

A APLICAÇÃO DA INTELIGÊNCIA ARTIFICIAL NA GESTÃO DA SEGURANÇA PÚBLICA: UMA ANÁLISE À LUZ DA PORTARIA MJSP Nº 961/2025

THE APPLICATION OF ARTIFICIAL INTELLIGENCE IN PUBLIC SECURITY MANAGEMENT: AN ANALYSIS IN LIGHT OF MJSP ORDINANCE NO. 961/2025

LA APLICACIÓN DE LA INTELIGENCIA ARTIFICIAL EN LA GESTIÓN DE LA SEGURIDAD PÚBLICA: UN ANÁLISIS A LA LUZ DE LA ORDENANZA MJSP N.º 961/2025

Andressa Ignácio Aguiar¹, Carla Mariana Café Botelho², Enock Rosa Paulino Filho³, Julia Matta e Moura⁴, Renata Ribeiro⁵, Luana Régia Rodrigues Gomes⁶

DOI: 10.54899/dcs.v23i96.7071

Recibido: 14/08/2026 | Aceptado: 09/09/2026 | Publicación en línea: 16/09/2026.

RESUMO

O presente estudo tem como escopo analisar a incorporação da inteligência artificial como ferramenta estratégica em políticas de segurança pública de tal modo a destacar seu impacto no aperfeiçoamento do policiamento preditivo bem como salientar os cuidados que devem ser tomados durante sua operabilidade diante de uma legislação específica, a Portaria MJSP nº 961/2025 que surgiu em decorrência da necessidade de estabelecer limites ao uso dos avanços tecnológicos a fim de que não houvesse a mitigação dos direitos fundamentais dos cidadãos. Conclui-se que apesar dessa portaria ter representado um marco regulatório significativo e que trará impactos positivos, o uso da IA na persecução penal ainda necessita de regulamentações complementares que contemplem questões ainda não dirimidas.

Palavras-chave: Inteligência Artificial. Direitos Fundamentais. Policiamento Preditivo. Políticas de Segurança Pública.

¹ Pós-graduada em Direito Penal e Criminologia pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), Porto Alegre, Rio Grande do Sul, Brasil. E-mail: andressapgmtr@gmail.com

² Doutora em Direito Constitucional pela Universidade Federal do Ceará (UFC), Fortaleza, Ceará, Brasil.

E-mail: carlamarianacafe@gmail.com Orcid: <https://orcid.org/0000-0002-8362-4315>

³ Mestrando em Direito Processual pela Universidade Federal do Espírito Santo (UFES), Vitória, Espírito Santo, Brasil. E-mail: enockRPF@hotmail.com Orcid: <https://orcid.org/0009-0002-0421-827X>

⁴ Graduada em Direito pela Faculdade Presbiteriana Mackenzie Rio, Rio de Janeiro, Rio de Janeiro, Brasil.

E-mail: juliamattaem@gmail.com Orcid: <https://orcid.org/0009-0002-1200-8192>

⁵ Mestranda em Direito pela Universidade Federal do Ceará (UFC), Fortaleza, Ceará, Brasil.

E-mail: renataribeiro60603@gmail.com Orcid: <https://orcid.org/0009-0008-0223-4704>

⁶ Pós-Graduada em Neuropsicologia pelo Instituto de Pós-Graduação e Graduação (IPOG), Goiânia, Goiás, Brasil. E-mail: psiluanagomes@gmail.com Orcid: <https://orcid.org/0009-0005-6286-9400>

ABSTRACT

This study aims to analyze the incorporation of artificial intelligence as a strategic tool in public security policies, highlighting its impact on improving predictive policing and highlighting the precautions that must be taken during its implementation, given a specific piece of legislation, Ordinance 961/2025, which arose from the need to establish limits on the use of technological advances to prevent the mitigation of citizens' fundamental rights. The conclusion is that, although this ordinance represents a significant regulatory framework and will bring positive impacts, the use of AI in criminal prosecution still requires additional regulations that address unresolved issues.

Keywords: Artificial Intelligence. Fundamental rights. Predictive policing. Public Safety Policies.

RESUMEN

El presente estudio tiene como objetivo analizar la incorporación de la inteligencia artificial como herramienta estratégica en las políticas de seguridad pública, destacando su impacto en la mejora de la vigilancia policial predictiva y señalando las precauciones que deben tomarse durante su implementación, ante una legislación específica, la Ordenanza 961/2025, surgida de la necesidad de establecer límites al uso de los avances tecnológicos para evitar la vulneración de los derechos fundamentales de los ciudadanos. Se concluye que, si bien esta ordenanza representa un marco regulatorio significativo y traerá impactos positivos, el uso de la IA en la persecución penal aún requiere de regulaciones complementarias que aborden cuestiones no resueltas.

Palabras clave: Inteligencia Artificial. Derechos Fundamentales. Vigilancia Policial Predictiva. Políticas de Seguridad Pública.



Esta obra está bajo una [Licencia Creative Commons Atribución- NoComercial 4.0 Internacional](https://creativecommons.org/licenses/by-nc/4.0/)

INTRODUÇÃO: A PERSECUÇÃO PENAL NA ERA DOS ALGORITMOS

Com o avanço tecnológico alcançando a esfera do direito penal, surgiu a necessidade de implementar políticas de segurança pública que atuem de forma eficaz no combate à criminalidade através da incorporação de um sistema de análise preditiva com o uso de algoritmos que demonstrem as similaridades dos contextos de determinados crimes que foram praticados com o ensejo de estabelecer parâmetros e particularidades a fim de que futuros delitos possam ser evitados.

Em contrapartida ao método convencional de atuação policial que consiste na relação entre vítima, criminoso e local de prática do delito e apresenta elementos subjetivos próprios de

infrator e dos policiais, a implementação da inteligência artificial como uma ferramenta estratégica na gestão da segurança pública surge com expectativas de que os obstáculos do modelo anterior possam ser superados para que o policiamento preditivo seja aperfeiçoado.

