

A UTILIZAÇÃO DE ALGORITMOS DE PREDIÇÃO CRIMINAL (PREDICTIVE POLICING) NO ÂMBITO DA POLÍCIA MILITAR DO ESTADO DO AMAZONAS: UMA ANÁLISE DA CONFORMIDADE COM A PROTEÇÃO DE DADOS E O PRINCÍPIO DA NÃO-DISCRIMINAÇÃO

THE USE OF CRIME PREDICTION ALGORITHMS (PREDICTIVE POLICING) WITHIN THE MILITARY POLICE OF THE STATE OF AMAZONAS: AN ANALYSIS OF COMPLIANCE WITH DATA PROTECTION AND THE PRINCIPLE OF NON-DISCRIMINATION

EL USO DE ALGORITMOS DE PREDICCIÓN DE DELITOS (PREDICTIVE POLICE) EN LA POLICÍA MILITAR DEL ESTADO DE AMAZONAS: UN ANÁLISIS DEL CUMPLIMIENTO DE LA PROTECCIÓN DE DATOS Y DEL PRINCIPIO DE NO DISCRIMINACIÓN

Jonathan Gomes da Silva¹
Denison Melo de Aguiar²
Flávio Humberto Pascarelli Lopes³
Bruno Patrício de Azevedo Campos⁴
Diego Bernardino da Silva⁵
Newton Suassuna da Silva Neto⁶

RESUMO: O presente artigo analisa o processo de tomada de decisão administrativa da Polícia Militar do Amazonas (PMAM) mediado por sistemas de inteligência artificial. O objeto central é a natureza jurídica do algoritmo policial como ato administrativo automatizado e sua conformidade com o ordenamento jurídico. O objetivo geral avalia a tensão entre a eficiência na alocação de recursos e a proteção de dados pessoais sensíveis, buscando identificar requisitos para que o policiamento preditivo não viole garantias constitucionais. A metodologia adota uma abordagem qualitativa e explicativa, utilizando os métodos dedutivo, bibliográfico e documental, além da análise de discurso. Os resultados indicam que a opacidade algorítmica e o uso de dados históricos viciados podem perpetuar a seletividade penal e o racismo estrutural. Conclui-se que a compatibilização tecnológica exige a adoção de um compliance algorítmico, garantindo a auditabilidade pelo Ministério Público e o direito à explicação humana. Tais balizas são fundamentais para assegurar que a inovação na segurança pública amazônica resulte em eficácia sem comprometer a dignidade e a liberdade do cidadão.

Palavras-chave: Policiamento Preditivo. Lei Geral de Proteção de Dados. Polícia Militar do Estado do AM. Não-discriminação. Ministério Público.

¹ Bacharelado em Segurança Pública e do Cidadão pela Universidade do Estado do Amazonas; Pós-graduado em Direito Público pela Universidade do Estado do Amazonas - UEA e Segurança Pública e Cidadania pela Facuminas. Bacharel em Direito pela UEA.

² Pós-Doutor UniSalento (Itália-2024), Doutor em Direito. Doutor em Direito pelo Programa de Pós-Graduação em Direito da Universidade Federal de Minas Gerais (PPGD/ UFMG). Mestre em Direito Ambiental pelo Programa de Pós- Graduação em Direito Ambiental da Universidade do Estado do Amazonas (PPGDA/ UEA). Advogado. Graduado em Direito pela Universidade da Amazônia (UNAMA/PA). Professor de ensino superior do curso de Direito da UEA. Professor da Academia de Polícia Militar do Amazonas (APM-PMAM). Professor de ensino superior do Centro Universitário de Ensino Superior do Amazonas (CIESA). Coordenador da Clínica de Mecanismos de soluções de Conflitos (MARbC/UEA). Coordenador da Clínica de Direito e Cidadania LGBTI (CLGBTI/UEA). Coordenador da Clínica de Direito dos Animais (YINUAKA-UEA). Editor-chefe da Revista Equidade. Integrante do Grupo de pesquisa Desafios do Acesso aos Direitos Humanos no Contexto Amazônico da Escola Superior da magistratura do Amazonas (ESMAM). Professor permanente do Programa de Pós-Graduação em Segurança Pública, cidadania e Direitos Humanos (PPGSP/UEA).

³ Pós-Doutor em Direito pela UniSalento. Bacharel em Direito pela Universidade Federal do Amazonas. Mestre em Direito pela Universidade Federal de Pernambuco. Doutor em Direito Constitucional pela Universidade de Fortaleza. Diretor da Escola Superior da Magistratura do Amazonas. Desembargador do Tribunal de Justiça do Estado do Amazonas.

⁴ Especialista em Docência do Ensino Superior pela Faculdade La Salle de Manaus - UNILASSALE, E em MBA em Gestão Estratégica da Administração Pública pela Faculdade Descomplica - DESCOMPLICA. Graduado em Direito pela Escola Superior Batista do Amazonas - ESBAM. Chefe do Estado Maior Geral e Coronel da Polícia Militar do Amazonas - PMAM. azevedoam@hotmail.com <http://lattes.cnpq.br/6612758484623284> <https://orcid.org/0009-0007-4983-6246>

⁵ Bacharel em Psicologia (Fametro-2012), Bacharel em Direito (Fametro-2020), Especialista em Psicologia Jurídica (Fametro-2015), Direito Constitucional (Facuminas-2022, Direito Penal (Facuminas-2022), Direito Processual Penal (Facuminas-2022) e Segurança Pública (Facuminas-2022). Bacharelado em Segurança Pública e do Cidadão pela Universidade do Estado do Amazonas (UEA). Cadete da Polícia Militar do Amazonas.

⁶ Graduação em Tecnologia em Gestão Financeira pela ESBAM. Especialista em direito penal pela UniBF. Cadete do curso de formação de Oficiais da Polícia Militar do Amazonas. Discente do curso de Bacharelado em Segurança Pública e do Cidadão pela Universidade do Estado do Amazonas (UEA).

ABSTRACT: This article analyzes the administrative decision-making process of the Amazonas Military Police (PMAM) mediated by artificial intelligence systems. The central focus is the legal nature of the police algorithm as an automated administrative act and its compliance with the legal system. The general objective is to evaluate the tension between efficiency in resource allocation and the protection of sensitive personal data, seeking to identify requirements so that predictive policing does not violate constitutional guarantees. The methodology adopts a qualitative and explanatory approach, using deductive, bibliographic, and documentary methods, in addition to discourse analysis. The results indicate that algorithmic opacity and the use of biased historical data can perpetuate penal selectivity and structural racism. It is concluded that technological compatibility requires the adoption of algorithmic compliance, guaranteeing auditability by the Public Prosecutor's Office and the right to human explanation. These guidelines are fundamental to ensuring that innovation in Amazonian public security results in effectiveness without compromising the dignity and freedom of the citizen.

Keywords: Predictive Policing. General Data Protection Law. Military Police of the State of Amazonas. Non-discrimination. Public Prosecutor's Office.

RESUMEN: Este artículo analiza el proceso de toma de decisiones administrativas de la Policía Militar del Amazonas (PMAM) mediado por sistemas de inteligencia artificial. El enfoque central es la naturaleza jurídica del algoritmo policial como acto administrativo automatizado y su conformidad con el ordenamiento jurídico. El objetivo general es evaluar la tensión entre la eficiencia en la asignación de recursos y la protección de datos personales sensibles, buscando identificar los requisitos para que la vigilancia predictiva no viole las garantías constitucionales. La metodología adopta un enfoque cualitativo y explicativo, utilizando métodos deductivos, bibliográficos y documentales, además del análisis del discurso. Los resultados indican que la opacidad algorítmica y el uso de datos históricos sesgados pueden perpetuar la selectividad penal y el racismo estructural. Se concluye que la compatibilidad tecnológica requiere la adopción de la conformidad algorítmica, garantizando la auditabilidad por parte del Ministerio Público y el derecho a la explicación humana. Estas directrices son fundamentales para asegurar que la innovación en la seguridad pública amazónica resulte en eficacia sin comprometer la dignidad y la libertad del ciudadano.

Palabras clave: Policía Predictiva. Ley General de Protección de Datos. Policía Militar del Estado de Amazonas. No discriminación. Ministerio Público.

INTRODUÇÃO

A segurança pública contemporânea atravessa uma transição paradigmática, migrando de modelos puramente reativos para estratégias proativas baseadas em dados. No estado do Amazonas, a Polícia Militar do Estado (PMAM) enfrenta o desafio de patrulhar uma geografia complexa e urbana, onde a eficiência operacional é vital. Nesse cenário, o uso de algoritmos de Predição Criminal (*Predictive Policing*) surge como uma ferramenta promissora, prometendo otimizar o alocamento de recursos e antecipar manchas criminais por meio da análise de grandes volumes de dados históricos.

