

INTELIGÊNCIA ARTIFICIAL NA GESTÃO E NA SEGURANÇA PÚBLICA: AVANÇOS, DESAFIOS E OPORTUNIDADES

Edinaldo Inocêncio Ferreira Junior ¹

 <http://lattes.cnpq.br/2516337673524886>

 <https://orcid.org/0009-0003-5675-8398>

Mayara Magna Oliveira Tavares ²

 <http://lattes.cnpq.br/7519004871481588>

 <https://orcid.org/0009-0007-6743-1322>

Maria Cristina Ferreira Marques ³

 <http://lattes.cnpq.br/5916761448356919>

 <https://orcid.org/0009-0009-0268-4315>

Paulo César Diniz de Araújo⁴

 <http://lattes.cnpq.br/3985654366144019>

 <https://orcid.org/0000-0002-0550-2996>

Resumo

O avanço da transformação digital tem impulsionado a adoção da Inteligência Artificial (IA) como ferramenta estratégica para modernizar a administração pública e fortalecer a segurança no Brasil. Nesse contexto, este artigo tem como objetivo analisar as potencialidades e os desafios da aplicação da IA nesses setores, destacando sua relevância para a inovação administrativa e para a formulação de políticas públicas mais eficazes. A metodologia empregada consistiu em pesquisa bibliográfica, fundamentada no estado da arte entre 2018 e 2024, associada a um estudo de caso múltiplo que examinou a experiência do Sistema Hélios da Polícia Militar de Minas Gerais e o programa de reconhecimento facial da Secretaria de Segurança Pública da Bahia. Os resultados demonstram que a IA tem proporcionado avanços significativos na gestão pública, com ganhos em eficiência, otimização de recursos e maior transparência, além de reforçar a segurança pública ao ampliar a capacidade de análise de dados, prever cenários e monitorar indivíduos e veículos. Todavia, foram identificados desafios

¹Aluno do Programa de Segurança Pública, Cidadania e Direitos Humanos da Universidade do Estado do Amazonas - UEA. E-mail: edinaldoferreira.adv@gmail.com Orcid: <https://orcid.org/0009-0003-5675-8398>

²Aluna do Programa de Segurança Pública, Cidadania e Direitos Humanos da Universidade do Estado do Amazonas - UEA. E-mail: mayaramagna@yahoo.com.br Orcid: <https://orcid.org/0009-0007-6743-1322>

³Aluna do Programa de Segurança Pública, Cidadania e Direitos Humanos da Universidade do Estado do Amazonas - UEA. E-mail: mcfmmsp25@uea.edu.br Orcid: <https://orcid.org/0009-0009-0268-4315>

⁴Professor Dr. do Programa de Segurança Pública, Cidadania e Direitos Humanos da Universidade do Estado do Amazonas - UEA. E-mail: <http://lattes.cnpq.br/3985654366144019> Orcid: <https://orcid.org/0000-0002-0550-2996>

INTELIGÊNCIA ARTIFICIAL NA GESTÃO E NA SEGURANÇA PÚBLICA: AVANÇOS, DESAFIOS E OPORTUNIDADES

importantes, como questões éticas relacionadas à privacidade, riscos de vieses algorítmicos, lacunas regulatórias no ordenamento jurídico e limitações técnicas ligadas à infraestrutura tecnológica e à capacitação de servidores. Conclui-se que a adoção da IA, quando acompanhada de regulamentação adequada, mecanismos de governança e observância de princípios éticos, representa uma oportunidade estratégica para consolidar práticas inovadoras na administração pública, fortalecendo a eficiência estatal e a proteção dos direitos fundamentais.

Palavras-chave: Algoritmos Preditivos; Ética Algorítmica; Governança Algorítmica; Políticas Públicas Digitais; Vigilância Inteligente.

Abstract

The rapid expansion of digital transformation has driven the adoption of Artificial Intelligence (AI) as a strategic tool to modernize public administration and strengthen public security in Brazil. In this context, the objective of this article is to analyze the potential and challenges of applying AI in these sectors, emphasizing its relevance for administrative innovation and the formulation of more effective public policies. The methodology employed consisted of bibliographic research, based on the state of the art between 2018 and 2024, combined with a multiple case study that examined the experience of the Hélios System of the Military Police of Minas Gerais and the facial recognition program of the Public Security Secretariat of Bahia. The results demonstrate that AI has generated significant advances in public management, with gains in efficiency, resource optimization, and increased transparency, in addition to strengthening public security by enhancing data analysis, scenario forecasting, and monitoring of individuals and vehicles. However, important challenges were identified, such as ethical issues related to privacy, risks of algorithmic bias, regulatory gaps in the Brazilian legal framework, and technical limitations associated with technological infrastructure and the training of public servants. It is concluded that the adoption of AI, when accompanied by adequate regulation, governance mechanisms, and adherence to ethical principles, represents a strategic opportunity to consolidate innovative practices in public administration, reinforcing state efficiency and the protection of fundamental rights.