Ademais, deve-se ressaltar a importância de as autoridades públicas estarem sempre atentas às mudanças ocorridas no modus operandi das ações criminosas tendo em vista que conforme os mecanismos de inteligência artificial são difundidos, os criminosos tendem a aperfeiçoar suas ações, destacando-se assim, a importância de que o sistema preditivo esteja sempre se aperfeiçoando na prevenção e repressão à criminalidade.

A justiça criminal brasileira vem se beneficiando nos últimos anos do uso da IA através de uma melhoria na investigação criminal por meio de algoritmos que propiciam uma coleta e análise de dados mais célere e precisa, otimizando assim a identificação de padrões e o mapeamento de ocorrências criminais contribuindo, portanto, de forma efetiva para uma política criminal sólida que consiga desenvolver estratégias hábeis no combate à criminalidade.

Este cenário revela uma transição estrutural na filosofia de atuação das forças de segurança, caracterizada pela passagem de um modelo puramente reativo focado na investigação pós-fato e na colheita tradicional de vestígios para um modelo eminentemente preditivo de controle social. Esta virada tecnológica, que se fundamenta na expansão massiva do Big Data e na promessa de uma governança orientada a dados, busca legitimar as intervenções estatais a partir de uma pretensa racionalidade matemática de prevenção de condutas desviantes. Todavia, esse deslocamento impõe severas tensões às bases garantistas do processo penal democrático, notadamente em face do princípio constitucional da presunção de inocência, o qual passa a ser tensionado por mecanismos que priorizam a contenção antecipada de perigos estatísticos em detrimento do exame da responsabilidade penal individualizada por fatos pretéritos concretos.

Outrossim, ao delegar a softwares proprietários a definição de 'manchas criminais' ou a identificação de 'perfis suspeitos', o Poder Público arrisca terceirizar o próprio juízo de suspeição e a discricionariedade policial a entes privados, sem o devido escrutínio democrático. Esse fenômeno gera uma opacidade epistêmica que obstaculiza o controle de legalidade das medidas preventivas, tornando imperiosa a formulação de um marco teórico que avalie se os instrumentos regulatórios infralegais, como a Portaria nº 961/2025, possuem densidade normativa suficiente para resguardar a cidadania contra a consolidação de um Estado policial algorítmico.

O presente artigo tem como objetivo analisar o papel da inteligência artificial nas políticas de segurança pública, destacando suas formas de aplicação. O estudo também abordará uma nova

norma destinada a regulamentar o uso dessa tecnologia. A relevância do tema decorre do impacto cada vez maior da IA nos processos decisórios que envolvem o sistema de justiça penal.

Nesse contexto, formula-se o seguinte problema de pesquisa: em que medida as diretrizes e salvaguardas estabelecidas pela Portaria MJSP nº 961/2025 são suficientes para mitigar os riscos de vieses cognitivos, discriminação racial e seletividade penal, garantindo o uso constitucionalmente adequado da inteligência artificial na persecução penal?

INTELIGÊNCIA ARTIFICIAL E POLÍTICAS PÚBLICAS DE SEGURANÇA

A Inteligência Artificial (IA) é um ramo da ciência da computação que se dedica ao desenvolvimento de sistemas capazes de realizar tarefas que normalmente requerem inteligência humana. Esses sistemas podem aprender, compreender, raciocinar, resolver problemas e tomar decisões. (Barbuda; Vieira; Silva, 2024).

A introdução de técnicas como redes neurais artificiais, aprendizado profundo (deep learning) e algoritmos de aprendizado de máquina (machine learning) permitiu avanços sem precedentes, tornando possível a criação de sistemas mais precisos e eficazes em tarefas complexas, como o reconhecimento de voz e imagem, a tradução automática e o diagnóstico médico (Cardoso, 2025).

Sob a perspectiva dogmática e regulatória estruturada por Patrícia Peck Pinheiro (2024), a implementação da inteligência artificial em políticas públicas exige uma governança digital ética e segura, em que a tecnologia deve atuar como um instrumento de transparência e eficiência do Estado, o que demanda que as inovações tecnológicas estejam sob constante monitoramento, assegurando que o desenvolvimento tecnológico no âmbito administrativo respeite a legalidade e a proteção aos dados pessoais dos indivíduos.

Para Pinheiro, a governança digital exige a realização prévia de estudos de impacto regulatório e a instituição de auditorias periódicas, garantindo que os algoritmos empregados pelo Estado não atuem de forma arbitrária ou imprecisa, sob pena de nulidade dos atos administrativos e consequente responsabilização civil do ente público por danos decorrentes de decisões automatizadas sem supervisão adequada.

A segurança pública também se beneficiou do uso da inteligência artificial em políticas públicas. No contexto do serviço de inteligência policial, a IA tem o potencial de revolucionar a

coleta e análise de dados, a vigilância e a identificação de padrões criminosos, aumentando a eficiência e a precisão das operações (Barbuda; Vieira; Silva, 2024).

Algoritmos de aprendizado de máquina são empregados em sistemas de vigilância para monitorar atividades suspeitas e prevenir crimes, aumentando a capacidade das forças de segurança para prevenir e responder a incidentes. As informações coletadas podem ser usadas para identificar padrões de comportamento e antecipar possíveis ameaças, sendo que um dos principais benefícios da análise de dados é a capacidade de identificar padrões temporais e geográficos em atividades criminais. (Cardoso, 2025).

No Brasil, alguns poucos governos já começaram a aplicar tecnologias muito próximas daquelas utilizadas no campo internacional, como o Detecta (Governo de São Paulo), o Córtex (Governo Federal) e o Sistema de Atendimento e Despacho de Emergências (SADE) (PM do Paraná), de forma que, em maior ou menor grau, tais programas já se utilizam de tecnologias com algoritmos fazendo o cruzamento dos dados captados, e não apenas realizando o armazenamento (Ambrosio; Barbosa, 2024).

Inicialmente, cumpre destacar a implementação do Sistema de Atendimento e Despacho de Emergências (SADE) pelo governo do estado do Paraná cuja forma de operação consistia primordialmente em cruzar dados a fim de propiciar um deslocamento mais eficiente das forças policiais para os locais de maior risco de criminalidade. Com o passar do tempo, o sistema se aprimorou e ganhou uma proporção maior no policiamento preditivo através de mecanismos de análise das relações entre vítima, infrator e lugar favorecendo o estudo de locais com potencial maior de ocorrência de delitos.

