadas com tecnologia de reconhecimento facial. Esta medida levanta preocupações sobre a privacidade e os direitos individuais, especialmente em meio aos debates sobre uma nova lei de

segurança nacional. A implementação dessas câmeras, combinada com a vigilância facial, pode oferecer ao governo uma poderosa ferramenta para monitorar e reprimir dissidentes, exacerbando a repressão política na região (Referencia, 2024).

No Brasil, o uso do reconhecimento facial na segurança pública está em ascensão, com as iniciativas estaduais Rio+seguro e Vídeo policiamento, respectivamente nos estados do Rio de Janeiro e Bahia, iniciativas do tipo são importantes porém estas enfrentam desafios específicos. Limitações financeiras dificultam a implementação de tecnologias de IA em larga escala, enquanto a regulamentação ainda é, de certa forma, precária, resultando em preocupações éticas adicionais, especialmente relacionadas à privacidade e ao uso indiscriminado da tecnologia (Negri; Oliveira; Costa, 2020).

A aplicação do reconhecimento facial baseado em IA na segurança pública tem o potencial de melhorar a eficiência na identificação de infratores e fortalecer as medidas de segurança. No entanto, é crucial abordar os desafios técnicos e éticos associados a essa tecnologia, garantindo que sua implementação seja feita de forma responsável e respeitando os direitos individuais. A comparação entre o contexto dos países desenvolvidos e o Brasil destaca a importância de uma abordagem adaptada às realidades locais, considerando às necessidades e preocupações específicas de cada região (Negri; Oliveira; Costa, 2020).

Os desafios técnicos e éticos do reconhecimento facial são aspectos cruciais a serem considerados diante da sua crescente aplicação na segurança pública. A precisão do sistema é uma preocupação central, uma vez que a identificação errônea de indivíduos pode resultar em graves consequências, como a prisão injusta de inocentes. Além disso, o viés algorítmico merece atenção, pois algoritmos de reconhecimento facial podem apresentar tendências discriminatórias, especialmente em relação a grupos minoritários, levando a uma desproporção no tratamento de diferentes segmentos da sociedade (Araujo; Cardoso; Paula, 2021).

A implementação do reconhecimento facial também suscita preocupações profundas sobre a privacidade e os direitos individuais. A coleta em massa de dados biométricos e a vigilância constante levantam questões sobre a autonomia e a liberdade dos cidadãos, podendo violar direitos fundamentais. A falta de consentimento informado e o uso indiscriminado dessas tecnologias podem minar a confiança pública nas instituições governamentais, sendo essencial estabelecer salvaguardas legais e mecanis-

mos de prestação de contas que garantam a transparência e o respeito aos direitos individuais (Venturini; Garay, 2021).

Outro desafio ético importante é a questão da responsabilidade e da tomada de decisão automatizada. À medida que os sistemas de IA assumem um papel mais proeminente na segurança pública, surgem questões sobre quem é responsável por erros ou abusos cometidos por essas tecnologias. A falta de clareza sobre os papéis e responsabilidades das partes envolvidas pode criar lacunas na prestação de justiça e na reparação de danos causados por decisões baseadas em algoritmos. Portanto, é fundamental estabelecer diretrizes claras e mecanismos de responsabilização para garantir que o uso do reconhecimento facial seja feito de maneira ética e justa (Aras; Pontes; Figueiredo, 2020).

A regulamentação e a legislação são fundamentais na governança do uso do reconhecimento facial na segurança pública. No Brasil, a ausência de uma legislação específica sobre o tema deixa lacunas significativas na proteção dos direitos individuais e na garantia de uma utilização ética e responsável dessa tecnologia. Analisar as melhores práticas adotadas por outros países pode fornecer elementos-chave para a legislação brasileira, como diretrizes claras para o uso do reconhecimento facial, mecanismos de supervisão e salvaguardas para proteger a privacidade e os direitos individuais dos cidadãos (Araujo; Cardoso; Paula, 2021).

A adaptação do reconhecimento facial à realidade brasileira envolve uma consideração cuidadosa das particularidades do contexto nacional, incluindo aspectos socioeconômicos, culturais e jurídicos. Dada a história do país em relação aos direitos humanos e à vigilância estatal, há uma sensibilidade especial em torno da proteção da privacidade dos cidadãos e da prevenção de abusos por parte das autoridades. Qualquer implementação deve ser acompanhada de garantias robustas de transparência, prestação de contas e respeito aos direitos individuais (Venturini; Garay, 2021).