Keywords: Algorithmic Ethics; Algorithmic Governance; Digital Public Policies; Intelligent Surveillance; Predictive Algorithms.

Introdução

O advento da era digital e o crescimento exponencial da disponibilidade de dados vêm transformando profundamente a forma como os governos e as instituições de segurança pública operam. Nesse contexto, a Inteligência Artificial (IA) emerge como uma tecnologia estratégica capaz de otimizar processos, ampliar a capacidade analítica e oferecer suporte à tomada de decisão em tempo real. A aplicação da IA na administração pública e na atividade de inteligência de segurança insere-se em um movimento global de modernização do Estado, no qual a eficiência, a transparência e a inovação se tornam imperativos para a governança contemporânea (Calvi; Machado, 2022).

No campo da gestão pública, a IA vem sendo utilizada para automatizar procedimentos burocráticos, melhorar o atendimento ao cidadão e apoiar a formulação de políticas baseadas em evidências. Experiências internacionais e nacionais demonstram que a análise de grandes volumes de dados possibilita a

identificação de padrões e tendências, contribuindo para decisões mais ágeis e assertivas (Maia et al., 2022; Toledo; Mendonça, 2023). Já na segurança pública, as ferramentas de machine learning, reconhecimento facial e videomonitoramento inteligente têm ampliado as possibilidades de prevenção e repressão qualificada, reforçando a atuação estratégica das forças policiais (De Ávila Negri, 2020). Contudo, a incorporação da IA na administração estatal e nas instituições de segurança não está isenta de dilemas. Entre os principais desafios destacam-se as preocupações éticas relativas à proteção da privacidade, a possibilidade de vieses algorítmicos reproduzirem desigualdades sociais, a ausência de um marco regulatório consolidado no Brasil e as barreiras técnicas decorrentes da insuficiência de infraestrutura e de capacitação dos servidores (Brasil, 2018; Brasil, 2020; Vélez et al., 2022). Tais limitações apontam para a necessidade de equilíbrio entre inovação tecnológica e responsabilidade social, a fim de assegurar que os ganhos da IA não comprometam direitos fundamentais.

A relevância deste estudo reside, portanto, em examinar as potencialidades e os limites da IA sob uma perspectiva integrada entre gestão pública e segurança pública. A literatura disponível ainda se mostra fragmentada, ora enfatizando os aspectos tecnológicos, ora discutindo apenas as dimensões éticas e jurídicas. Assim, este artigo busca contribuir para um diálogo interdisciplinar, capaz de fundamentar políticas públicas inovadoras que conciliem eficiência administrativa, proteção de dados e fortalecimento democrático (Gonçalves, 2008; Do Valle, 2020).

A partir desse diagnóstico, formula-se a seguinte questão norteadora: de que maneira a aplicação da inteligência artificial pode contribuir para a modernização da gestão pública e para o aprimoramento da segurança pública no Brasil, sem comprometer os direitos fundamentais e a legitimidade democrática das instituições?

O objetivo geral do artigo é analisar como a aplicação da Inteligência Artificial pode promover avanços na modernização da gestão pública e no aprimoramento da segurança pública no Brasil, identificando, ao mesmo tempo, os desafios éticos, técnicos e regulatórios que limitam sua adoção. Especificamente, pretende-se: (i) revisar o estado da arte sobre IA aplicada à administração pública e à segurança; (ii) examinar experiências concretas de uso da IA em órgãos brasileiros, como os sistemas da Polícia Militar de Minas Gerais e da Secretaria de Segurança Pública da Bahia; e (iii) discutir as oportunidades e riscos associados à adoção dessas tecnologias no setor público.

Dessa forma, este artigo estrutura-se em cinco seções, além desta introdução. A segunda seção apresenta o referencial teórico, discutindo conceitos fundamentais, aplicações e desafios da IA. A terceira seção descreve a metodologia utilizada. A quarta seção expõe os resultados e a discussão, destacando achados a partir do estudo de caso. Por fim, a quinta seção apresenta as conclusões, sintetizando as contribuições do trabalho e apontando recomendações para a formulação de políticas públicas e para futuras pesquisas.

Metodologia

A metodologia adotada neste estudo estrutura-se a partir da natureza aplicada da pesquisa, uma vez que o objetivo principal é gerar conhecimento direcionado à prática e capaz de subsidiar gestores públicos e instituições de segurança na adoção de soluções inovadoras com base em Inteligência Artificial (IA). Esse caráter aplicado diferencia o presente trabalho de investigações puramente teóricas, pois busca não apenas compreender o fenômeno, mas também oferecer recomendações que possam ser implementadas no âmbito da administração pública e da segurança.

