www.revistaft.com.br

Revista FT | ISSN 1678-0817 | v. 30, n. 159, 2026 | DOI: 10.69849/r0av2z03

Inteligência artificial na Polícia Militar do Pará: desafios éticos, legais e de transparência algorítmica

Artificial intelligence in the Military Police of Pará: ethical, legal, and algorithmic transparency challenges

Rogério Fernandes Oliveira[1]
Eder Bruno Bezerra Barros[2]
Kerlyson Carlos Viana Araujo[3]
Keile da Silva Nascimento[4]

RESUMO

À medida que as forças de segurança incorporam sistemas de IA em suas rotinas, torna-se necessário reavaliar a organização administrativa e a execução de tarefas operacionais. Na Polícia Militar do Pará (PMPA), a adoção dessas tecnologias esbarra em lacunas regulatórias e riscos inerentes à opacidade algorítmica. O problema de pesquisa é: como a PMPA pode implementar soluções de IA em suas atividades-meio e fim, garantindo a transparência algorítmica e a supervisão humana efetiva, em conformidade com o marco legal emergente e mitigando vieses discriminatórios? O objetivo geral é analisar como a PMPA pode implementar essas soluções, propondo diretrizes de governança alinhadas ao marco regulatório nacional e às necessidades institucionais. Metodologicamente, esta pesquisa adota uma abordagem qualitativa, de natureza aplicada, assumindo caráter exploratório e descritivo a partir de fontes bibliográficas e documentais, cujos dados foram submetidos a análise crítica de conteúdo. Os resultados apontam que o uso de IA na segurança pública é de alto risco, revelam vieses discriminatórios em sistemas preditivos e evidenciam a ausência de protocolos de auditabilidade na Corporação, propondo-se a adoção de Avaliações de Impacto Algorítmico como parâmetros obrigatórios. O estudo argumenta que a operacionalização do PL nº 2.338/2023 e da Portaria MJSP nº 961/2025 exige governança adaptada à realidade local, justificando a representação da PMPA no Grupo de Trabalho da Estratégia Paraense de

[1] 3º SGT PMPA. Especialista em Internet das Coisas - IOT. Bacharel em Engenharia de Computação pelo Centro Universitário Internacional (UNINTER). Castanhal, Pará, Brasil. E-mail: grupocastanhal@hotmail.com. ORCID: 0009-0001-9455-7269.
[2] 3º SGT PMPA. Especialista em Treinamento Desportivo. Graduado em Educação Física pela Universidade Norte do Paraná (UNOPAR). Castanhal, Pará, Brasil. E-mail: edersd17@gmail.com.
[3] 3º SGT PMPA. Especialista em Educação a Distância: Gestão e Tutoria. Graduado em Geografia pelo Centro Universitário Leonardo da Vinci (UNIASSELVI). Belém, Pará, Brasil. E-mail: kerlysoncarlos@gmail.com.
[4] 3º SGT PMPA. Especialista em Gestão Pública, Bacharel em Serviço Social pela Universitário Norte do Paraná (UNOPAR). Castanhal, Pará, Brasil. E-mail: keiletrindade@yahoo.com.

IA (EPIA). A pesquisa conclui que a inovação tecnológica na PMPA só se legitima sob controle hierárquico rigoroso e transparência algorítmica, resguardando os direitos fundamentais da população paraense.

Palavras-chave: Opacidade decisória; Viés discriminatório; Governança tecnológica; Auditabilidade; Regulamentação.

ABSTRACT

The integration of artificial intelligence into military police routines demands a concurrent reassessment of the administrative frameworks and operational procedures. In the Military Police of Pará (PMPA), the adoption of these technologies faces regulatory gaps and risks inherent in algorithmic opacity. The research problem is: how can the PMPA implement AI solutions in its core and support activities, ensuring algorithmic transparency and effective human oversight, in accordance with the emerging legal framework and mitigating discriminatory biases? The overall objective is to analyze how the PMPA can implement these solutions, proposing governance guidelines aligned with the national regulatory framework and institutional needs. Methodologically, this research adopts a qualitative approach, of an applied nature, assuming an exploratory and descriptive character based on bibliographic and documentary sources, whose data were subjected to critical content analysis. The results indicate that the use of AI in public security is high-risk, reveals discriminatory biases in predictive systems, and highlights the absence of auditability protocols within the Corporation, proposing the adoption of Algorithmic Impact Assessments as mandatory parameters. The study argues that the implementation of Bill No. 2,338/2023 and Ministry of Justice and Public Security Ordinance No. 961/2025 requires governance adapted to the local reality, justifying the PMPA's representation in the Working Group of the Pará AI Strategy (EPIA). The research concludes that technological innovation in the PMPA is only legitimate under rigorous hierarchical control and algorithmic transparency, safeguarding the fundamental rights of the population of Pará.

Keywords: Decision opacity; Discriminatory bias; Technological governance; Auditability; Regulation.