Um debate público aberto e transparente sobre o uso do reconhecimento facial na segurança pública é indispensável para garantir que as decisões reflitam os valores e interesses da sociedade como um todo. Um diálogo inclusivo envolvendo diversos setores é fundamental para avaliar os impactos dessa tecnologia e definir diretrizes adequadas para sua implementação (Alves, 2020).

Por fim, é importante reconhecer que o reconhecimento facial é apenas uma ferramenta em um arsenal mais amplo de estratégias de apli-

cação da lei. Embora ofereça benefícios em termos de eficiência e precisão na identificação de infratores, não deve ser vista como uma solução única para todos os desafios de segurança. Investir em abordagens holísticas e baseadas em evidências para prevenir e combater o crime, levando em consideração tanto as capacidades técnicas quanto as necessidades e preocupações das comunidades locais, é essencial (Alves, 2020).

5 CONCLUSÃO

A utilização da inteligência artificial (IA), especificamente do reconhecimento facial, na segurança pública, tem mostrado grande potencial para melhorar a eficiência e a eficácia na identificação de infratores. No entanto, este avanço tecnológico não está isento de desafios e preocupações significativas.

Além dos desafios técnicos, a questão da privacidade é um ponto crítico. A implementação generalizada de câmeras de reconhecimento facial levanta sérias preocupações sobre a vigilância em massa e a potencial violação dos direitos humanos. A falta de regulamentação específica e robusta, como observado no Brasil, agrava essas preocupações, tornando essencial o desenvolvimento de um marco regulatório que equilibre segurança e direitos individuais.

A comparação entre diferentes contextos internacionais, como os Estados Unidos, a Europa e Hong Kong, revela abordagens variadas e destaca a importância de adaptar as práticas às realidades locais. Enquanto na Europa se observa uma tendência para restringir ou proibir o uso de reconhecimento facial em espaços públicos, em Hong Kong a expansão dessa tecnologia levanta alertas sobre o uso para repressão política. No Brasil, além das barreiras técnicas e financeiras, há uma urgência em criar diretrizes claras que regulem o uso da tecnologia, protegendo a privacidade e os direitos dos cidadãos.

Portanto, a implementação do reconhecimento facial na segurança pública deve ser feita com cautela e responsabilidade. É essencial que as autoridades invistam em melhorar a precisão dos sistemas e em desenvolver regulamentações que garantam transparência, responsabilidade e respeito aos direitos individuais. A criação de um debate público inclusivo e transparente sobre o uso dessa tecnologia é crucial para assegurar que ela seja implementada de forma ética e justa, beneficiando a sociedade sem comprometer as liberdades e os direitos fundamentais dos indivíduos.

Como trabalhos futuros recomenda-se realizar um estudo ético

mais focalizado e aplicado, com métricas e comparações de resultados a fim de elencar pontos de atenção e/ou melhora nos diversos países estudados e principalmente no Brasil.

REFERÊNCIAS

ALEXANDRE, A. d. C. **Novos Desafios da Administração Pública: Inteligência Artificial e Ética nos Sistemas Inteligentes com Autonomia**. Tese (Doutorado) — Instituto Superior de Ciências Sociais e Políticas, 2022.

ALVES, I. S. **Reconhecimento Facial no auxílio à segurança pública da cidade de Florianópolis**. TCC, Florianópolis, 2020. Acesso em: 24 abril 2024. Disponível em: <https://repositorio.animaeducacao.com.br/handle/ANIMA/11998>.

ARAS, J.; PONTES, M.; FIGUEIREDO, P. C. o. **A aplicabilidade da Lei Geral de Proteção de Dados à Administração Pública**. Salvador: Mente Aberta, 2020.

ARAUJO, R. A.; CARDOSO, N. D.; PAULA, A. M. **Regulação e uso do Reconhecimento facial na Segurança Pública do Brasil**. Brasília-DF, 2021. v. 112.

ARAUJO, V. S. D.; ZULLO, B. A.; TORRES, M. **Big data, algoritmos e inteligência artificial na administração pública: reflexões para a sua utilização em um ambiente democrático**. A & C-Revista de Direito Administrativo & Constitucional, 2020. v. 20, n. 80, 241-261 p. Acesso em: 23 jun. 2023.

BIONDI, G. M. C. B.; CERNEV, A. K. **Nuveo: Ética Digital e Inteligência Artificial para Desafios do Mundo Real**. Revista de Administração Contemporânea, 2023. v. 27. Acesso em: 03 Mar. 2023.

BONACCORSO, G. **Machine Learning Algorithms**. Birmingham: Packt Publishing, 2017. Acesso em: 20 Set. 2023.