No que concerne aos objetivos, a pesquisa apresenta um delineamento exploratório e descritivo. É exploratória porque se propõe a investigar fenômenos ainda recentes e em constante evolução, como a IA na gestão e na segurança pública, identificando categorias analíticas, desafios e oportunidades que não se encontram totalmente consolidados no campo científico. Simultaneamente, é descritiva porque busca detalhar as características, potencialidades e limitações das experiências práticas analisadas, permitindo uma visão panorâmica e fundamentada sobre a aplicação de tecnologias emergentes em instituições estatais.

Quanto à abordagem metodológica, a pesquisa é predominantemente qualitativa, pois privilegia a interpretação crítica e a análise de significados, contextos e implicações sociojurídicas e institucionais da adoção da IA. Reconhece-se, contudo, o uso de dados secundários de caráter quantitativo, extraídos de relatórios e documentos oficiais, que auxiliam na contextualização empírica dos casos estudados. A integração entre abordagens qualitativa e quantitativa assegura maior robustez analítica, permitindo compreender o objeto tanto em sua dimensão técnica quanto em suas consequências sociais e normativas.

O principal procedimento adotado foi a pesquisa bibliográfica e documental. A pesquisa bibliográfica contemplou um levantamento sistemático de obras científicas — artigos, livros e capítulos — publicados em bases de dados como Scopus, Web of Science, SciELO e Google Scholar, priorizando o recorte temporal de 2018 a 2024. O objetivo dessa etapa foi mapear o estado da arte e identificar consensos, divergências e lacunas na literatura. No caso da pesquisa documental, foram considerados apenas documentos oficiais ou oriundos de instituições reconhecidas (como legislações, pareceres, relatórios técnicos nacionais e internacionais e registros institucionais de secretarias de segurança). Documentos com informações incompletas, ausência de fonte verificável ou caráter opinativo foram descartados, a fim de garantir maior confiabilidade das evidências utilizadas. Além disso, foi adotado o estudo de caso múltiplo como estratégia metodológica complementar. Foram selecionados dois casos emblemáticos no contexto brasileiro: (i) o Sistema Hélios, da Polícia Militar de Minas Gerais, que utiliza reconhecimento automático de placas veiculares e integração em tempo real com bases de interesse policial; e (ii) o programa de reconhecimento facial da Secretaria de Segurança Pública da Bahia, voltado para a identificação de foragidos e a prevenção de crimes em grandes eventos e espaços urbanos. A escolha desses dois casos deve-se a três razões principais: (a) representatividade setorial, pois ambos são referências nacionais em inovação tecnológica aplicada à segurança; (b) impacto social

comprovado, dado o alcance de suas operações e a repercussão pública de seus resultados; e (c) disponibilidade de informações documentais confiáveis, fator essencial para análises críticas em pesquisas acadêmicas. Reconhece-se que a adoção de apenas dois casos pode limitar a validade externa, mas a representatividade das experiências garante sua relevância como amostras paradigmáticas.

O processo de análise seguiu os princípios da análise de conteúdo temática (Bardin, 2010), que organiza e interpreta informações a partir de categorias definidas previamente. Para este estudo, foram estabelecidas três categorias centrais: (a) benefícios e avanços proporcionados pela IA, como eficiência, inovação e capacidade analítica; (b) riscos e desafios, incluindo questões éticas, lacunas regulatórias e limitações técnicas; e (c) oportunidades futuras, relacionadas à governança algorítmica, à formulação de políticas públicas digitais e à integração da IA com princípios de cidadania e direitos fundamentais. Outro aspecto relevante foi a triangulação de fontes. O cruzamento entre literatura científica, documentos normativos e experiências práticas buscou reduzir vieses e assegurar consistência analítica. Por exemplo, quando um documento oficial reportava determinado número de prisões associadas ao uso de reconhecimento facial na Bahia, essa informação foi confrontada com dados divulgados pela imprensa e com análises críticas da literatura. Em casos de divergência, adotou-se o critério de prevalência de fontes primárias oficiais, sem deixar de registrar interpretações acadêmicas que questionavam sua validade. Essa triangulação possibilitou avaliar a IA em três dimensões complementares: técnica (eficiência e funcionamento dos algoritmos), institucional (implementação nas estruturas administrativas) e normativa (implicações éticas e jurídicas).

Por fim, cabe apontar as limitações metodológicas. A principal refere-se à dependência de dados secundários, já que nem todas as informações sobre sistemas de IA em uso no Brasil estão disponíveis publicamente. Além disso, como as tecnologias analisadas estão em constante atualização, existe o risco de que certas conclusões se tornem datadas em curto prazo. Tais limitações foram mitigadas por meio da seleção de casos emblemáticos, do uso de documentos oficiais e do recorte temporal atualizado (2018–2024), garantindo maior validade e relevância ao estudo.