O policiamento preditivo, geralmente descreve qualquer sistema que analisa dados disponíveis para prever onde um crime pode ocorrer em um determinado período de tempo, baseado em local, ou quem estará envolvido em um crime como vítima ou perpetrador, baseado em pessoa (BRAGA, 2019).

Assim, o objetivo do policiamento preditivo é a prevenção de ocorrências de crimes ocorrendo assim a otimização na tomada de decisão e eficácia no cumprimento da missão

institucional de polícia preventiva, preservar a ordem pública e o meio ambiente do estado do Amazonas mediante um policiamento ostensivo de excelência (CAVALCANTE, 2024 p. 12 apud MORAES, 2022).

Entretanto, a implementação dessas tecnologias não ocorre em um vácuo ético ou jurídico. A coleta e o processamento de dados para fins de segurança pública encontram limites fundamentais na Lei Geral de Proteção de Dados (LGPD) — e especificamente na discussão sobre a "LGPD Penal". A tensão reside no equilíbrio entre o legítimo interesse do Estado em garantir a ordem pública e o direito individual à privacidade e à autodeterminação informativa (BOFF, 2014).

Além da proteção de dados, surge um debate crítico sobre o Princípio da Não-Discriminação. Algoritmos de predição, se alimentados por bases de dados que refletem preconceitos históricos ou atuação repressiva em determinadas áreas periféricas, correm o risco de perpetuar e automatizar o racismo estrutural e a estigmatização de comunidades vulneráveis. O fenômeno conhecido como feedback loop, onde a polícia é enviada para reprimir, onde sempre foi, gerando mais prisões e retroalimentando o algoritmo com os mesmos dados, coloca em xeque a imparcialidade estatal (NUNES, 2019).

Este artigo propõe analisar como a Polícia Militar do Estado do Amazonas pode integrar ferramentas de inteligência preditiva sem violar os direitos fundamentais. Através de uma revisão bibliográfica e documental, busca-se responder: é possível conciliar a eficiência algorítmica com o rigor da proteção de dados e a garantia de um policiamento que não discrimine por raça ou CEP? O objetivo é delinear diretrizes que assegurem que a inovação tecnológica na Amazônia sirva como instrumento de justiça, e não como uma nova máscara para velhas desigualdades.

O **objeto do trabalho** em exame é o processo de tomada de decisão administrativa da Polícia Militar do Amazonas (PMAM), usando de sua discricionariedade na tomada de decisão quando mediado por sistemas de inteligência artificial para policiamento preditivo. Analisando o software de predição não como mera ferramenta técnica, mas como um ato administrativo automatizado que deve obediência aos princípios da legalidade, impessoalidade e publicidade, conceituando assim a natureza jurídica do algoritmo Policial, como é em qualquer atuação da Administração Pública (DI PEITRO, 2023).

Isso será possível compreendendo o fluxo de dados sensíveis que ocorre com o tratamento de informações de segurança pública sob a ótica da Lei Geral de Proteção de Dados,

especificamente no que tange à coleta e processamento de dados que podem levar à estigmatização de grupos ou territórios no Amazonas.

Outro elemento em análise por consequência do exposto é a seletividade tecnológica que gera o “confronto” entre a eficiência operacional (alocação de viaturas e efetivo) e a proteção de direitos fundamentais (presunção de inocência e não-discriminação), observando se a “neutralidade” do algoritmo pode mascarar preconceitos estruturais.

A abordagem apresenta **justificativa** na necessidade premente de compreender as transformações tecnológicas na segurança pública sob o prisma do Estado Democrático de Direito, estruturando-se em três pilares fundamentais.

O primeiro é a relevância acadêmica, que consiste no fortalecimento do pensamento jurídico amazônida. Diante da carência de estudos locais, este trabalho busca preencher a lacuna sobre a intersecção entre Inteligência Artificial e Direito Público na Amazônia. A obra desafia a academia regional, como a Universidade do Estado do Amazonas e a Academia de Polícia Militar Coronel Neper da Silveira Alencar, a assumir o protagonismo na construção de um Direito Digital Amazônico. Ao debater o policiamento preditivo, estimula-se a produção de um saber jurídico que considere as peculiaridades e as dimensões continentais da segurança pública no estado.

4

O segundo pilar é a relevância científica, que busca inovação na linha de pesquisa de direito público. O trabalho contribui para o Direito Público ao investigar a validade do ato administrativo automatizado, tema de fronteira na modernização do Estado. A pesquisa fornece critérios de legalidade e governança de dados que fundamentam futuros estudos científicos, permitindo que a produção acadêmica amazônica dialogue em igualdade com centros globais de tecnologia e direito.

Por fim o ultimo pilar, a relevância social, que é a proteção e eficiência para a sociedade amazônida. Essa, marcada por profundas desigualdades socioeconômicas e por uma diversidade étnica e cultural única, é a maior interessada, e a mais vulnerável na implementação dessas tecnologias.

A importância da pesquisa é evidenciada pois o uso de algoritmos sem controle pode gerar uma “guetização” digital de bairros periféricos de Manaus ou comunidades do interior, intensificando a seletividade penal.

O trabalho busca garantir que a busca por eficiência - polícia chegando mais rápido onde o crime ocorre - não se transforme em estigmatização, polícia abordando pessoas com base

em preconceitos de código. Ao final, o trabalho serve como um mecanismo de defesa da cidadania, assegurando que a inovação tecnológica na Polícia Militar do Estado do Amazonas resulte em segurança real, sem comprometer a liberdade e a dignidade do cidadão amazonense.

Nessa abordagem, a missão da Polícia Militar do Amazonas de preservar a ordem pública e meio ambiente mediante um policiamento ostensivo preventivo, sendo a prevenção criminal o alicerce da atuação policial milita, o policiamento preditivo é instrumento imprescindível para a concretude dessa missão.

O **objetivo da obra** é compreender como funciona o policiamento predito, o uso de dados automatizado pela administração pública como forma de garantir a eficácia administrativa sem violar os direitos e garantias fundamentais.

O **objetivo geral da pesquisa** é avaliar a tensão entre a eficiência administrativa na alocação de recursos policiais via inteligência artificial e a proteção de dados pessoais sensíveis no âmbito da Polícia Militar do Amazonas, buscando identificar os requisitos necessários para que o policiamento preditivo atue como ferramenta de gestão pública sem violar as garantias individuais consagradas na Constituição Federal de 1988. **Os objetivos específicos** são: 1 - compreender o funcionamento do policiamento preditivo e sua fundamentação no Direito Administrativo; 2 - analisar o regime jurídico da Lei Geral de Proteção de Dados frente às atividades de Segurança Pública; 3 - Identificar os riscos de violação de garantias individuais e a formação de vieses algorítmicos; e 4 - propor balizas para o controle externo e a tutela coletiva pelo Ministério Público.

5

A pesquisa investiga como compatibilizar o policiamento preditivo na PMAM com a transparência e a não-discriminação da Lei Geral de Proteção de Dados (LGPD), evitando que a eficiência gere seletividade penal. A hipótese sustenta que o uso de algoritmos opacos (caixa-preta) baseados em dados históricos viciados viola direitos fundamentais, mas que tal conflito pode ser mitigado por um compliance algorítmico que assegure a auditabilidade pelo Ministério Público e o direito à explicação humana.

A pesquisa será conduzida sob uma abordagem qualitativa, utilizando o método dedutivo, partindo da análise das normas gerais como a Constituição Federal da República Federativa do Brasil de 1981 e a Lei Geral de Proteção de Dados, para a compreensão do fenômeno específico, policiamento preditivo na Polícia Militar do Estado do Amazonas. A presente investigação adota uma abordagem que se subdivide nos seguintes critérios.

O primeiro se refere a natureza e abordagem, consistindo em uma pesquisa qualitativa,

uma vez que não busca a mensuração estatística de dados, mas sim a interpretação e a compreensão profunda dos fenômenos jurídicos. O foco está na análise da validade e da legitimidade do uso de algoritmos, interpretando-os à luz dos princípios constitucionais e das normas de proteção de dados.

O **segundo critério envolve os objetivos, materializando-se em uma pesquisa explicativa ou causal.** Diferente da pesquisa meramente descritiva, que apenas narra o que é a Inteligência Artificial (IA), esta pesquisa é explicativa. Ela busca identificar os fatores determinantes, causas, que levam um algoritmo de policiamento a gerar resultados discriminatórios. O objetivo é explicar a relação de causalidade entre a opacidade algorítmica e a violação de direitos fundamentais, propondo soluções jurídicas para mitigar esses efeitos.

A **técnicas de pesquisa se utilizará de documentação via revisão** sistemática da literatura especializada, nacional.