No estado de São Paulo, o sistema Detecta (sistema inteligente de monitoramento criminal) vem alcançando resultados promissores tendo na sua atuação o emprego de técnicas de monitoramento e vigilância de vias e espaços públicos em diversos municípios do estado. E recentemente, o sistema evoluiu para a possibilidade de leitura de placas e seus fragmentos, armazenar a cor dos veículos e acessar o banco nacional de mandados de prisão integrados (Ambrosio; Barbosa, 2024), contribuindo assim, para um aumento do banco de dados e aperfeiçoamento dos métodos convencionais de atuação da polícia.

Conforme dados analisados, o Detecta contribuiu para 'a prisão de 4.731 pessoas em flagrante delito, interceptação de 3.320 veículos, apreensão de 276 armas de fogo e leitura de 200 bilhões de placas de automóveis' (Ambrosio; Barbosa, 2024). Recentemente, esse sistema foi integrado ao Programa Muralha Paulista que atua de forma mais abrangente conectando câmeras

de monitoramento e de reconhecimento facial e sensores e leitores de placas diretamente aos sistemas policiais.

Nesse contexto de centralização e compartilhamento de dados, sobressai a relevância de plataformas federais de vigilância integrada como o sistema Córtex, gerido pelo Ministério da Justiça e Segurança Pública. O Córtex atua como um repositório multibiométrico de larga escala, capaz de consolidar e cruzar, em tempo real, dados cadastrais, registros criminais e informações de tráfego veicular captadas por milhares de câmeras e sensores em todo o território nacional. Essa volumetria informacional, ao mesmo tempo que potencializa as capacidades de repressão estatal no âmbito de programas como o 'Muralha Paulista' em São Paulo, evidencia o risco iminente de monitoramento indiscriminado da população. A ausência de parâmetros legais rígidos para regular a interoperabilidade dessas bases de dados e o cruzamento automatizado de informações sensíveis gerava um cenário de acentuada desproteção, no qual o pragmatismo da eficiência policial sobrepujava as exigências de necessidade e proporcionalidade estrita.

O Estado da Bahia é um dos pioneiros no uso da IA no reconhecimento facial, em apoio às forças de segurança do Estado, principalmente para a Polícia Militar no tocante a tentativa de identificação e localização de foragidos da justiça e outros indivíduos procurados por quaisquer delitos que tenham praticado (Barbuda; Vieira; Silva, 2024).

Conforme preleciona Leal (2024), o Plano Nacional de Segurança Pública de 2018 introduziu, como estratégia nº 8, o videomonitoramento com reconhecimento facial biométrico, destacando-se as habilidades que softwares de computadores possuem de analisar rostos humanos constantes de uma base de dados específica, utilizando conexões de internet para catalogar indivíduos, via captação de sua biometria extraída por smartphones, computadores e câmeras de vigilância. Esta política pública, no Brasil, estava voltada precipuamente para a fiscalização de fronteiras, divisas interestaduais, portos, aeroportos, rodoviárias e ferrovias. Mas agora também espaços públicos urbanos estão sendo tomados por estes mecanismos, como ocorre na experiência da plataforma de videomonitoramento Smart Sampa, em São Paulo, que tinha como previsão integrar mais de 20 mil câmeras até 2024 na capital.

POLICIAMENTO PREDITIVO, VIESES ALGORÍTMICOS E SELETIVIDADE PENAL

No âmbito da inteligência artificial, uma de suas aplicações é a polícia preditiva voltada para a prevenção do crime através de pressupostos de análise criminológica.

O policiamento preditivo baseia-se em várias teorias estabelecidas do comportamento do crime e na oportunidade do crime, explicando a concentração e a repetição do crime, e por que o crime ocorre em alguns lugares e não em outros (Telles, 2021). Consiste na análise de dados e relatórios policiais através do uso de algoritmos que permitem identificar áreas de risco que apresentam maior ocorrência de delitos, propiciando assim, uma previsibilidade das ações criminosas, desencadeando dessa forma, uma alocação de recursos e policiais treinados para essas regiões, impactando positivamente na redução da criminalidade, de modo também a evitar reiteraões delitivas.

A fim de promover uma maior racionalidade na investigação criminal auxiliando na tomada de decisões, alguns softwares concentram-se nos lugares de risco, outros são baseados na pessoa, através do uso da ferramenta de reconhecimento facial.

Com a crescente utilização desses recursos tecnológicos, observa-se um aumento gigantesco da possibilidade de vigilância e controle do espaço público pelas forças de segurança pública. O que seria para um policial humano até mesmo impossível agora se tornou realidade, como detectar um veículo roubado pela placa numa rodovia cheia de veículos, reconhecer o rosto de um foragido na multidão, saber onde cada pessoa se encontra ou em um dado momento pela identificação do geoposicionamento do seu celular ou até mesmo possuir uma visão privilegiada de um cenário com o uso de drones (Telles, 2021).

Os ganhos operacionais advindos dos mecanismos tecnológicos inseridos na esfera penal através da análise comportamental, mapeamento de áreas de risco e reconhecimento facial por meio do videomonitoramento trouxeram benefícios inegáveis para o policiamento preditivo.

Diante dos desafios encontrados na gestão da segurança pública e com o crescente aperfeiçoamento das ações criminosas, a predição de crimes cujas técnicas analíticas são capazes de prever crimes propiciando uma intervenção policial mais precisa e eficaz contribui indubitavelmente para o processo de tomada de decisões além de oferecer mecanismos que aprimoram as técnicas de repressão, tornando-as mais qualificadas e sobretudo, favorecendo um policiamento ostensivo preventivo.

A disseminação de recursos tecnológicos no âmbito da segurança pública encontra ampla aceitação na medida em que é cada vez mais reconhecido que apenas um Estado repressivo não basta para combater uma criminalidade que cresce de forma exponencial nos dias atuais, sendo necessário a adoção de políticas públicas criminais preventivas que adotem estratégias eficazes.