Assim, a metodologia aqui descrita, ao articular pesquisa bibliográfica, documental e estudo de caso múltiplo, fornece um caminho sólido para compreender como a IA está sendo implementada na gestão pública e na segurança, bem como os dilemas éticos, técnicos e regulatórios que emergem desse processo. Mais do que descrever experiências, a proposta busca extrair lições que possam orientar políticas públicas responsáveis, inovadoras e alinhadas à proteção dos direitos fundamentais.

Fundamentação Teórica:

A IA consolidou-se, nas últimas décadas, como um campo interdisciplinar de pesquisa e aplicação prática, envolvendo ciência da computação, matemática, estatística, filosofia e psicologia cognitiva. Seu desenvolvimento histórico remonta às formulações pioneiras de Alan Turing, com a proposição do “Teste de Turing” em 1950, que questionava a possibilidade de máquinas

simularem o raciocínio humano, e às contribuições de McCulloch e Pitts, ao estabelecerem modelos computacionais inspirados em redes neurais biológicas (Russell; Norvig, 2004). Desde então, a IA tem evoluído de sistemas baseados em regras para algoritmos de aprendizado de máquina, processamento de linguagem natural e redes neurais profundas, configurando-se como uma tecnologia capaz de transformar profundamente a gestão pública e a segurança (Sanchez, 2023).

Na administração pública, a IA é apontada como um vetor de inovação e modernização institucional. Estudos recentes destacam seu potencial para automatizar tarefas burocráticas, ampliar a capacidade de análise de dados governamentais e personalizar serviços de acordo com as necessidades dos cidadãos (Comba et al., 2024; Maia et al., 2022). Além da otimização de recursos, observa-se a emergência de práticas orientadas por dados (data-driven government), em que algoritmos preditivos são aplicados para identificar padrões sociais e antecipar demandas, fortalecendo a eficiência estatal e a qualidade das políticas públicas (Toledo; Mendonça, 2023). Essa perspectiva conecta-se à noção de governança algorítmica, segundo a qual a administração pública passa a depender, de forma crescente, de sistemas computacionais que não apenas apoiam, mas moldam decisões estratégicas (Do Valle, 2020; Vélez et al., 2022).

No âmbito da segurança pública, a IA é incorporada às atividades de inteligência e policiamento, com destaque para sistemas de videomonitoramento inteligente, reconhecimento facial e análise massiva de dados criminais (Vieira; Barbuda, 2024). Experiências implementadas no Brasil ilustram esse processo: em Minas Gerais, o Sistema Hélios possibilita a leitura automática de placas veiculares, integrando informações de interesse para a segurança; na Bahia, o uso de reconhecimento facial já resultou na prisão de milhares de foragidos, demonstrando a aplicabilidade prática da tecnologia em operações policiais (Brito et al., 2022; De Aguiar Araújo et al., 2021). Essas iniciativas dialogam com tendências internacionais, nas quais a IA é utilizada para detecção de anomalias, policiamento preditivo e gestão integrada de riscos (De Menezes; Sanllehí, 2021). Contudo, a incorporação da IA à gestão pública e à segurança suscita dilemas éticos, regulatórios e técnicos. Um dos riscos mais discutidos refere-se aos vieses algorítmicos, que podem reproduzir discriminações de gênero, raça e classe, caso os sistemas sejam treinados com bases de dados enviesadas (Fernandes et al., 2024). O’Neil (2017) alerta que tais algoritmos podem transformar-se em verdadeiras “armas de destruição matemática”, replicando desigualdades de forma invisível e automatizada. Pasquale (2015), por sua vez, argumenta que a opacidade dos sistemas cria uma “caixa-preta algorítmica”, dificultando a fiscalização social e a responsabilização jurídica. Essa crítica se soma à visão de Zuboff (2023), que denuncia a tendência de consolidação de uma lógica de “capitalismo de vigilância”, na qual a coleta massiva de dados gera novas formas de controle social. Esses autores internacionais, amplamente utilizados em periódicos de alto impacto, reforçam que o debate sobre IA vai além da eficiência tecnológica, alcançando questões estruturais de poder, justiça e democracia. Esse problema conecta-se à necessidade de transparência e auditabilidade dos algoritmos, de modo a garantir legitimidade democrática às decisões automatizadas (Cortez, 2023). Além disso, a literatura enfatiza a vulnerabilidade dos sistemas a ataques cibernéticos e a dependência de

infraestrutura tecnológica adequada, aspectos críticos em países que ainda enfrentam desigualdades no acesso a tecnologias de ponta (Belli et al., 2023).