DISCUSSÃO E RESULTADOS

I. A TRANSIÇÃO PARA O POLICIAMENTO PROATIVO NO AMAZONAS

Historicamente, a atuação das forças de segurança pública no Brasil, e de forma acentuada na região amazônica, pautou-se por um modelo predominantemente reativo, o chamado “policiamento de incidentes”. Nesse paradigma, a Polícia Militar do Estado do Amazonas era acionada prioritariamente após a consumação do ilícito, operando em uma lógica de resposta a chamados via Centro Integrado de Operações - CIOPs ou patrulhamento ostensivo sem o suporte de análise de dados em tempo real. Contudo, o aumento da complexidade da criminalidade organizada e as particularidades geográficas do Amazonas — que exigem uma gestão estratégica de recursos escassos em um território vasto — impulsionam a migração para o Policiamento Proativo.

A transição para o modelo proativo no Amazonas não é apenas uma mudança tática, mas uma evolução doutrinária. Ela se fundamenta na premissa de que a segurança pública deve atuar nas causas e nos padrões criminais antes que o delito ocorra, em consonância com a missão institucional da Polícia Militar do Amazonas. No contexto de Manaus e das cidades polos do interior, essa transição é catalisada pela necessidade de otimizar o emprego do efetivo e das viaturas. O policiamento deixa de ser uma atividade baseada puramente na intuição do comandante ou na aleatoriedade do patrulhamento e passa a ser orientado pela inteligência e pela estatística criminal.

Nesse cenário, o advento das tecnologias de informação permite à Polícia Militar do

Estado do Amazonas integrar bases de dados que mapeiam as chamados "manchas criminais" (*hotspots*). A proatividade, portanto, manifesta-se no esforço de antecipação: o Estado não mais aguarda o crime para agir, mas posiciona-se de forma estratégica com base na probabilidade de ocorrência. Entretanto, essa modernização traz consigo o desafio de conciliar a rapidez da resposta operacional com o respeito absoluto aos limites da legalidade administrativa e aos direitos fundamentais, uma vez que a eficácia da prevenção não pode atropelar as garantias individuais consagradas no Estado Democrático de Direito e basilados nos princípios da Administração Pública, conforme preleciona CARVALHO FILHO (2014, p. 18):

Os princípios constantes do Direito Administrativo são os postulados fundamentais que inspiram todo o modo de agir da Administração Pública. Representam cânones pré-normativos, norteando a conduta do Estado quando no exercício de atividades administrativas.

Esta mudança de paradigma é o pano de fundo necessário para compreender a introdução do policiamento preditivo (*predictive policing*). Se o policiamento proativo é a intenção de agir antecipadamente, os algoritmos são as ferramentas que prometem viabilizar essa intenção com precisão cirúrgica. Contudo, no Amazonas, onde a diversidade social e as desigualdades territoriais são latentes, essa transição exige uma análise crítica sobre como tais dados são coletados e processados, sob pena de automatizarmos preconceitos estruturais em nome de uma suposta eficiência técnica.

7

2. DEFINIÇÃO E ESCOPO DO POLICIAMENTO PREDITIVO (*PREDICTIVE POLICING*)

O policiamento preditivo não deve ser compreendido como uma tecnologia isolada, mas como um método analítico que utiliza algoritmos e processamento de grandes volumes de dados para identificar alvos e locais de potencial atividade criminal. De forma técnica, essa ferramenta geralmente descreve qualquer sistema que analisa dados disponíveis para prever onde um crime pode ocorrer em um determinado período de tempo (foco no local) ou quem estará envolvido em um crime como vítima ou perpetrador (foco na pessoa), nesse sentido, RODRIGUES (2013, p. 51, *apud* CHAN, et al. 2018, p. 807) conceitua o policiamento preditivo:

Como um fenômeno, o policiamento preditivo é mais do que um conjunto de ferramentas. O policiamento preditivo é também uma premissa de que é possível utilizar a tecnologia para prever crimes antes mesmo dele ocorrer, que os instrumentos de previsão podem realizar tal previsão com precisão, e que a polícia utilizará este conhecimento eficazmente para reduzir a criminalidade.

O escopo desta ferramenta no âmbito da segurança pública é, essencialmente, a **prevenção de ocorrências de crimes**. Ao permitir a otimização na tomada de decisão, o

policciamento preditivo busca conferir maior eficácia ao cumprimento da missão institucional da Polícia Militar, que consiste em preservar a ordem pública e o meio ambiente mediante um policiamento ostensivo de excelência. Afirma-se, portanto, que esta tecnologia está intimamente relacionada com as políticas criminais em sua fase instrumental e operacional.

Antes de analisarmos propriamente a aplicação do Policiamento Preditivo, é necessário distinguir dado, informação e conhecimento. Dado é o registro isolado de um evento, objetivo como, data do fato, local, endereço. Já a informação é o conjunto de dados processados com significados para o sistema e contexto definido, *verbi gratia*, o boletim de ocorrência preenchido com os dados da ocorrência. Por fim, conhecimento é o resultado de ações e interações entre sujeitos e objetos, é a informação devidamente tratada, como casos extraídos do QlikView, uma plataforma líder de *Business Intelligence* (BI) e análise de dados, focada no conceito de inteligência de negócios direcionada ao usuário final (JUNIOR 2021, et al, p.37)

Compreendendo esses conceitos, a aplicação do *predictive policing* divide-se em quatro categorias operacionais principais.

O primeiro é o método de previsão de crimes utilizados para identificar locais e tempos de maior risco de ocorrência criminosa. Como exemplo, temos os dados estatísticos da Segurança Pública do Estado do Amazonas disponíveis no Sistema *Powerbi*⁷, em que há registro de mortes, crimes contra o patrimônio, crimes contra o idoso, pessoas desaparecidas roubo e localização de veículos, mulher vítimas de violência doméstica, crimes contra criança e adolescente, apreensões de armas e drogas, crimes ambientais e outros.

Com demonstração podemos pegar por amostragem os crimes contra o patrimônio no Estado do Amazonas:

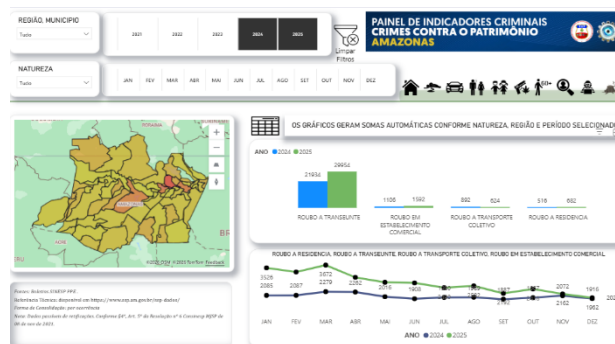


Imagem 01 – Crimes contra o patrimônio no estado do Amazonas. Por SSP AM

⁷Disponível em: <https://app.powerbi.com/view?r=eyJrIjoiYWQ1OTIzODUtZjg2OS00NmJhLTgzMmUtNGIwZjIzOGYxNWVliiwidCI6Ijg1NDczOTk4LTZmODRlNDExYzYk3LTg3YWUwNGUzMTIwNCJ9>. Acesso em: 23/01/2025

Na supracitada imagem, o uso do Policiamento preditivo indicará um desdobramento de tropa aos municípios com maior mancha criminal de crimes contra o patrimônio, que foram, no ano de 2025, respectivamente, Manaus, Manacapuru e Coari.

O segundo métodos é a previsão de infratores, que buscam identificar indivíduos com maior probabilidade de cometer crimes no futuro. Esse, consiste na utilização de técnicas de análise algorítmica e mineração de grandes bases de dados para identificar indivíduos que, segundo padrões estatísticos previamente definidos, apresentariam maior probabilidade de envolvimento em práticas criminosas no futuro. Esse modelo, também denominado *person-based predictive policing*, opera a partir do cruzamento de variáveis como histórico criminal, vínculos sociais, localização, recorrência de abordagens policiais e outros dados socioespaciais, convertendo trajetórias de vida em indicadores de risco.

Outro método é o de previsão de identidades de perpetradores, voltados para criar perfis de suspeitos em investigações em curso. Esse se utiliza da método do *profiling*, conforme definição de OLIVEIRA (2021, p. 13):

(...)de um modo geral, é uma técnica de análise e resposta comportamental, inicialmente baseada na análise da pessoa com quem está interagindo e, se possível, registrando os fatos para que seja possível analisar os dados coletados.

9

Com base nesses dados comportamentais, é possível prever um comportamento desviante levando em consideração os registros comportamentais de indivíduos suspeitos que estão sendo investigados, o *Criminal Profiling*.

Por fim, tem o método de previsão de vítimas de crimes, destinados a identificar grupos ou indivíduos vulneráveis a ataques, intimamente ligado a vitimologia.