Não se pode olvidar, entretanto, que esses softwares de vigilância eletrônica apesar de aprimorarem as técnicas investigativas e conseguirem vincular informações similares através dos algoritmos, são passíveis de falhas por serem dados meramente estatísticos que não abrangem as particularidades de cada caso concreto, não abrangendo, portanto, o contexto do delito de forma específica (Vieira; Santos, 2025).

Em que pese a adoção de mecanismos de inteligência artificial apresentar resultados inquestionáveis, alguns pontos sensíveis que podem comprometer sua confiabilidade e consequentemente sua eficácia precisam ser destacados, como os vieses algorítmicos que são capazes de contaminar os resultados reproduzindo frequentemente padrões discriminatórios e tendenciosos.

Essas ferramentas preditivas compreendem o homem a partir de uma perspectiva meramente estatística e por sua própria natureza, a IA não abarca a singularidade de cada comportamento e seu contexto único, o que é vital no âmbito da segurança pública e do processo penal. Exatamente por essa razão, é possível apontar exemplos de erros cometidos por softwares de IA que utilizam a tecnologia de predição, decorrentes de vieses existentes nas práticas do sistema criminal, as quais servem como base de dados para esses softwares (Vieira; Santos, 2025).

Conforme adverte Aury Lopes Jr. (2024), a justiça criminal não pode capitular diante de um 'tecnofetichismo' que substitui o juízo de valor e a presunção de inocência por métricas estatísticas de culpabilidade. O autor destaca que algoritmos preditivos, ao se basearem em registros históricos de ocorrências, operam como uma profecia autorrealizável, focando o aparato repressivo nas mesmas áreas e populações historicamente marginalizadas, comprometendo as garantias processuais fundamentais sob o pretexto de eficiência científica.

A advertência formulada pelo autor acerca do perigo de capitulação do processo penal perante o 'tecnofetichismo' judicial ganha especial relevo quando aplicada aos standards probatórios exigidos para a restrição de direitos fundamentais, como nas buscas pessoais e domiciliares. O autor sustenta que o conceito processual de 'fundada suspeita', previsto no artigo 244 do Código de Processo Penal para legitimar a busca sem mandado, constitui uma garantia

de cunho individualizado e concreto, a qual não pode ser preenchida por meras projeções probabilísticas extraídas de uma IA preditiva. Quando o aparato policial justifica a abordagem ou a invasão do domicílio unicamente com base no fato de que o algoritmo classificou aquele cidadão ou aquela coordenada geográfica como 'de alto risco', ocorre uma inadmissível inversão do ônus probatório. Transfere-se ao indivíduo o ônus de demonstrar a inconsistência de uma inferência de suspeição gerada por uma máquina, convertendo garantias constitucionais em barreiras de eficiência procedimental sob a égide de um neo- inquisitorialismo tecnológico.

Outrossim, como assevera Aury Lopes Jr. (2024), a crença cega na neutralidade científica dos softwares de inteligência artificial induz a um desarmamento crítico dos sujeitos processuais, em especial dos magistrados. Esse 'viés de automação' (automation bias) faz com que relatórios produzidos por sistemas preditivos ou softwares de reconhecimento facial sejam recebidos com uma presunção de veracidade científica quase inabalável, em detrimento de uma avaliação epistêmica crítica das fontes de prova. O resultado é o esvaziamento do princípio do livre convencimento motivado e do dever constitucional de fundamentação analítica das decisões judiciais (artigo 93, inciso IX, da Constituição Federal), uma vez que a argumentação jurídica do juiz é substituída pela mera adesão aos resultados estatísticos fornecidos por algoritmos de código-fonte fechado, os quais permanecem completamente inacessíveis à auditoria e à contestação pela defesa técnica do acusado.

Insta salientar que o policiamento preditivo não pode ocorrer de forma discricionária reproduzindo vieses discriminatórios que reforcem preconceitos e o racismo comumente observados no sistema penal brasileiro que embora contenha predominantemente traços do sistema inquisitório, sabe-se que na prática a justiça penal brasileira tem como um dos principais escopos a punição e satisfação de uma sociedade que impulsionada por dados crescentes de criminalidade e por insatisfações com o controle estatal sobre o crime, anseia por medidas punitivistas mais severas.

A “algoritmização” da vida, que está presente nas redes sociais e streamings, e tem ganhado espaço em inúmeros campos, tem influenciado cada vez mais políticas de segurança pública. A despeito disto, problemas de discriminação e preconceito estrutural em determinadas políticas desta natureza continuam os mesmos, e o uso discriminatório e preconceituoso da IA não pode tirar a responsabilidade do Estado (Leal, 2024).

Tal preocupação não é desmedida, pois dentre todos os prejuízos que um sistema algorítmico pode causar na esfera da segurança pública, aquele que demonstra maior

sensibilidade e impacto na discussão pública é justamente o potencial discriminatório que tais algoritmos podem causar, pois ao mesmo tempo que a ferramenta busca facilitar o combate e a prevenção ao crime, seu uso frequentemente acaba por abrir espaço para a discriminação racial e de gênero, o que não apenas é vedado pela Constituição Federal como, também, é tipificado na legislação penal brasileira (Ambrosio; Barbosa, 2024).

A discriminação algorítmica é um dos pontos críticos, uma vez que sistemas de IA, ao processarem grandes volumes de dados, podem reforçar preconceitos e desigualdades (Pinheiro, 2024). A discriminação racial e de gênero é um dos principais obstáculos ao amplo uso da inteligência artificial na esfera da segurança pública, pois conforme analisado nos artigos estudados, o sistema algorítmico apresenta vieses raciais discriminatórios numa frequência muito alta para serem ignorados e essas falhas precisam ser corrigidas primordialmente a fim de que não seja perpetuado um problema já destacado na justiça penal brasileira que frequentemente adota medidas punitivas mais severas contra uma população mais vulnerável.