Aqui, emerge a dimensão jurídica: no Brasil, a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) estabelece princípios de privacidade e uso de dados pessoais, mas não aborda de forma específica os impactos da IA em segurança pública. Em contraste, o Regulamento Geral de Proteção de Dados da União Europeia (RGPD) avança ao assegurar, por exemplo, o direito à explicação em decisões automatizadas e mecanismos mais claros de responsabilização. Essa comparação evidencia uma lacuna regulatória no Brasil, que torna urgente a formulação de políticas públicas voltadas à governança algorítmica, com ênfase na transparência e na proteção de direitos fundamentais.

A análise de Junior, Santos e De Aguiar (2023) sobre o Cadastro Ambiental Rural (CAR) demonstra como instrumentos digitais concebidos para o ordenamento territorial podem, em determinadas circunstâncias, ser apropriados de forma distorcida, legitimando práticas de grilagem em terras públicas. Essa constatação é altamente relevante para o debate sobre inteligência artificial, pois evidencia que sistemas tecnológicos, quando desprovidos de mecanismos robustos de regulação e fiscalização, podem produzir efeitos contrários aos objetivos originais. No caso da IA aplicada à gestão pública e à segurança, o risco é semelhante: algoritmos sem governança adequada podem reforçar desigualdades e até legitimar práticas abusivas. De modo complementar, Junior e Nascimento (2024) argumentam que a educação ambiental desempenha papel estratégico no empoderamento de comunidades tradicionais e na defesa de seus direitos humanos. Essa reflexão pode ser transposta para o contexto da IA, indicando que sua adoção na gestão e na segurança pública só será efetiva e legítima se acompanhada de processos participativos, transparência e conscientização social. Tal perspectiva reforça que a introdução de tecnologias disruptivas deve estar alinhada não apenas a critérios de eficiência, mas também à valorização da cidadania e ao respeito à diversidade cultural.

Portanto, o referencial teórico indica que a IA ocupa uma posição ambivalente no setor público: por um lado, representa um instrumento promissor para modernização administrativa e fortalecimento da segurança; por outro, carrega riscos que exigem cautela, regulamentação e governança responsável. Ao conjugar os achados de estudos recentes com casos concretos do Brasil, observa-se que a IA pode se consolidar como ferramenta estratégica de inovação, desde que articulada a uma agenda ética e normativa que assegure a proteção da cidadania e a transparência das ações governamentais. Ao conjugar os achados de estudos recentes com casos concretos do Brasil e com reflexões críticas internacionais, observa-se que a IA pode se consolidar como ferramenta estratégica de inovação, desde que articulada a uma agenda ética, normativa e participativa que assegure a proteção da cidadania e a transparência das ações governamentais.

Resultados e discussões:

Os resultados da pesquisa confirmam que a aplicação da IA na gestão pública e na segurança se apresenta como um campo em rápida evolução,

trazendo tanto ganhos de eficiência quanto riscos que demandam constante reflexão crítica. A análise dos casos da Polícia Militar de Minas Gerais (PMMG) e da Secretaria de Segurança Pública da Bahia (SSP/BA) ilustra esse duplo caráter, em que a inovação tecnológica precisa ser acompanhada de salvaguardas éticas, normativas e institucionais.

No caso da PMMG, o Sistema Hélios destaca-se como uma ferramenta inovadora de monitoramento veicular, baseada em câmeras inteligentes e softwares de reconhecimento automático de placas. A principal contribuição desse sistema está na integração de dados em tempo real, permitindo às equipes policiais localizar veículos roubados ou clonados com maior rapidez, além de auxiliar no rastreamento de rotas utilizadas por organizações criminosas. A literatura aponta que esse tipo de tecnologia potencializa o policiamento orientado por dados (data-driven policing), conferindo às forças de segurança maior capacidade preditiva e preventiva (Comba et al., 2024; Vieira; Barbuda, 2024). Do ponto de vista operacional, o Hélios representa um avanço na racionalização de recursos humanos, ao reduzir a dependência de abordagens aleatórias e direcionar esforços para alvos previamente identificados por cruzamento de informações.

Entretanto, a experiência mineira também revela limitações. Embora o sistema reduza a exposição de dados biométricos, a dependência de infraestrutura tecnológica robusta e de conectividade estável representa um desafio em regiões periféricas ou de baixa cobertura digital. Além disso, como salientam Comba et al. (2024) e Vieira e Barbuda (2024), a confiabilidade do sistema depende da qualidade e atualização das bases de dados. Erros de cadastro, duplicidades ou omissões podem comprometer a eficácia do monitoramento, gerando falsas ocorrências e desgastes institucionais.