Assim, diferente do policiamento tradicional, que depende da presença física e da observação empírica do agente, o escopo preditivo transfere parte da carga decisória para modelos estatísticos. No estado do Amazonas, essa ferramenta surge com a promessa de antecipar "manchas criminais", permitindo que o comando da corporação antecipe o posicionamento de viaturas e efetivo antes que o delito se consume. Todavia, como o objetivo das políticas criminais engloba a adoção de soluções práticas para a prevenção de condutas, o escopo desses sistemas deve estar obrigatoriamente alinhado aos princípios administrativos e penais, sob pena de desvio de finalidade.

3. A NATUREZA JURÍDICA DO ALGORITMO POLICIAL COMO ATO ADMINISTRATIVO AUTOMATIZADO

A introdução de algoritmos de predição criminal na Polícia Militar do Amazonas não representa apenas um upgrade tecnológico, mas uma alteração na própria dinâmica da formação do ato administrativo. No contexto da Segurança Pública Datificada, a utilização de *Big Data* permite à polícia processar volumes massivos de informações para orientar o patrulhamento (RODRIGUES, 2022). Juridicamente, o *output* gerado por esses sistemas deve ser compreendido como um ato administrativo automatizado, o qual, embora execute uma tarefa técnica, permanece submetido aos princípios da legalidade, impessoalidade e motivação.

A doutrina destaca que a inteligência artificial aplicada ao policiamento opera sob uma lógica de "antecipação", buscando prever comportamentos e locais de crime (OLIVEIRA JUNIOR; SANTOS, 2022). Entretanto, essa transição para decisões mediadas por máquinas introduz o desafio da "opacidade algorítmica". Conforme aponta Braga (2019), a utilização de sistemas de "caixa-preta" (*black boxes*) pode comprometer a transparência administrativa, uma vez que o processo decisório do algoritmo muitas vezes é inacessível até mesmo para os próprios gestores da segurança pública.

Nesse cenário, a discricionariedade de um Comandante ao alocar o efetivo passa a ser mediada por uma "discricionariedade técnica" do algoritmo. Como ressalta Lucena (2019), há um risco inerente de que a tecnologia, ao invés de neutralizar preconceitos, acabe por conferir uma roupagem de objetividade científica a práticas de racismo algorítmico. Portanto, a natureza jurídica desse ato exige que ele seja passível de auditoria, especialmente considerando que a proteção de dados pessoais é um pilar fundamental no espaço de liberdade, segurança e justiça, conforme o modelo adotado pela União Europeia (CORREIA; JESUS, 2014).

A validade do algoritmo como instrumento de gestão pública na Amazônia depende, assim, de sua conformidade com o devido processo informacional. Como o crime não é um evento aleatório, mas possui padrões, a tecnologia pode ser uma aliada da eficiência; contudo, a "neutralidade" do dado é um mito se não considerarmos que o dado é fruto de escolhas humanas prévias (CAVALCANTE, 2024). Assim, o ato administrativo mediado por Inteligência Artificial (IA) na PMAM só será legítimo se for transparente, motivado e imune a reproduções de seletividade penal.

4. DISCRICIONARIEDADE TÉCNICA E O PRINCÍPIO DA EFICIÊNCIA NA POLÍCIA MILITAR DO ESTADO DO AMAZONAS

A busca pela eficiência na Administração Pública, elevada a princípio constitucional pela Emenda nº 19/98, encontra no policiamento preditivo uma de suas expressões mais ambiciosas no século XXI. No âmbito da Polícia Militar do Amazonas, a alocação de recursos humanos e logísticos — tradicionalmente inserida no campo da discricionariedade do Comandante — passa a ser orientada por uma discricionariedade técnica mediada por dados. A premissa é que a inteligência artificial, ao processar volumes massivos de informações (*Big Data*), permita que a segurança pública atue de forma gerencial, otimizando o posicionamento de viaturas em áreas de maior probabilidade criminal.

Contudo, a eficiência não pode ser interpretada de forma isolada, sob o risco de atropelar garantias individuais. A doutrina alerta que a "eficiência" algorítmica muitas vezes mascara uma seletividade tecnológica. Isso ocorre porque os algoritmos não são entes neutros; eles são programados por seres humanos e alimentados por dados que podem refletir práticas policiais viciadas do passado. Assim, a escolha técnica do software sobre onde patrulhar pode acabar por reproduzir padrões históricos de criminalização de determinados territórios e grupos sociais no Amazonas.

11

A discricionariedade técnica, portanto, não afasta o dever de motivação do ato administrativo. Se um algoritmo indica o deslocamento de tropa para um bairro periférico de Manaus em detrimento de outro, essa "sugestão" tecnológica deve ser passível de explicação e controle. A eficiência, no contexto do Direito Público, deve ser entendida como a busca pelo melhor resultado para a sociedade com o menor sacrifício possível de direitos fundamentais.

Dessa forma, a implementação dessas ferramentas na Polícia Militar do Amazonas (PMAM) exige que a eficiência administrativa seja equilibrada com o princípio da impessoalidade. A inovação tecnológica só cumprirá seu papel gerencial se for utilizada para democratizar o acesso à segurança pública, e não para automatizar a estigmatização de bairros e cidadãos amazonenses sob o pretexto de otimização de recursos.

5. LIMITES ÉTICOS E JURÍDICOS DA ATUAÇÃO PREDITIVA

A implementação do policiamento preditivo não ocorre em um vácuo ético, mas em um campo de intensas tensões normativas entre a pretensão de segurança estatal e a preservação da dignidade humana. A utilização de algoritmos na Polícia Militar do Amazonas deve respeitar

limites intransponíveis que impedem a prevalência da técnica sobre o Direito, especialmente no que tange à transparência e à vedação de práticas discriminatórias.

O primeiro limite fundamental é a **transparência algorítmica**. A doutrina alerta para o risco dos sistemas de "caixa-preta" (*black box*), cuja opacidade impede que o cidadão e os órgãos de controle compreendam os critérios que levaram à indicação de uma determinada "mancha criminal" ou à suspeição de um indivíduo. Sob a ótica do Direito Público, a falta de explicabilidade compromete o dever de motivação do ato administrativo e o exercício do contraditório, uma vez que não se pode contestar uma decisão cujos fundamentos técnicos são inacessíveis.

Outro limite ético-jurídico essencial é a **proteção contra o viés discriminatório**, nesse sentido preleciona SILVA NETO, F. M. M. da, MIYADAIRA, F. Y., & MELO DE AGUIAR, D. (2025):

Nesse novo horizonte, a Polícia Militar é desafiada a transcender sua origem repressora para se consolidar como agente de cidadania, abandonando a lógica do confronto para atuar como garantidora dos direitos fundamentais e da dignidade das populações historicamente marginalizadas.

Como o crime não é um evento aleatório, mas um fenômeno influenciado por padrões geográficos e sociais, a alimentação de algoritmos com dados históricos que refletem um policiamento historicamente seletivo pode gerar o efeito de *feedback loop*. Nesse ciclo, a tecnologia passa a retroalimentar preconceitos, direcionando o braço armado do Estado prioritariamente para territórios periféricos e grupos vulnerabilizados, o que configura uma seletividade penal automatizada.

Ademais, a atuação preditiva encontra balizas na **Lei Geral de Proteção de Dados (LGPD)**, especificamente no que tange à autodeterminação informativa. O tratamento de dados sensíveis para fins de segurança pública não é absoluto; ele deve observar os princípios da finalidade, necessidade e adequação, nos termos do art. 2º da Lei nº 13.709, de 14 de agosto de 2018, evitando a coleta indiscriminada de informações que possam levar à vigilância em massa ou à estigmatização social.

Dessa forma, os limites éticos e jurídicos em consonância com a dignidade da pessoa humana exigem que a inovação na PMAM seja acompanhada de mecanismos de prestação de contas (*accountability*) e auditoria externa.

A dignidade da pessoa humana, macroprincípio consagrado na Constituição Federal, é um valor essencial que permeia todos os direitos fundamentais, fornecendo uma base sólida para a avaliação de sua inviolabilidade. Ao utilizar drones para policiamento, é necessário garantir que essa dignidade não seja comprometida, mesmo quando se busca promover a segurança pública. (LOUREIRO et al;

AGUIAR, 2025).

A ciência aplicada à segurança pública no Amazonas só será legítima se assegurar que o algoritmo funcione como um suporte à decisão humana qualificada, e nunca como um substituto soberano da justiça e da igualdade perante a lei, respeitando a dignidade da pessoa humana.