Em perspectiva comparada, estudos internacionais como os de Cathy O'Neil (2020) sobre os 'algoritmos de destruição em massa' demonstram como modelos matemáticos pretensamente neutros codificam preconceitos históricos, amplificando as desigualdades sociais. No contexto brasileiro, como analisa Silvio Almeida (2019), o racismo estrutural molda as instituições de controle social, de modo que a alimentação de sistemas de aprendizado de máquina (machine learning) com dados policiados de maneira racista e seletiva apenas automatiza e perpetua a rotulagem de corpos negros como suspeitos preferenciais.

Conforme preleciona O'Neil, esses modelos matemáticos criam ciclos perniciosos de retroalimentação automática: ao direcionarem o patrulhamento ostensivo prioritariamente para as regiões classificadas pela base de dados histórica como violentas, os policiais realizam mais prisões em flagrante de pequenos delitos nessas áreas periféricas; esses novos dados de prisões em flagrante são reintroduzidos no sistema de IA, o qual 'confirma' que a região é de fato perigosa, exigindo ainda mais policiamento ostensivo ali. Quando essa lógica é transposta para o contexto nacional sob a lente do racismo estrutural analisado por Silvio Almeida (2019), o algoritmo atua como um poderoso instrumento de institucionalização e reprodução da seletividade penal, automatizando a suspeição baseada na cor da pele e na origem social e blindando a atuação discriminatória das agências policiais sob uma aparente máscara de neutralidade matemática e rigor computacional.

A vigilância (ou criminalização) automatizada, que decorre da atuação tecnopolítica de antecipar delitos e criar estratégias de segurança pública balizadas pelo tratamento de dados colhidos previamente, reproduz o *modus operandi* dos agentes de controle social, marcado pela seletividade das práticas de policiamento. Justamente devido aos vieses e à discriminação algorítmica, é importante indagar quais informações são empregadas para efetuar essas previsões, como elas são avaliadas pelas ferramentas tecnológicas e como isso repercute na maximização de chances de erros (Vieira; Santos, 2025).

O fenômeno da seletividade penal pode ser observado pela participação diminuta dos que não são da raça branca tanto na política como no sistema de justiça, que pode influenciar no Machine Learning da inteligência artificial, transformando o algoritmo em um meio para fornecer informações de cunho racista ou excludente. No âmbito do reconhecimento facial, a questão acima pontuada merece preocupação quanto ao emprego da tecnologia de reconhecimento facial, em especial para fins da alimentação dos bancos de dados, pois, caso as fotos e dados que são inseridos sejam apenas de condenados e/ou indivíduos que tenham sido identificados para fins investigatórios, por determinados tipos de delitos, a possibilidade de se considerar um resultado seletivo é muito grande. (Junior; Jorge, 2023).

A PORTARIA MJSP Nº 961/2025 E SUAS DIRETRIZES REGULAMENTARES

Destarte, cabe-se ressaltar que para que os avanços tecnológicos sejam bem-sucedidos, é necessário que haja respeito aos valores éticos e morais dos indivíduos de tal modo que seus direitos fundamentais não sejam violados.

Os principais entraves à utilização da inteligência artificial de uma forma mais abrangente e eficiente até então eram a falta de transparência dos órgãos públicos que fazem uso dessa ferramenta, e as lacunas que existiam na legislação brasileira que infelizmente não acompanharam o avanço da tecnologia de forma concomitante, fazendo assim com que o ordenamento jurídico brasileiro carecesse de regulamentações específicas que disciplinassem sobre os principais desafios e impactos do uso de algoritmos nas políticas de segurança pública.

Nesse contexto, deve-se enfatizar que embora a Lei Geral de Proteção de Dados (LGPD) tenha grande importância, tendo sido um marco revolucionário no tocante à proteção dos direitos fundamentais do indivíduo, como o direito à privacidade, ela não pode ser utilizada como único amparo legal na regulamentação dos instrumentos provenientes do desenvolvimento tecnológico

no âmbito da segurança pública, tendo em vista que na persecução penal o Estado faz uso rotineiramente de análise de dados pessoais, além do reconhecimento facial que frequentemente viola direitos individuais e apresenta vieses cognitivos, o que demonstra uma problemática que comprova que a aplicação da lei supracitada é insuficiente para legislar sobre assuntos referentes a essa temática.

Essa grave assimetria regulatória decorre, em grande medida, da exclusão expressa contida no artigo 4º, inciso III, alínea 'a', da LGPD, que estabelece a não aplicação das regras gerais de proteção de dados ao tratamento realizado para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. Como destaca a doutrina de Patrícia Peck Pinheiro (2024), essa lacuna legislativa deveria ser colmatada por meio de uma legislação específica de idêntico status normativo, o que se convencionou chamar no debate público e acadêmico de 'LGPD Penal'. Todavia, o prolongado atraso do Congresso Nacional na aprovação desse marco legislativo criou um vácuo no qual o Estado trata dados pessoais e biométricos de suspeitos e cidadãos sob regras vagas e fragmentadas. Embora a edição da Portaria nº 961/2025 pelo Ministério da Justiça represente um esforço de autorregulação estatal, ela padece de uma intransponível limitação de hierarquia normativa, uma vez que atos administrativos infralegais são desprovidos de competência constitucional para criar limitações legítimas a direitos e garantias fundamentais ou para substituir a exigência de reserva de lei formal.

Conforme destaca Cardoso (2025), outro dilema ético está no consentimento informado no uso da inteligência artificial, especialmente em relação à coleta e outras operações de tratamento de dados pessoais. Em muitas aplicações de inteligência artificial, os dados dos usuários são coletados, analisados e utilizados para tomar decisões ou personalizar experiências. Porém, na maior parte dessas situações, os indivíduos não têm plena consciência de como seus dados estão sendo utilizados ou das implicações de sua coleta, o que pode levar a controvérsias sobre a observância da Lei Geral de Proteção de Dados Pessoais, e o respeito à privacidade e à autodeterminação informativa.

A segurança pública, direito fundamental previsto no artigo 5 da Constituição de 1988 (Brasil, 1988) necessita de políticas públicas que o contemplem, podendo prevalecer sobre direitos individuais num contexto que abarque a coletividade. Entretanto, isso não significa um respeito ilimitado para uma inserção desenfreada de ferramentas tecnológicas que possam gerar riscos à sociedade, para que não haja assim, a mitigação de outros direitos fundamentais.