Já a experiência da Bahia com o programa de reconhecimento facial evidencia um patamar mais avançado de exposição a dilemas éticos e jurídicos. O sistema, utilizado inicialmente em grandes eventos como o carnaval e posteriormente expandido para áreas urbanas estratégicas, já resultou na captura de centenas de indivíduos foragidos, inclusive de alta periculosidade (Comba et al., 2024). Esse resultado reforça o potencial da IA em aumentar a eficácia investigativa e reduzir o tempo de resposta operacional. Contudo, o programa gerou críticas de especialistas e organizações da sociedade civil, que alertam para riscos de falsos positivos, vieses raciais e ausência de protocolos claros sobre armazenamento, uso e compartilhamento dos dados biométricos coletados. Essas críticas encontram respaldo na literatura, que demonstra que algoritmos de reconhecimento facial frequentemente apresentam taxas de erro mais elevadas em indivíduos negros e pardos, reforçando desigualdades sociais já presentes na prática policial (Vieira; Barbuda, 2024). No contexto brasileiro, marcado por desigualdades raciais e socioeconômicas, esse risco ganha maior relevância e exige salvaguardas normativas, como auditorias independentes e mecanismos de accountability, para evitar que tecnologias de segurança se tornem instrumentos de selevidade punitiva.

Ao comparar os dois casos, observa-se que ambos confirmam a tese de Junior, Santos e De Aguiar (2023), segundo a qual instrumentos digitais podem ser apropriados de forma distorcida quando não há regulação eficaz. No caso do CAR, a ausência de controles robustos resultou na legitimação de práticas ilegais de grilagem; já nos sistemas de IA, a falta de governança pode levar à ampliação

de injustiças sociais. A lição comum é que a tecnologia, sem regulação adequada, corre o risco de se converter em meio de legitimação de desigualdades, em vez de instrumento de modernização democrática. A reflexão de Junior e Nascimento (2024) sobre a importância da educação ambiental para o empoderamento de comunidades tradicionais também se aplica à IA: para que haja legitimidade na adoção dessas tecnologias, é fundamental investir em educação cidadã, transparência e participação social. Assim como comunidades tradicionais precisam de informação e consciência crítica para enfrentar ameaças ambientais, os cidadãos urbanos necessitam compreender como funcionam os algoritmos que influenciam sua vida cotidiana, sobretudo em contextos de vigilância e segurança.

Os resultados obtidos podem ser organizados em três dimensões analíticas:

Benefícios: A IA aumenta a eficiência administrativa e operacional, possibilita decisões mais rápidas e baseadas em dados, amplia a capacidade de prevenção e contribui para a modernização do Estado. No caso da PMMG, esses ganhos se traduzem na redução de tempo de resposta e no direcionamento mais preciso de operações.

Desafios: As limitações técnicas (como falhas em bases de dados e infraestrutura precária), os dilemas éticos (vieses algorítmicos e riscos de discriminação) e as lacunas regulatórias (ausência de marco jurídico consolidado sobre IA no Brasil) são barreiras que precisam ser superadas para que os avanços não resultem em retrocessos.

Oportunidades: A adoção da IA pode consolidar uma nova agenda de governança algorítmica, pautada pela regulação transparente, participação social e integração com princípios de direitos humanos. Se adequadamente implementada, a IA pode não apenas fortalecer a segurança pública, mas também ampliar a confiança social nas instituições, tornando-se elemento estratégico para políticas públicas digitais e inclusivas.

Em síntese, os resultados e a discussão apontam para um cenário ambivalente: a IA é, ao mesmo tempo, promessa e risco. Promessa porque moderniza práticas administrativas e de segurança; risco porque, sem controle, pode reforçar exclusões históricas. A principal conclusão é que a tecnologia deve ser compreendida como um processo sociotécnico, no qual eficiência e legitimidade precisam caminhar juntas. Nesse sentido, os casos analisados revelam que a inovação em segurança pública não pode ser reduzida a uma questão de desempenho técnico, mas deve ser entendida como um fenômeno institucional e democrático, que exige governança responsável, regulamentação eficaz e constante participação da sociedade civil.

Considerações Finais:

Este estudo analisou como a Inteligência Artificial pode contribuir para a modernização da gestão pública e o aprimoramento da segurança no Brasil. Os resultados confirmaram que a tecnologia possui um caráter ambivalente: de um lado, constitui um instrumento capaz de transformar práticas estatais, tornando-as mais eficientes, transparentes e orientadas por dados; de outro, se mal regulada, pode reforçar desigualdades históricas, comprometer direitos

fundamentais e gerar questionamentos sobre a legitimidade democrática das instituições.