6. O REGIME JURÍDICO DA PROTEÇÃO DE DADOS NA SEGURANÇA PÚBLICA

A aplicabilidade da Lei nº 13.853, de 08 de julho de 2019, no âmbito da segurança pública enfrenta desafios estruturais devido à exclusão parcial prevista em seu art. 4º, inciso III, que afasta a incidência da norma geral sobre o tratamento de dados para fins de segurança pública e persecução penal (BRASIL, 2019). Essa lacuna normativa gera uma insegurança jurídica quanto aos limites da coleta e processamento de informações sensíveis, exigindo a urgente promulgação de uma "Lei Geral de Proteção de Dados" Penal" que harmonize a eficácia das investigações com a proteção de direitos fundamentais, como a autodeterminação informativa e a privacidade.

No contexto brasileiro, enquanto essa legislação específica não é consolidada, a atuação estatal deve se pautar pela aplicação direta dos princípios constitucionais e por balizas interpretativas que evitem a vigilância desproporcional, garantindo que o combate à criminalidade, inclusive no ambiente cibernético, não resulte em um retrocesso nas garantias individuais dos cidadãos, ocasionando uma proteção deficiente.

13

7. O FLUXO DE DADOS SENSÍVEIS E A AUTODETERMINAÇÃO INFORMATIVA

A discussão sobre o fluxo de dados sensíveis e a autodeterminação informativa ganha relevância no contexto da segurança pública, especialmente quando se observa a atuação da Polícia Militar do Amazonas (PMAM). A Lei Geral de Proteção de Dados (LGPD) estabelece parâmetros para o tratamento de informações pessoais, impondo limites e responsabilidades que impactam diretamente as corporações policiais.

Segundo Santos (2024), “a aplicação da LGPD [...] apresenta inúmeros desafios devido à sensibilidade dos dados tratados e à necessidade de garantir a segurança pública” (SANTOS, 2024, p. 10). No âmbito da PMAM, que atua em uma região marcada por peculiaridades geográficas e sociais, como a vasta extensão territorial e a diversidade cultural da Amazônia, o fluxo de dados sensíveis precisa ser compatibilizado com a realidade operacional da corporação.

A autodeterminação informativa, entendida como o direito do indivíduo de controlar

seus próprios dados, encontra respaldo na Constituição Federal, que assegura “a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas” (BRASIL, 1988, art. 5º, X). Nesse sentido, a PMAM deve adotar práticas que respeitem tais garantias, mesmo diante da necessidade de coleta e tratamento de informações para fins de segurança.

O desafio está em equilibrar a proteção da privacidade com a eficácia das investigações e operações policiais. Como destaca Chuy (2021), o anteprojeto da chamada “LGPD Penal” busca “equilibrar tanto a proteção do titular contra mau uso e abusos como acesso de autoridades a todo potencial de ferramentas e plataformas modernas para segurança pública e investigações” (CHUY, 2021, p. 3). Essa perspectiva é essencial para a PMAM, que frequentemente lida com dados sensíveis em operações de inteligência e policiamento ostensivo.

Além disso, a LGPD prevê que “o tratamento de dados pessoais deve ser realizado apenas para finalidades específicas, legítimas e necessárias para a investigação policial” (SANTOS, 2024, p. 11). No caso da PMAM, isso implica em estabelecer protocolos claros para coleta, armazenamento e compartilhamento de dados, evitando excessos e garantindo proporcionalidade.

Outro ponto relevante é a necessidade de adoção de técnicas de anonimização e pseudonimização, que permitem o uso de dados sem comprometer a identidade dos titulares. Santos (2024) observa que “a pseudonimização permite que os dados sejam utilizados de forma mais segura em investigações complexas” (SANTOS, 2024, p. 17). Para a PMAM, tais técnicas podem ser aplicadas em relatórios internos e na cooperação com outros órgãos de segurança, reduzindo riscos de exposição indevida.

Por fim, cabe destacar que a globalização do crime exige cooperação e compartilhamento de dados entre instituições. Chuy (2021) ressalta que “o compartilhamento de informações constantes em bancos de dados [...] mostra-se indispensável não só para o enfrentamento direto do delito, mas para estrategicamente ser traçado um planejamento efetivo que resulte na efetiva prevenção ao crime” (CHUY, 2021, p. 8). No contexto amazônico, onde a PMAM enfrenta desafios como o tráfico transnacional e crimes ambientais, esse compartilhamento deve ocorrer de forma controlada e em conformidade com a LGPD.

Assim, o fluxo de dados sensíveis e a autodeterminação informativa, quando correlacionados às peculiaridades da PMAM, revelam a necessidade de um equilíbrio entre a proteção dos direitos fundamentais e a eficiência da segurança pública. A adoção de protocolos claros, técnicas de proteção de dados e cooperação interinstitucional são medidas indispensáveis

para que a corporação atue de forma constitucional e eficaz.

A conformidade e as salvaguardas no tratamento de dados pela Polícia Militar são essenciais para equilibrar a proteção da privacidade com a eficiência das operações. A LGPD determina que os dados sejam coletados apenas para finalidades legítimas e necessárias (SANTOS, 2024, p. 11), enquanto o anteprojeto da “LGPD Penal” busca garantir proteção contra abusos sem limitar o acesso a ferramentas modernas de investigação (CHUY, 2021, p. 3). No caso da PMAM, isso implica protocolos claros e medidas de segurança que respeitem a autodeterminação informativa e assegurem a legitimidade das ações policiais.

8. VIESES ALGORÍTMICOS E SELETIVIDADE TECNOLÓGICA - O FENÔMENO DO FEEDBACK LOOP E A ESTIGMATIZAÇÃO DE TERRITÓRIOS AMAZÔNIDAS

A expansão das tecnologias de reconhecimento facial e de sistemas algorítmicos no Brasil tem revelado impactos significativos sobre populações vulneráveis, especialmente em territórios periféricos e amazônidas. Conforme Lima (2022), “os programas erram grosseiramente quando se trata de imagens contendo pessoas negras, e esses erros não são devidos ao acaso, mas resultantes do preestabelecimento do racismo estrutural” (LIMA, 2022, p. 13). Esse dado evidencia como os algoritmos, ao serem alimentados por bases enviesadas, reforçam desigualdades históricas e produzem um ciclo de retroalimentação discriminatória (feedback loop).

O fenômeno do feedback loop ocorre quando sistemas tecnológicos, ao coletarem dados em territórios já estigmatizados, reforçam padrões de vigilância e criminalização. Como destaca a autora, “o racismo algorítmico [...] é entendido como um fenômeno sociotécnico decorrente do aspecto estrutural inserido na era tecnológica” (LIMA, 2022, p. 16). No contexto amazônico, marcado por desigualdades socioeconômicas e pela presença de comunidades tradicionais, esse processo pode intensificar a marginalização, vinculando tais territórios a índices de risco e insegurança de forma automática e acrítica.

A seletividade tecnológica, portanto, não é neutra. Ela reflete escolhas políticas e sociais que se materializam nos códigos e bases de dados. Lima (2022) observa que “as tecnologias contribuindo para os processos de racialização e injustiças incitam a luta para eliminar o racismo e outras formas de subordinação” (LIMA, 2022, p. 17). No caso da Amazônia, a utilização de sistemas de vigilância algorítmica pode reforçar estigmas sobre populações indígenas, ribeirinhas e negras, perpetuando a lógica de exclusão e invisibilidade.

Assim, o feedback loop tecnológico, ao invés de promover segurança, pode consolidar práticas discriminatórias e estigmatizar territórios amazônidas como espaços de risco permanente. A crítica ao racismo algorítmico, conforme a Teoria Racial Crítica aplicada por Lima (2022), exige que se reconheça a “necessidade de compromisso com a justiça social” (LIMA, 2022, p. 17), o que implica em repensar a aplicação dessas tecnologias e garantir salvaguardas jurídicas e éticas que respeitem a diversidade e os direitos fundamentais.

9. VIESES ALGORÍTMICOS E SELETIVIDADE TECNOLÓGICA: O *FEEDBACK LOOP* E A ESTIGMATIZAÇÃO DE TERRITÓRIOS AMAZÔNIDAS

A utilização de sistemas de reconhecimento facial em diversas cidades brasileiras tem demonstrado como os algoritmos podem reproduzir e intensificar desigualdades sociais. Em estudo citado por Lima (2022), observa-se que “os programas erram grosseiramente quando se trata de imagens contendo pessoas negras, e que esses erros não são devidos ao acaso, mas resultantes do preestabelecimento do racismo estrutural” (LIMA, 2022, p. 13). Esse dado revela que o viés algorítmico não apenas compromete a precisão tecnológica, mas também reforça estigmas históricos, criando um ciclo de retroalimentação discriminatória (*feedback loop*).