À luz do constitucionalismo e dos inúmeros questionamentos a respeito da aplicação da inteligência artificial na área criminal em virtude da proteção dos direitos fundamentais do cidadão, já se elucidou a necessidade de uma legislação específica que trate dessa temática estabelecendo as diretrizes do seu uso na persecução penal. Nesse contexto, cabe-se destacar uma importante medida adotada pelo Ministério da Justiça e Segurança Pública (MJSP) que ao regulamentar a Portaria MJSP nº 961/2025 (Brasil, 2025) definiu diretrizes para o uso da IA em atividades de investigação criminal e inteligência de segurança pública pelos órgãos federais de segurança, abrangendo também órgãos estaduais, municipais e distritais quando utilizarem recursos dos fundos nacionais de segurança pública e penitenciário. Trata-se de um marco que irá impactar positivamente na regulamentação do uso das inovações tecnológicas aliadas à proteção dos direitos fundamentais.

Dessa forma, é imperioso ressaltar o artigo 10 da referida portaria que dispõe da seguinte redação: 'A utilização de soluções de inteligência artificial nas atividades de investigação criminal e inteligência de segurança pública deverá ser proporcional, observar o dever de prevenção de riscos e as leis aplicáveis à espécie. Parágrafo único. Na hipótese de haver risco de lesão a direitos fundamentais, os agentes de segurança pública responsáveis pela aplicação das soluções referidas no caput revisarão o resultado da inferência algorítmica.' (Brasil, 2025, art. 10).

Não obstante a Portaria nº 961/2025, em seu artigo 10 e parágrafo único, pretenda salvaguardar o devido processo ao instituir a revisão humana obrigatória da inferência algorítmica diante do risco de lesão a direitos fundamentais, a eficácia desse mecanismo regulatório esbarra em sérios limites de ordem cognitiva e operacional. O 'viés de automação' indica que os agentes públicos, operando em rotinas de trabalho exaustivas e em condições de escassez de recursos técnicos, tendem a aceitar de forma acrítica as conclusões fornecidas pelos sistemas de inteligência artificial, adotando-as como um atalho cognitivo de legitimação de suas condutas. A previsão de supervisão humana (human-in-the-loop) corre, assim, o risco de ser reduzida a uma mera formalidade administrativa e burocrática, desprovida de qualquer conteúdo epistêmico de verificação e controle da idoneidade dos parâmetros de dados de entrada, servindo tão somente para conferir um verniz de legitimidade jurídica a uma decisão substancialmente automatizada pela máquina.

Impende notar que o momento para a criação dessa portaria fora extremamente oportuno em virtude de já ter sido destacado que as inovações tecnológicas cada vez mais presentes na

investigação criminal careciam de uma regulamentação específica para pautar critérios singulares para o seu uso, sendo que agora os diversos questionamentos que permeavam o uso da inteligência artificial no âmbito do direito penal poderão ser esclarecidos à luz dessa legislação.

Inicialmente faz-se necessário analisar que logo em seus primeiros artigos, a Portaria ressalta a proteção aos direitos fundamentais previstos na Constituição de 1988, demonstrando que mesmo diante da pertinência das investigações criminais, os interesses dos órgãos públicos jamais podem preponderar sobre os princípios constitucionais, estabelecendo, portanto, critérios para o uso de inteligência artificial como disposto no artigo 3º, que prevê o seguinte: 'esta portaria tem por objetivo assegurar: I- a legalidade, a adequação, a necessidade e a proporcionalidade como condições do uso de sistemas de tecnologia da informação nas atividades de investigação criminal e inteligência de segurança pública que possam gerar riscos à privacidade e a outros direitos fundamentais'. (Brasil, 2025, art. 3º).

Outrossim, assegura a padronização das técnicas e critérios norteadores da utilização da inteligência artificial, destacando valores como o direito à privacidade, ao sigilo das comunicações e dos dados pessoais, o respeito ao devido processo legal, a transparência nas ações de investigação criminal, entre outros, vedando de forma explícita e vinculante o 'uso indiscriminado, sem objetivo certo ou declarado, das soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública', ratificando assim, a necessidade de controle sobre o uso desmedido dessas ferramentas tecnológicas pela justiça criminal.

No tocante às atribuições dos órgãos de segurança pública, cumpre ressaltar que a portaria elucida as finalidades para as quais as inovações tecnológicas podem ser utilizadas nos estabelecimentos prisionais, como por exemplo, na detecção de dispositivos móveis apreendidos dentro das unidades prisionais com o fim exclusivo de que seja efetuado o bloqueio de sinais e a apreensão dos aparelhos, além de afirmar de forma categórica que para obtenção de dados sigilosos, os órgãos supracitados precisam de decisão judicial específica que autorize tal ação, demonstrando assim, nítida preocupação com a garantia dos direitos fundamentais dos indivíduos. (Brasil, 2025).

Ademais, vale destacar a importância dessa norma ao vedar aos órgãos referidos a utilização de soluções de inteligência artificial que permitam a identificação biométrica à distância, em tempo real, em espaços públicos, exceto em algumas situações de extrema relevância para o andamento das investigações criminais, como nos casos de instrução de

inquérito ou processo criminal em que a prova não puder ser obtida por outros meios disponíveis; na 'busca de vítimas de crimes, de pessoas desaparecidas ou em circunstâncias que envolvam ameaça grave e iminente à vida ou à integridade física de pessoas naturais'; no flagrante delito de crimes com pena privativa de liberdade máxima superior a dois anos; em recaptura de réus ou detentos envolvidos e por fim, em cumprimento de mandados de prisão e das medidas e penas previstas. (Brasil, 2025).

Nesse sentido, é imperioso salientar a importância dessas medidas que impuseram limitações aos videomonitoramentos que são constantemente alvo de debates por não terem sua eficácia comprovada na redução da criminalidade e sobretudo, por serem amplamente utilizados de forma abusiva expondo uma população mais vulnerável e aumentando os riscos de discriminação e uso indevido de dados.