O objetivo geral foi plenamente alcançado ao demonstrar que a IA, quando incorporada de maneira planejada e responsável, eleva a capacidade do Estado em responder às demandas sociais e fortalece a atuação das forças de segurança. Os objetivos específicos também foram atendidos: a revisão teórica mostrou que a IA deve ser compreendida como fenômeno sociotécnico, a análise de casos brasileiros revelou lições valiosas sobre benefícios e limitações, e a discussão final destacou oportunidades e riscos que condicionam a legitimidade de sua adoção.

A originalidade do trabalho reside na abordagem integrada entre gestão pública e segurança, articulando discussões teóricas, análise empírica e comparações internacionais. Diferentemente de estudos fragmentados que se concentram apenas nos aspectos técnicos ou exclusivamente nos riscos éticos, esta pesquisa propôs um diálogo interdisciplinar, capaz de fundamentar políticas públicas inovadoras e de ampliar o debate acadêmico com base na realidade brasileira.

No plano prático, os resultados permitem apontar recomendações que podem orientar gestores e legisladores. É necessário avançar na criação de marcos regulatórios específicos para a IA, que contemplem a explicabilidade dos algoritmos, a proteção de dados sensíveis e critérios claros de responsabilização. Também se recomenda investir em capacitação continuada dos servidores públicos, de modo que a adoção da IA não se restrinja a ganhos técnicos, mas esteja alinhada a valores democráticos e sociais. Outro ponto essencial é a instituição de mecanismos independentes de auditoria e accountability, capazes de monitorar a imparcialidade dos algoritmos. Por fim, torna-se indispensável o fortalecimento da participação social, garantindo que a inovação tecnológica seja inclusiva e acompanhada de transparência. As limitações da pesquisa concentram-se na dependência de dados secundários, que restringe a análise empírica, e na velocidade de evolução das tecnologias de IA, que pode tornar algumas conclusões datadas em curto prazo. Ainda assim, a seleção de casos emblemáticos e a triangulação metodológica asseguraram a validade e a relevância do estudo.

As perspectivas futuras incluem a ampliação do escopo para outros estados e áreas da administração pública, a realização de comparações internacionais mais sistemáticas e o aprofundamento dos impactos da IA sobre populações vulneráveis. Esse direcionamento permitirá compreender melhor se a tecnologia contribui para reduzir ou, ao contrário, reforçar desigualdades sociais. Em síntese, conclui-se que a IA não deve ser compreendida apenas como ferramenta técnica, mas como processo sociopolítico que redefine a relação entre Estado e sociedade. Sua adoção exige escolhas conscientes, baseadas em princípios éticos, jurídicos e democráticos, de forma que a tecnologia se converta em aliada da segurança pública, do desenvolvimento sustentável e da consolidação da cidadania.

Referências:

BARDIN, Laurence. **Análise de conteúdo.** 4. ed. Lisboa: Edições70, 2010.

INTELIGÊNCIA ARTIFICIAL NA GESTÃO E NA SEGURANÇA PÚBLICA: AVANÇOS, DESAFIOS E OPORTUNIDADES

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União**: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/ato2015-2018/lei/L13709.htm. Acesso em: 08 ago. 2025.

BRASIL. Projeto de Lei nº 21, de 2020. Estabelece princípios, direitos e deveres para o uso de inteligência artificial no Brasil. **Diário do Senado Federal**: Brasília, DF, 29 set. 2020. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento/download/f6698c0a-62ec-4e8e-93b8-a736e2c94c66>. Acesso em: 08 ago. 2025.

BELLI, Luca et al. **Cibersegurança: uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano**. Rio de Janeiro: FGV Direito Rio, 2023.

BRITO, Emerson de Araújo Garro; CARNEIRO, Marco Túlio; DE SOUZA GUERRA, Vitor. As novas tecnologias aplicadas à prevenção e repressão qualificada aos crimes de furto e roubo de veículos: sistema hélios na polícia militar de Minas Gerais. *O Alferes*, v. 32, n. 80, 2022. DOI: <https://doi.org/10.51912/alf.v32i80.890>.

CALVI, Jenifer; MACHADO, Hilka. Coevolução da inteligência natural e artificial: Uma revisão da literatura sobre inteligência híbrida. *Revista Inteligência Empresarial*, v. 46, 2022.

COMBA, Biof Bucut et al. Inteligência Artificial na gestão pública: desafios e oportunidades. *Pesquisa e Ensino em Ciências Exatas e da Natureza*, v. 8, p. 1-6, 2024.

CORTEZ, Florian. Artificial intelligence, climate change and innovative democratic governance. *European Journal of Risk Regulation*, v. 14, n. 3, p. 484-503, 2023.

DE AGUIAR ARAÚJO, Romulo; CARDOSO, Naiara Deperon; DE PAULA, Amanda Marcélia. Regulação e uso do reconhecimento facial na segurança pública do Brasil. *Revista de Doutrina Jurídica*, v. 112, p. e021009-e021009, 2021. DOI: <https://doi.org/10.22477/rdj.v112i00.734>.