Exemplos práticos já foram identificados em capitais como Salvador e Rio de Janeiro, onde sistemas de reconhecimento facial foram utilizados em grandes eventos e operações policiais. A Rede de Observatórios da Segurança apontou que “a proporção de prisões efetuadas com uso de reconhecimento facial” (LIMA, 2022, p. 43) recaiu majoritariamente sobre pessoas negras, evidenciando a seletividade tecnológica e a reprodução de padrões discriminatórios.

No contexto amazônico, a aplicação dessas tecnologias pode gerar impactos ainda mais graves. A região é marcada por comunidades indígenas, ribeirinhas e negras, que historicamente enfrentam invisibilidade e marginalização. Assim, deve ser respeitado o princípio da autodeterminação dos povos indígenas.

O direito à livre determinação dos povos indígenas está expresso na Declaração Americana sobre direitos dos Povos Indígenas aprovada em 15 de junho de 2016 pela Organização dos Estados Americanos. Segundo este tratado internacional, foi reconhecido que: “Os povos indígenas têm direito à livre determinação. Em virtude desse direito, definem livremente sua condição política e buscam livremente seu desenvolvimento econômico, social e cultural” (RODRIGUES et al; AGUIAR, 2023)

A adoção de sistemas algorítmicos sem salvaguardas adequadas pode estigmatizar territórios amazônidas como espaços de risco permanente, vinculando-os a índices de

criminalidade de forma acrítica. Como destaca Lima (2022), “o racismo algorítmico [...] é entendido como um fenômeno sociotécnico decorrente do aspecto estrutural inserido na era tecnológica” (LIMA, 2022, p. 16), o que reforça a necessidade de compreender que tais ferramentas não são neutras, mas carregam escolhas políticas e sociais embutidas em seus códigos.

Esse processo de estigmatização territorial, alimentado pelo *feedback loop*, tende a consolidar práticas de vigilância intensiva em áreas periféricas e amazônicas, reforçando a lógica de exclusão. A autora enfatiza que “as tecnologias contribuindo para os processos de racialização e injustiças incitam a luta para eliminar o racismo e outras formas de subordinação” (LIMA, 2022, p. 17). Portanto, a crítica ao uso indiscriminado dessas ferramentas deve considerar não apenas os erros técnicos, mas também os efeitos sociais e políticos que perpetuam desigualdades.

Assim, a análise dos vieses algorítmicos e da seletividade tecnológica revela que o *feedback loop* não é apenas um problema técnico, mas um fenômeno que pode reforçar estigmas e marginalizar territórios amazônidas. A adoção de salvaguardas jurídicas, éticas e sociais é indispensável para que a tecnologia não se torne instrumento de perpetuação do racismo estrutural, mas sim ferramenta de inclusão e respeito aos direitos fundamentais.

10. VIESES ALGORÍTMICOS E SELETIVIDADE TECNOLÓGICA NO SISTEMA PAREDÃO

Esse processo de identificação leva processo temporal. A identificação civil da pessoa humana no Brasil percorre uma trajetória permeada por avanços e transformações. A princípio, a preocupação era com a identificação civil, algumas vezes usada para definir propriedades, posteriormente foi necessária para identificar criminalmente os indivíduos nocivos à sociedade (PORTELA; AGUIAR, 2026), nesse contexto, surgiu o sistema de identificação no amazonas.

O Sistema Paredão foi lançado em 2025 com a promessa de ampliar o monitoramento urbano e apoiar a prisão de foragidos. As câmeras de reconhecimento facial foram instaladas em pontos estratégicos da capital e em municípios do interior, integrando inclusive sistemas privados de segurança.

Entretanto, estudos como o de Lima (2022) demonstram que “os programas erram grosseiramente quando se trata de imagens contendo pessoas negras, e esses erros não são devidos ao acaso, mas resultantes do preestabelecimento do racismo estrutural” (LIMA, 2022,

p. 13). Essa constatação é crucial para compreender que, ao serem aplicados em contextos amazônicos, os algoritmos podem reforçar desigualdades históricas e criar um ciclo de retroalimentação discriminatória (*feedback loop*).

II. ANÁLISE DO DISCURSO: A "NEUTRALIDADE" TÉCNICA VS. O RACISMO ESTRUTURAL - PRESUNÇÃO DE INOCÊNCIA E A "GUETIZAÇÃO" DIGITAL

A ideia de neutralidade técnica, frequentemente invocada no campo jurídico e tecnológico, revela-se como uma estratégia discursiva que mascara desigualdades raciais e legitima práticas discriminatórias. Conforme Lôbo e Cardoso (2025), “a neutralidade jurídica atua como ferramenta de manutenção das desigualdades raciais, ao aplicar normas de forma descontextualizada da realidade social” (LÔBO; CARDOSO, 2025, p. 297). Essa constatação é fundamental para compreender como o discurso da neutralidade, tanto no direito quanto na tecnologia, contribui para a invisibilização do racismo estrutural.

No ambiente digital, a chamada “guetização” ocorre quando algoritmos e sistemas de vigilância reforçam estigmas sociais, associando determinados grupos e territórios a índices de risco e criminalidade. Lima (2022) observa que “os programas erram grosseiramente quando se trata de imagens contendo pessoas negras, e esses erros não são devidos ao acaso, mas resultantes do preestabelecimento do racismo estrutural” (LIMA, 2022, p. 13). Esse viés tecnológico, ao ser naturalizado como neutro, compromete a presunção de inocência e intensifica a seletividade penal, sobretudo em comunidades periféricas e amazônicas.

A presunção de inocência, princípio constitucional consagrado no artigo 5º, inciso LVII, da Constituição Federal, é tensionada pela lógica algorítmica que transforma suspeitas em verdades estatísticas. Como destacam Lôbo e Cardoso (2025), o direito “longe de ser neutro, participa ativamente da manutenção das hierarquias raciais” (LÔBO; CARDOSO, 2025, p. 297). Assim, quando sistemas digitais classificam indivíduos com base em padrões enviesados, ocorre uma inversão da lógica garantista: a inocência deixa de ser presumida e passa a ser condicionada ao crivo de tecnologias que reproduzem desigualdades.

Nesse sentido, a “guetização digital” pode ser entendida como a extensão contemporânea da seletividade penal, que historicamente criminaliza corpos negros e marginalizados. Lima (2022) enfatiza que “o racismo algorítmico [...] é entendido como um fenômeno sociotécnico decorrente do aspecto estrutural inserido na era tecnológica” (LIMA, 2022, p. 16). A associação automática de determinados grupos a riscos potenciais não apenas

reforça estigmas, mas também legitima práticas de vigilância intensiva, criando verdadeiros “guetos digitais” que limitam o exercício pleno da cidadania.

Portanto, a análise do discurso sobre neutralidade técnica evidencia que tanto o direito quanto a tecnologia não são instrumentos neutros, mas sim campos permeados por relações de poder e hierarquias raciais. A crítica à neutralidade, articulada pela Teoria Crítica da Raça, revela que a presunção de inocência e a proteção dos direitos fundamentais só podem ser efetivas se houver o reconhecimento da seletividade estrutural e a implementação de salvaguardas que impeçam a reprodução da “guetização” digital.

12. MECANISMOS DE CONTROLE E DIRETRIZES PARA O MINISTÉRIO PÚBLICO

12.1. O CONTROLE EXTERNO DA ATIVIDADE POLICIAL À LUZ DA RESOLUÇÃO Nº 279/2023 DO CNMP

O controle externo da atividade policial é atribuição constitucional do Ministério Público, previsto no art. 129, VII, da Constituição Federal, e regulamentado pela Lei Complementar nº 75/1993. Trata-se de função essencial para assegurar a legalidade e a eficiência da atuação policial, evitando abusos e garantindo a proteção dos direitos fundamentais. Como destacam Kurkowski e Silva (2023), “os organismos policiais estão sujeitos à fiscalização do MP, consequência dos mecanismos de equilíbrio existentes em qualquer Estado de Direito” (KURKOWSKI; SILVA, 2023, p. 462).

A Resolução nº 279/2023 do Conselho Nacional do Ministério Público (CNMP) atualizou e consolidou diretrizes para o exercício desse controle, reforçando a necessidade de institucionalizar práticas de fiscalização que sejam compatíveis com a cooperação em inteligência. Nesse sentido, o controle externo não deve ser compreendido como mera ingerência, mas como instrumento de aperfeiçoamento da segurança pública. Conforme os autores, “a dimensão desse controle externo da atividade policial pelo MP pode ser fonte de antagonismo institucional [...]” (KURKOWSKI; SILVA, 2023, p. 463), o que evidencia a importância da Resolução nº 279/2023 em estabelecer parâmetros claros para reduzir tensões e fortalecer a confiança entre instituições.