Com efeito, merece destaque o Capítulo III da Portaria que contemplou as obrigações dos órgãos gestores, sendo de suma importância especificar detalhadamente as atribuições dos órgãos de segurança pública a fim de que estes possam desenvolver medidas estritamente necessárias e previstas nessa norma para que a implementação das inovações tecnológicas cumpra os requisitos desejados.

Ao dispor sobre o controle do acesso, ressaltando que apenas agentes no pleno exercício de suas funções e previamente autorizados possam incrementar o ingresso nas instalações e utilizar as inovações tecnológicas, a norma estabelece mesmo que de forma implícita a necessidade de capacitação para esses agentes a fim de que seja assegurada uma melhor operabilidade e padronização dos procedimentos para o uso de soluções de tecnologia da informação, conforme dispõe o artigo 3º da referida portaria. (Brasil, 2025).

Nessa vereda, assevera de forma incisiva que tão somente aos agentes que possuam prerrogativas correspondentes pode ser dado o acesso ao uso de perfis habilitados para atividades de inteligência, exigindo que estes agentes estejam lotados em órgãos com tal atribuição.

Aduz ainda, que deve ser implementado um controle capaz de estabelecer a 'adoção e a revisão periódica de perfis, que definam papéis, privilégios e direitos de acesso às funcionalidades e às informações, assim como regras para a sua concessão e revogação'.

Por oportuno, vale ressaltar que a norma contemplou ainda a observância ao princípio da transparência ao exigir que os órgãos de segurança pública adotem as medidas necessárias para garantir a transparência das contratações e a disponibilização de informações relevantes,

atualizadas e íntegras sobre os processos licitatórios através da incorporação de mecanismos de transparência, auditabilidade, responsabilização e prestação de contas. (BRASIL, 2025).

Ademais, instituiu que em até 90 dias, os órgãos supracitados deverão reavaliar e atualizar contratos, licitações e regulamentos vinculados ao uso de tecnologias em investigações criminais e inteligência de segurança pública, apresentando os ajustes e um plano de adequação para aprovação do ministro responsável. (Brasil, 2025).

Impende destacar a preocupação da referida norma com a capacitação dos usuários das ferramentas de inteligência artificial na investigação criminal ao dispor sobre esse assunto reiterando que o uso adequado que preserve valores éticos deve ser feito de forma responsável por agentes capacitados, além de serem adotadas medidas com o intuito de coibir o uso inadequado dessas soluções estratégicas, sob pena de estarem sujeitos à responsabilização nas esferas administrativa, civil e criminal.

Por esta forma, é viável observar a importância da avaliação periódica desses serviços tecnológicos, visto que seu acompanhamento supervisionado viabiliza sua evolução e manutenção adequada a fim de que possam ser feitas melhorias que aprimorem seu uso diante das necessidades que apresentar.

Nessa esteira, a Portaria ressalta o cuidado que deve ser feito na 'identificação e investigação de casos de acessos indevidos mediante a adoção de políticas de alerta contra usos maliciosos e atípicos das soluções tecnológicas' e através da realização periódica de auditorias e do monitoramento de eficácia das medidas de segurança técnicas, administrativas e organizacionais.

CONSIDERAÇÕES FINAIS: DESAFIOS PARA A CONSTITUCIONALIZAÇÃO DA INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA PÚBLICA

Diante do exposto, pode-se constatar que a implementação da inteligência artificial nas políticas de segurança pública deve ser feita de forma cautelosa e sempre observando os critérios para o seu uso de forma a impactar positivamente na redução da criminalidade sem mitigar os direitos dos cidadãos. Nessa vereda, há de se reconhecer que a Portaria MJSP nº 961/2025 (Brasil, 2025) surgiu em um momento extremamente necessário tendo em vista que o uso dos avanços tecnológicos na persecução penal carecia de uma legislação específica que preenchesse as lacunas existentes.

Noutro giro, deve-se destacar alguns pontos em que a referida norma suscita questionamentos relevantes, tendo em vista que apesar de ter representado um marco regulatório no âmbito da aplicação da inteligência artificial no direito penal, uma análise crítica necessita ser feita com o intuito de elucidar dúvidas que possam surgir.

Um dos pontos que merece destaque seria o possível fortalecimento exacerbado da atuação policial, podendo centralizar o controle do manejo das soluções tecnológicas apenas nas mãos de poucos reproduzindo técnicas repressivas e discriminatórias sem uma fiscalização por órgãos externos e sem atuação em conjunto de ouvidorias e defensorias responsáveis pela proteção de direitos fundamentais dos acusados, o que evidencia uma desigualdade na paridade de armas.

Essa centralização do controle policial na ausência de fiscalização por órgãos externos denota uma severa debilidade institucional. Sob a ótica constitucional, o controle externo da atividade policial é atribuição precípua do Ministério Público (art. 129, VII, CRFB/88), o qual deve exercer papel ativo na fiscalização das ferramentas de inteligência artificial empregadas pelas forças de segurança. A omissão da Portaria nº 961/2025 em articular canais de cooperação e prestação de contas (accountability) com o Ministério Público, com as Defensorias Públicas e com ouvidorias externas cria zonas de opacidade corporativa. Sem um controle externo técnico-jurídico independente, a 'autotutela' e o monitoramento interno previstos na norma tornam-se insuficientes para conter abusos procedimentais e o uso arbitrário de dados pessoais, enfraquecendo a proteção de direitos fundamentais e o equilíbrio democrático.

De fato, a ausência de canais externos e independentes de controle viola frontalmente os preceitos do republicanismo democrático e as garantias processuais do acusado. Ao silenciar sobre o papel do Ministério Público, do Conselho Nacional de Justiça, das Defensorias Públicas e de comitês técnicos independentes da sociedade civil na auditoria contínua dos sistemas preditivos, a Portaria nº 961/2025 cria zonas de opacidade corporativa infensas ao escrutínio externo. A autotutela e o controle estritamente internos previstos na portaria são insuficientes para conter desvios de finalidade e abusos de poder no tratamento de dados e nas investigações, aprofundando o desequilíbrio na paridade de armas que sustenta a estrutura do processo penal acusatório.