BRASíLIA. **Relatório de prestação de contas final referente à Copa das Confederações FIFA em 2013 e à Copa do mundo FIFA em 2014**. [S.l.], 2017. Acesso em: 18 Out. 2023. Disponível em: <http://arquivo.esporte.gov.br/arquivos/futebolDireitosTorcedor/copa2014/prestacao_de_contas_copa2014_final.pdf>.

BRIGADE, D. B. **A diferença entre inteligência artificial, machine learning e deep learning**. [S.l.], 2016. Acesso em: 03 Out. 2023. Disponível em: <https://medium.com/data-science-brigade/a-diferen%C3%A7a-entreintelig%C3%AAncia-artificial-machine-learning-e-deep-learning-930b5cc2aa42/>.

CAMPBELL, B. **How AI Can Improve Public Safety**. 2023. <https://aithority.com/machine-learning/how-ai-can-improve-public-safety/>. Acesso em: 29 mar. 2023.

DIGITAL, C. **Europa avança com Lei que proíbe reconhecimento facial em espaços públicos**. [S.l.], 2023. Acesso em: 12 abril 2024. Disponível em: <https://www.convergenciadigital.com.br/Seguranca/Europa-avanca-com-Lei-que-proibe-reconhecimento-facial-em-espacos...-publicos-63199.html?UserActiveTemplate=mobile>.

FLORES, H. S. et al. **A segurança Pública Brasileira no Paradigma do Sistema de Informação.** Revista Ibero-Americana de Humanidades, Ciências e Educação, 2021. v. 7, n. 2, 1020-1037 p. Acesso em: 9 Out. 2023.

GONCALVES, T. C. N. M.; VARELLA, M. **Os desafios da Administração Pública na disponibilização de dados sensíveis**. V. 14 N. 2, MAIO-AGO 2018, 2018. Acesso em: 18 de Out de 2023.

HENMAN, P. **Improving public services using artificial intelligence: possibilities, pitfalls, governance**. Routledge, 2020. v. 42, n. 4, 209-221 p. Acesso em: 29 Out. 2023.

LEARDINI, I. **O uso da inteligência artificial para o exercício do poder de vigilância estatal**. Percurso, 2021. v. 3, n. 40, 95-99 p. Acesso em: 23 jun. 2023.

LOHN, J. M. **Tecnologias aplicadas à segurança pública: livro didático**. Palhoça, 2012. Design instrucional Marina Melhado Gomes da Silva. Disponível em: <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/21949/1/fulltext.pdf>.

NEGRI, S. M. C. d. ; OLIVEIRA, S. R. D.; COSTA, R. S. **O Uso de Tecnologias de Reconhecimento Facial Baseadas em Inteligência Artificial e o Direito à Proteção de Dados**. [S.l.], 2020. v. 17, n. 93. Acesso em: 26 jun. 2023. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3740>.

NETO, L. C. S. **Análise de algoritmos de biometria facial para controle de pessoas em espaços privativos**. Universidade Federal do Maranhão, 2019. Acesso em: 04 Nov. 2023.

RAI, A.; CONSTANTINIDES, P.; SARKER, S. **Next generation digital platforms: toward human-AI hybrids**. Mis Quarterly, 2019. v. 43, n. 1, iii–ix p. Acesso em: 29 Out. 2023.

REFERENCIA, A. **Hong Kong usará milhares de câmeras para aumentar a vigilância sobre seus cidadãos**. 2024. <https://areferencia.com/asia-e-pacifico/hong-kong-usara-milhares-de-cameras...-para-aumentar-a-vigilancia-sobre-seus-cidadaos/>. Acesso em: 12 abril 2024.

SARLIN, J. **EUA: Polícia prende inocente a partir de sistema de reconhecimento facial**. 2021. <https://www.cnnbrasil.com.br/internacional/sistema-de-reconhecimento-facial-enviou-este-homem-inocente-... para-a-prisao>. Acesso em: 12 abril 2024.

SELA, V. M.; SOARES, A. C. d. C. **Os desafios da administração pública na era do conhecimento e da informação**. [S.l.], 2014. v. 22, n. 1. Acesso em: 7 Out. 2023. Disponível em: <https://periodicos.uem.br/ojs/index.php/CadAdm/article/download/23122/16047/>.

STONE, P. et al. **Artificial intelligence and life in 2030: the one hundred year study on artificial intelligence**. [S.l.]: arXiv preprint arXiv:2211.06318, 2022. Acesso em: 29 Out. 2023.

VENTURINI, J.; GARAY, V. **Reconhecimento facial na América Latina: tendências na implementação de uma tecnologia perversa**. 2021. Acesso em: 24 abril 2024. Disponível em: <https://www.alsur.lat/ptbr/relatorio/reconhecimento-facial-na-america-latina-tendencias-na-... implementacao-umatecnologia>.