A Resolução também reafirma que o Ministério Público, ao exercer o controle externo, deve observar os princípios constitucionais da legalidade, moralidade, publicidade e eficiência (art. 37 da CF). Isso implica que a fiscalização não se limita ao aspecto disciplinar, mas abrange a análise da conformidade das práticas policiais com os direitos fundamentais. Como ressaltam

Kurkowski e Silva (2023), “a atuação do Ministério Público no controle externo da atividade policial pode estar relacionada ao policiamento de segurança pública em geral ou à atividade de investigação criminal” (KURKOWSKI; SILVA, 2023, p. 460).

Portanto, à luz da Resolução nº 279/2023, o controle externo da atividade policial deve ser compreendido como mecanismo de equilíbrio institucional, que busca compatibilizar fiscalização e cooperação. A institucionalização da confiança entre Ministério Público e forças policiais, por meio de protocolos claros e interoperabilidade técnica, é condição indispensável para que o controle externo cumpra sua função constitucional sem comprometer a eficiência da segurança pública.

12.2. COMPLIANCE ALGORÍTMICO, AUDITABILIDADE E O DIREITO À EXPLICAÇÃO

O avanço da inteligência artificial e dos algoritmos no âmbito empresarial trouxe novos desafios para o compliance corporativo, especialmente no que se refere à proteção de dados e à transparência das decisões automatizadas. Pinheiro e Brega (2021) destacam que “o uso de algoritmos gera riscos cujo devido enfrentamento não é resolvido apenas pelo seguimento dos comandos dispostos na legislação de proteção de dados” (PINHEIRO; BREGA, 2021, p. 161). Isso demonstra que a simples adequação à Lei Geral de Proteção de Dados (LGPD) não é suficiente para mitigar os riscos relacionados à opacidade algorítmica.

Nesse cenário, a auditabilidade dos sistemas torna-se essencial. Introna (2016) alerta que os algoritmos apresentam “inescrutabilidade” e “executabilidade”, ou seja, operam de forma automática e muitas vezes não podem ser inspecionados (INTRONA, 2016, p. 17). Essa característica reforça a necessidade de mecanismos de auditoria independentes, capazes de verificar os inputs e outputs dos sistemas, garantindo que não se transformem em verdadeiras “caixas-pretas” (PINHEIRO; BREGA, 2021, p. 171).

O direito à explicação, por sua vez, emerge como garantia fundamental diante da crescente automatização das decisões. A *Information Commissioner’s Office* (ICO), autoridade de dados do Reino Unido, já havia advertido que a incorporação da inteligência artificial “leva a uma opacidade do processo decisório dos algoritmos, uma vez que o motivo pelo qual tomaram determinada decisão não é compreensível para os seres humanos” (INFORMATION COMMISSIONER’S OFFICE, 2016 apud PINHEIRO; BREGA, 2021, p. 171). Assim, assegurar ao titular dos dados o direito de compreender como e por que determinada decisão foi tomada é condição indispensável para a proteção da dignidade e da autonomia informacional.

Portanto, compliance algorítmico, auditabilidade e direito à explicação formam um tripé indispensável para a governança ética das tecnologias digitais. O compliance deve ir além da mera adequação normativa, incorporando práticas de auditoria contínua e garantindo explicações acessíveis aos cidadãos. Somente dessa forma será possível evitar que os algoritmos perpetuem desigualdades e consolidem um modelo de exclusão digital.

12.3. PROPOSTAS PARA UMA INOVAÇÃO TECNOLÓGICA DEMOCRÁTICA E NÃO-DISCRIMINATÓRIA NA POLÍCIA MILITAR DO ESTADO DO AMAZONAS

A implementação de tecnologias de predição criminal na Polícia Militar do Estado do Amazonas deve ser acompanhada por um arcabouço normativo e ético que assegure a prevalência dos direitos fundamentais sobre a técnica.

Além disso, a autonomia individual, reconhecida pela Constituição como núcleo essencial da liberdade, revela tensões quando confrontada com o poder punitivo do Estado. A criminalização da conduta do companheiro poderia significar restrições indevidas ao direito de autodeterminação reprodutiva, levantando questionamentos sobre proporcionalidade e razoabilidade. (SILVA et al, AGUIAR. 2025)

Uma inovação verdadeiramente democrática exige o abandono de modelos de "caixa-preta", uma vez que "a transparência algorítmica é condição essencial para a legitimidade do ato administrativo". Nesse sentido, propõe-se a adoção do princípio da explicabilidade, garantindo que toda decisão automatizada de patrulhamento ou triagem possa ser compreendida e revisada por supervisão humana, respeitando o "direito à explicação" previsto na lógica da proteção de dados pessoais.

Para mitigar a seletividade penal automatizada, é imperativo que a PMAM adote mecanismos de auditoria constante das bases de dados. A ciência demonstra que "o policiamento preditivo tende a reproduzir padrões históricos de discriminação se não houver um controle rigoroso sobre os dados de entrada". Assim, uma proposta concreta é a realização de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) específicos para algoritmos de segurança pública, permitindo identificar e corrigir vieses de raça ou classe social antes da operacionalização da tropa.

Ademais, o papel do Ministério Público do Amazonas (MPAM) é central como guardião do regime democrático. Propõe-se que o controle externo da atividade policial inclua a fiscalização técnica da governança de dados da PMAM, pautada pela futura "LGPD Penal". Esta fiscalização deve assegurar que a "eficiência administrativa não seja convertida em vigilância desproporcional ou em uma 'guetização' digital de territórios vulneráveis". Somente

através de uma inovação que preveja a *accountability* (prestação de contas) e a participação da sociedade civil será possível transformar a predição criminal em um instrumento de justiça, e não em um mecanismo de exclusão no território amazônica.

CONSIDERAÇÕES FINAIS

A transição para um policiamento baseado em evidências e algoritmos na Polícia Militar do Estado do Amazonas representa um avanço na busca pela eficácia administrativa, mas impõe um rigoroso dever de vigilância sobre a conformidade constitucional. A natureza jurídica da inteligência artificial aplicada à segurança pública foi identificada não apenas como um suporte técnico, mas como um ato administrativo automatizado que, embora pautado no princípio da eficiência, permanece vinculado aos princípios da legalidade e da impessoalidade.

A análise conduzida valida a hipótese de que a utilização de algoritmos de "caixa-preta", alimentados por bases de dados que espelham preconceitos históricos, resulta em uma violação sistêmica aos direitos fundamentais e ao princípio da não-discriminação. O risco de um *feedback loop* — onde o reforço de patrulhamento em áreas já estigmatizadas gera novas prisões que retroalimentam o sistema — confirma que a "neutralidade" tecnológica pode mascarar e

Entretanto, a pesquisa demonstra que essa tensão é resolvível mediante a implementação de um *compliance* algorítmico. Isso significa que a eficácia operacional da Polícia Militar do Estado do Amazonas depende da garantia de auditabilidade do código-fonte e do respeito ao direito à explicação humana, assegurando que nenhuma decisão sobre a liberdade ou a privacidade do cidadão amazonense seja tomada de forma puramente opaca por uma máquina.

Para o futuro, a aplicação dos resultados deste trabalho sugere que o Ministério Público, no exercício do controle externo da atividade policial, deve transpor sua fiscalização do campo estritamente físico para o campo digital, auditando os critérios de treinamento das Inteligências Artificiais utilizadas pela força policial. Recomenda-se a criação de protocolos de transparência ativa e a capacitação contínua de oficiais e promotores na governança de dados sensíveis, conforme preconizado pela LGPD.

Em última análise, o que esta pesquisa revela é que a inovação tecnológica na Amazônia só alcançará sua missão de preservar a ordem pública se for utilizada para democratizar a segurança, e não como uma ferramenta de exclusão social. A tecnologia deve servir ao Estado

Democrático de Direito, garantindo que a eficiência da Polícia Militar do Estado do Amazonas caminhe lado a lado com a proteção da dignidade humana

REFERÊNCIAS

BOFF, Salete Oro; FORTES, Vinícius Borges. A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil. **Revista Sequência**, Florianópolis, n. 68. Disponível em: <chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/https://www.scielo.br/j/seq/a/LqY93YW8FMSNPgkVBg75nbH/?format=pdf&lang=pt.acesso em 22/01/2026>

BRASIL. Conselho Nacional do Ministério Público. **Resolução nº 279, de 12 de dezembro de 2023**. Dispõe sobre o exercício do controle externo da atividade policial pelo Ministério Público. Disponível em: <https://www.cnmp.mp.br/portal/atos-e-normas/norma/10379/> Acesso em 29/01/2026

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm Acesso em 29/01/2026

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe acerca Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em 29/01/2026

CARVALHO FILHO, José dos Santos. Manual de Direito Administrativo. 30. ed. ver. atual e ampl. – São Paulo: Atlas, 2016.