De igual modo, a lei é omissa no tocante à obtenção de dados, bem como deixa de dirimir de que forma a fiscalização será feita a fim de reduzir os vieses algorítmicos que contaminam uma investigação criminal e comprometem a efetividade do uso das soluções tecnológicas.

A omissão da Portaria nº 961/2025 em regular a obtenção e o tratamento de dados pessoais no âmbito penal ganha contornos dramáticos quando confrontada com a doutrina da cadeia de custódia da prova. Como assevera Geraldo Prado (2019), a idoneidade epistêmica e a integridade da prova digital exigem uma rastreabilidade rigorosa de todas as suas fases de captação e processamento. No campo da inteligência artificial, se as bases de dados alimentadoras do sistema forem opacas, incompletas ou de origem ilícita, o resultado da inferência algorítmica restará irremediavelmente contaminado (fenômeno do *garbage in, garbage out*). Ademais, a falta de regulação sobre a auditabilidade dos algoritmos — protegidos comercialmente sob o manto do segredo de negócio das empresas fornecedoras (caixa-preta algorítmica) — impossibilita a defesa de exercer o contraditório de forma plena. A paridade de armas, pilar do sistema processual penal acusatório, é frontalmente violada quando o réu é incapaz de periciar e contestar a lógica decisória que fundamentou uma medida constritiva ou cautelar em seu desfavor.

Conforme assegura Geraldo Prado (2019), a integridade epistêmica da prova penal exige a observância estrita das diretrizes que orientam a cadeia de custódia das evidências digitais, garantindo a rastreabilidade e a inalterabilidade das fontes de informação desde a fase de captação até o julgamento final. A omissão da Portaria nº 961/2025 em regular a cadeia de custódia de dados biométricos e estatísticos processados por inteligência artificial compromete irremediavelmente a confiabilidade do acervo probatório. Se as agências policiais se utilizam de bancos de dados opacos, sem registro detalhado de histórico de alimentação, treinamento e ponderação dos algoritmos (*logging técnico*), resta impossibilitada a realização de uma contraperícia defensiva eficaz. A ausência de regras sobre a auditabilidade dos softwares proprietários, blindados contratualmente sob a égide do segredo comercial, inviabiliza a paridade de armas e anula a presunção de inocência, ao impor ao réu a impossibilidade de periciar a racionalidade matemática que motivou sua restrição de liberdade.

Sendo assim, infere-se que, embora a Portaria nº 961/2025 represente um marco regulatório pioneiro ao estabelecer parâmetros procedimentais de governança e controle, ela se mostra insuficiente devido a lacunas estruturais críticas, notadamente a ausência de fiscalização por órgãos de controle externo e a falta de regulação sobre a cadeia de custódia das provas digitais, o que acaba por legitimar e perpetuar a seletividade penal histórica sob uma aparente neutralidade técnica. Somente com esse amparo normativo mais robusto será possível assegurar que a implementação da inteligência artificial nas políticas de segurança pública alcance a

efetividade desejada e produza resultados concretos na sociedade concomitantemente à preservação dos valores éticos e morais.

REFERÊNCIAS

ALMEIDA, Silvio. **Racismo Estrutural**. São Paulo: Pólen Livros, 2019.

AMBROSIO, G.P.F.; BARBOSA, A.L.J. O paradigma da implantação da inteligência artificial na segurança pública brasileira: regulação versus eficiência. **Revista de Estudos Jurídicos da UNESP**, v. 28, n. 48, 2024.

BARATTA, Alessandro. **Criminologia Crítica e Crítica do Direito Penal: introdução à sociologia do direito penal**. Rio de Janeiro: Revan, 2002.

BARBUDA, A.S.; VIEIRA, P.H.B.; SILVA, R.V. A aplicação da inteligência artificial na atividade de inteligência de segurança pública. **Revista Jurídica do Nordeste Mineiro**, v. 8, 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018].

BRASIL. Ministério da Justiça e Segurança Pública. Gabinete do Ministro. **Portaria MJSP nº 961, de 24 de junho de 2025**. Estabelece diretrizes sobre uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública. **Diário Oficial da União**, Seção 1, p. 104-105, 30 de junho de 2025.

CARDOSO, O. V. Inteligência artificial e políticas públicas: desafios regulatórios e perspectivas futuras. **Revista Jurídica da Presidência**, v. 27, n. 141, jan./abr. 2025.

JUNIOR, J.K.; JORGE, D.M. Inteligência artificial no reconhecimento facial em segurança pública: dados sensíveis e seletividade penal. **Revista Eletrônica Direito & TI**, Porto Alegre, v. 1, n. 15, jan./abr. 2023.

LEAL, R.G. Segurança pública e inteligência artificial: novos paradigms. **Int. J. Digit. Law**, Belo Horizonte, ano 5, n. 2, p. 81-99, maio/ago. 2024.

LOPES JR., Aury. **Direito Processual Penal**. São Paulo: Saraiva Educação, 2024.

O'NEIL, Cathy. **Algoritmos de destruição em massa: como o Big Data aumenta a desigualdade e ameaça a democracia**. Santo André: Editora Rua do Sabão, 2020.

PINHEIRO, F.M.L. O papel da tecnologia e da inteligência artificial na segurança pública: desafios e convergências com os direitos fundamentais individuais e sociais. **Revista do Ministério Público do Estado do Rio de Janeiro**, nº 94, out./dez. 2024.

PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Saraiva Educação, 2024.

PRADO, Geraldo. **A Cadeia de Custódia da Prova no Processo Penal**. Rio de Janeiro: Marcial Pons, 2019.

TELLES, P.S.B. Inteligência artificial e política preditiva: limites e possibilidades. **Boletim Científico ESMPU**, Brasília, a. 20, n. 57, jul./dez. 2021.

VIEIRA, A.B.C.; SANTOS, H.L.R. Investigação criminal e tecnologias digitais: algumas reflexões sobre o policiamento preditivo e a admissibilidade de provas digitais. **Revista Brasileira de Direito Processual Penal**, v. 11, n. 1, jan./abr. 2025.