DE ÁVILA NEGRI, Sergio Marcos Carvalho; DE OLIVEIRA, Samuel Rodrigues; COSTA, Ramon Silva. O uso de tecnologias de reconhecimento facial baseadas em inteligência artificial e o direito à proteção de dados. *Direito Público*, v. 17, n. 93, 2020.

DE MENEZES, Cyntia Souza; SANLLEHÍ, José Ramon Agustina. Big data, inteligência artificial e policiamento preditivo: bases para uma adequada regulação legal que respeite os direitos fundamentais. *Novos Estudos Jurídicos*, v. 26, n. 1, p. 103-135, 2021. DOI: <https://doi.org/10.14210/nej.v26n1.p103-135>.

DO VALLE, Vanice Lírio. Inteligência artificial incorporada à Administração Pública: mitos e desafios teóricos. A&C-Revista de Direito Administrativo & Constitucional, v. 20, n. 81, p. 179-200, 2020. DOI: <https://doi.org/10.21056/aec.v20i81.1346>.

FERNANDES, Allysson Barbosa et al. A ética no uso de inteligência artificial na educação: implicações para professores e estudantes. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 3, p. 346-361, 2024.

GONÇALVES, Joanisval Brito. **Sed quis custodiet ipso custodes?** O controle da atividade de inteligência em regimes democráticos: os casos de Brasil e Canadá. 2008. 837p. 2008. Tese de Doutorado. Tese (Doutorado em Relações Internacionais) – Instituto de Relações Internacionais, Universidade de Brasília, Brasília, 2008. Disponível em: http://bdtd.bce.unb.br/tedesimplificado/tde_busca/arquivo.php. Acesso em: 20 ago. 2025.

JUNIOR, E. I. F.; NASCIMENTO, M. H. R. Educação Ambiental como instrumento de empoderamento e garantia dos direitos humanos das comunidades tradicionais no Estado do Amazonas. Revista Brasileira De Educação Ambiental (RevBEA), v. 19, n. 1, p. 102-117, 2024. DOI: <https://doi.org/10.34024/revbea.2024.v19.15202>.

JÚNIOR, E. I. F.; SANTOS, R. P.; DE AGUIAR, D. M. Cadastro ambiental rural: a legitimação da grilagem em terras públicas e as estratégias de combate. Boletim de Conjuntura (BOCA), v. 16, n. 46, p. 241-263, 2023. DOI: <https://doi.org/10.5281/zenodo.10011885>.

MAIA, Marcelo et al. Dados no apoio à gestão pública estadual: conhecendo o "Programa Inteligência Artificial do Paraná-PIÁ". Revista Tecnologia e Sociedade, v. 18, n. 50, p. 61-79, 2022. DOI: <https://doi.org/10.3895/rts.v18n50.13236>.

O'NEIL, Cathy. **Weapons of math destruction: How big data increases inequality and threatens democracy.** Crown, 2017.

PASQUALE, Frank. **The black box society: The secret algorithms that control money and information.** Harvard University Press, 2015.

RUSSEL, S.; NORVIG, P. **Inteligência Artificial: Uma abordagem moderna.** 3a. ed. Rio de Janeiro: Elsevier Editora 2004.

SANCHEZ, Wagner. **Aplicações de inteligência artificial.** Editora Senac São Paulo, 2023.

TOLEDO, Adriana Teixeira de; MENDONÇA, Milton. A aplicação da inteligência artificial na busca de eficiência pela administração pública. Revista do Serviço

**INTELIGÊNCIA ARTIFICIAL NA GESTÃO E NA SEGURANÇA PÚBLICA:
AVANÇOS, DESAFIOS E OPORTUNIDADES**

Público, v. 2, n. 74, p. 410–438, 2023. DOI:
<https://doi.org/10.21874/rsp.v74i2.6829>.

VÉLEZ, María Isabel; GÓMEZ SANTAMARÍA, Cristina; OSORIO SANABRIA, Mariutsi Alexandra. Conceptos fundamentales y uso responsable de la inteligencia artificial en el sector público. Informe 2. Caracas: CAF, 2022.

VIEIRA, Paulo Henrique Brant; BARBUDA, Alex Soares. A aplicação da inteligência artificial na atividade de segurança pública. Revista Jurídica do Nordeste Mineiro, v. 8, n. 1, 2024. DOI: DOI:
<https://doi.org/10.61164/rjnm.v8i1.2936>.

ZUBOFF, Shoshana. **The age of surveillance capitalism.** In: Social theory rewired. Routledge, 2023. p. 203-213.

Recebido em: 10/10/2025
Aprovado em: 28/10/2025
Publicado em: 30/11/2025