CAVALCANTE, Carlos Daniel Oliveira et al. **Policciamento preditivo e discriminação de raça e classe social: uma análise das experiências dos Estados Unidos e do Brasil**. 2024. Disponível em: <https://www.repositorio.ufal.br/handle/123456789/14551> Acesso em 22/01/2026.

CHUY, José Fernando Moraes. **O sistema de investigação brasileiro, a “LGPD Penal” e a efetiva garantia de direitos fundamentais**. 2021. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx> Acesso em 29/01/2026

DI PIETRO, Maria Sylvia Zanella. – 30.ed. Rev., atual. e ampl. – Rio de Janeiro: Forense, 2017.

INFORMATION COMMISSIONER'S OFFICE. **Big data, artificial intelligence, machine learning and data protection**. Londres: ICO, 2016.

INTRONA, L. D. Algorithms, Governance and Governmentality: on governing academic writing. **Science, Technology, & Human Values**, v. 41, n. 1, p. 17-49, 2016.

JUNIOR, Ilson de Oliveira; SANTOS, Franck Cione Coelho dos. Inteligência artificial e

policciamento preditivo: possibilidades de inovação tecnológica para a Polícia Militar do Paraná no enfrentamento aos crimes violentos contra o patrimônio com emprego de explosivos. **Brazilian Journal of Technology**, Curitiba – PR, 2021. Disponível em <https://ojs.brazilianjournals.com.br/ojs/index.php/BJT/article/view/45351> Acesso em 23/01/2026

KURKOWSKI, Rafael Schwez; SILVA, Rodney da. A compatibilização do controle externo da atividade policial com a confiança necessária à cooperação em inteligência. **Revista Brasileira de Ciências Policiais**, Brasília, v. 14, n. 11, p. 455-481, jan./abr. 2023. Disponível em: https://scholar.google.com/scholar?hl=ptBR&as_sdt=0%2C5&q=O+CONTROLE+EXTERRNO+DA+ATIVIDADE+POLICIAL+%C3%80+LUZ+DA+RESOLU%C3%87%C3%83O+N%C2%BA+279%2F2023+DO+CNMP+&btnG= Acesso em 29/01/2026

LIMA, Bruna Dias Fernandes. **Racismo Algorítmico**: o enviesamento tecnológico e o impacto aos direitos fundamentais no Brasil. Dissertação (Mestrado em Direito) – Universidade Federal de Sergipe, São Cristóvão, 2022. Disponível em: <https://ri.ufs.br/handle/riufs/15173> Acesso em 29/01/2026

LÔBO, Vinícius Henrique Cavalcante; CARDOSO, Fernando da Silva. **A aplicação do conceito de racismo reverso no Habeas Corpus 929002/AL**: análise desde a interpretação do STJ e as respostas jurídicas ao racismo estrutural. *Revista Direitos Sociais e Políticas Públicas*, v. 13, n. 3, 2025. Disponível em: <https://portal.unifafibe.com.br/revista/index.php/direitos-sociais-politicas-pub/article/view/1791> Acesso em 29/01/2026

LOUREIRO, A. J. C., AGUIAR, D. M. de, & ZOGAHIB, A. L. N. (2025). Desafios e perspectivas jurídicas da constitucionalidade do policiamento com drones. *Revista Ibero-Americana De Humanidades, Ciências E Educação*, 11(12), 6176–6190. Disponível em: <https://doi.org/10.51891/rease.viii12.23367> Acesso em 03/02/2026

NUNES, Pablo. **Novas ferramentas, velhas práticas**: reconhecimento facial e policiamento no Brasil. (2019). Disponível em: https://scholar.google.com/citations?view_op=view_citation&hl=pt-BR&user=yzcYezIAAAAJ&citation_for_view=yzcYezIAAAAJ:ZeXyd9-uunAC Acesso em: 22/01/2026

OLIVEIRA, Jade Fontes Sobral de. **O profiling como método suplementar de abordagem investigativa e seus campos de atuação**; São Cristovão – SE, 2021. Disponível em: chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/https://ri.ufs.br/bitstream/riufs/14530/2/Jade_Fontes_Sobral_Oliveira.pdf Acesso em: 23/01/2026

OLIVEIRA, Marcos Vinícius. **O sistema de investigação brasileiro, a “LGPD Penal” e a efetiva garantia de direitos fundamentais**. Disponível: https://scholar.google.com/scholar?hl=pt-BR&as_sdt=0%2C5&q=O+sistema+de+investiga%C3%A7%C3%A3o+brasileiro%2C+a+%E2%80%9D+CLGPD+Penal%E2%80%9D+e+a+efetiva+garantia+de+direitos+fundamentais.+&btnG= Acesso em 29/01/2026

PINHEIRO, Caroline Rosa; BREGA, Gabriel Ribeiro. Inteligência artificial e compliance – a (in)suficiência dos marcos de proteção de dados. **Revista Semestral de Direito Empresarial**, Rio de Janeiro, n. 28, p. 161-171, jan./jun. 2021. Disponível em:

https://scholar.google.com/scholar?hl=ptBR&as_sdt=0%2C5&q=PINH+artificial+e+compliance+%E2%80%93+a+%28in%29sufici%C3%A4ncia+dos+marcos+de+prote%C3%A7%C3%A3o+de+dados.+Revista+Semestral+de+Direito+Empresarial%2C+Rio+de+Janeiro&btnG= Acesso em 29/01/2026

PORTELA, R. L., & AGUIAR, D. M. de. (2026). Histórico da identificação civil e as contribuições para a análise criminal no sistema de segurança pública do Amazonas. *Revista Ibero-Americana De Humanidades, Ciências E Educação*, 12(1), 1–20. Disponível em: <https://doi.org/10.51891/rease.v12i1.23685> Acesso 04/02/2026

RODRIGUE, Gabriela de Sousa. **Segurança pública datificada e policiamento preditivo: Uma breve análise acerca do uso do Big Data pela polícia, seus métodos e vulnerabilidades.** Rio de Janeiro, 2022. Disponível em: <https://pantheon.ufrj.br/handle/11422/18942> Acesso em 23/01/2026

RODRIGUES, A. L. da S., AGUIAR, D. M. de, & LACERDA, D. L. de. (2023). Princípio da autodeterminação para demarcação de territórios indígenas em Manaus. Nova Hileia | Revista Eletrônica De Direito Ambiental Da Amazônia - ISSN 2525-4537, 15(4). Disponível em: <http://periodicos.uea.edu.br/index.php/novahileia/article/view/2926/1598> Acesso em 04/02/2026

SANTOS, Paula Hillaury Barbosa dos. **O impacto da Lei Geral de Proteção de Dados nos inquéritos policiais: desafios e possíveis soluções para a condução de investigações respeitando a privacidade.** Goiânia: PUC Goiás, 2024. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/8214> Acesso em 29/01/2026

25

SILVA, Paulo Eduardo da. **O impacto da Lei Geral de Proteção de Dados nos inquéritos policiais.** Disponível em: https://scholar.google.com/scholar?hl=ptBR&as_sdt=0%2C5&q=SILVA%2C+Paulo+Eduardo+da.+O+impacto+da+Lei+Geral+de+Prote%C3%A7%C3%A3o+de+Dados+nos+inqu%C3%A9ritos+policiais.+&btnG= Acesso em 29/01/2026

SILVA NETO, F. M. M. da, MIYADAIRA, F. Y., & MELO DE AGUIAR, D. (2025). Análise da juridicidade do policiamento em terras indígenas: competência constitucional da polícia militar do Amazonas frente ao pacto federativo. *Revista Ibero-Americana De Humanidades, Ciências E Educação*, 11(12), 7131–7149. Disponível em: <https://doi.org/10.51891/rease.v11i12.2352> Acesso em 03/02/2026

SILVA, C. M. da, SILVA, M. E. M. da, & AGUIAR, D. M. de. (2025). A corresponsabilidade penal do companheiro nos casos de aborto consentido: dilemas jurídicos e perspectivas no direito brasileiro. *Revista Ibero-Americana De Humanidades, Ciências E Educação*, 11(10), 31–46. Disponível em: <https://doi.org/10.51891/rease.v11i10.21319> Acesso em 04/02/2026

SOUZA, Bruno da Silva; MORAIS, Leonardo de. **Lei Geral de Proteção de Dados e sua aplicação no combate aos crimes cibernéticos.** Disponível em: https://scholar.google.com/scholar?hl=ptBR&as_sdt=0%2C5&q=SOUZA%2C+Bruno+da+Silva%3B+MORAIS%2C+Leonardo+de.+Lei+Geral+de+Prote%C3%A7%C3%A3o+de+Dados+e+sua+aplica%C3%A7%C3%A3o+no+combate+aos+crimes+cibern%C3%A9ticos&btnG= Acesso em 29/01/2026