1 INTRODUÇÃO

Nos últimos anos, a PMPA vem passando por uma modernização operacional com a

adoção de equipamentos de captação e plataformas de integração, como câmeras corporais (*bodycams*) (Virgolino, 2024), Aeronave Remotamente Pilotada (RPA), totens de segurança (Amorim, 2025) e a integração estratégica ao Sistema Nacional de Informações de Segurança Pública (Sinesp) (Brasil, 2025a). Contudo, tais ferramentas ainda se limitam ao monitoramento passivo, mantendo a atuação da tropa atrelada a uma vigilância majoritariamente reativa (Nagata, 2024).

Ao romper esse limite, a Inteligência Artificial (IA) ultrapassa o uso restrito aos sistemas de consulta e monitoramento, passando a condicionar diretamente as decisões no policiamento ostensivo. Sob a aparência de eficiência, todavia, a tecnologia traz o risco imediato de perpetuar vieses discriminatórios, conceituados como distorções sistemáticas nos resultados algorítmicos que reproduzem preconceitos históricos e impactam desproporcionalmente grupos vulneráveis, ao replicar desigualdades históricas presentes nos dados de treinamento (Dal Pizzol, 2025; Costa; Oliveira, 2025).

Somado a isso, o uso dessas ferramentas pode gerar opacidade algorítmica, fenômeno caracterizado pela impossibilidade de rastrear a rota lógica das inferências da máquina, dificultando a responsabilização por decisões automatizadas (Lima; D'ornellas; Pessoa, 2025). Conforme sustenta Dal Pizzol (2025), a IA não é um recurso técnico neutro; ela atua como mediador entre o Estado e o indivíduo, podendo amplificar desigualdades históricas se não submetida a crivos éticos rigorosos. A máquina não assume a responsabilidade pela decisão policial, apenas a transfere para uma estrutura lógica inacessível que o próprio operador humano é incapaz de questionar ou auditar.

Ao exercer sua missão constitucional de policiamento ostensivo, definido pelo Manual de Policiamento Ostensivo Geral (POG), Volume I, da PMPA (Pará, 2024), como o policiamento que atende às necessidades basilares de segurança de uma localidade por meio da presença real e potencial do policial militar, sendo responsável pelo primeiro atendimento à população, e preservação da ordem pública, a Corporação defronta-se com a necessidade imediata de modernizar suas práticas sem ferir os direitos fundamentais.

Atualmente, a implementação de sistemas de reconhecimento facial em centros urbanos da Região Metropolitana de Belém (RMB) e em municípios do interior do Estado compõe o escopo das inovações da PMPA. Essa estrutura tecnológica se materializa por meio dos totens de segurança do projeto 'Cidades Inteligentes', iniciativa do Governo do Estado do Pará liderada pela Secretaria de Segurança Pública e Defesa Social (SEGUP). Equipados com inteligência artificial embarcada para reconhecimento facial e de placas veiculares, esses

dispositivos não possuem gestão direta da Corporação; integram-se ao Centro Integrado de Operações (CIOp) da Segup, gerando alertas em tempo real que subsidiam o deslocamento tático das guarnições da PMPA para a localização de foragidos e veículos roubados (Pará, 2025b).

Todavia, a realidade operacional da tropa impõe cautelas que o entusiasmo tecnológico frequentemente ignora. Como alerta Nagata (2024), os sistemas de IA na segurança pública enfrentam desafios críticos de confiabilidade e interpretabilidade, pois a lógica da máquina nem sempre é clara para quem a opera. Na prática diária, seja no despacho do Núcleo Integrado de Operações (NIOp), presente nas grandes metrópoles, ou na atuação de unidades operacionais, como os Batalhões de Polícia Militar (BPM), as Companhias Independentes de Polícia Militar (CIPM), a Companhia Independente De Missões Especiais (CIME), ou o Batalhão De Rondas Ostensivas Táticas Motorizadas (ROTAM), um algoritmo que direciona viaturas ou aponta um suspeito via câmeras pode estar replicando vieses sistêmicos camuflados sob um manto de objetividade matemática.

Apesar desse arcabouço em formação, identifica-se uma dissonância palpável entre a velocidade da adoção tecnológica nas unidades operacionais da PMPA (Amorim, 2025) e a carência de internalização de protocolos de governança algorítmica, correspondente ao conjunto de diretrizes que asseguram o controle e a auditoria da automação, (Dal Pizzol, 2025) no plano estratégico institucional. O Comitê Gestor da Internet no Brasil (CGI.br) já alertava, em sua Nota Pública de 2023, que as tecnologias de IA não são neutras, sendo imperativa a manutenção de classificações de riscos, que categorizam os sistemas conforme potencial ofensivo, e mecanismos de explicabilidade, que permitem a compreensão da lógica decisória da máquina por agentes humanos, para mitigar propósitos discriminatórios (CGI.br, 2023).

Superar esse descompasso exige enfrentar dois desafios estruturantes no cotidiano operacional da tropa: assegurar a transparência algorítmica, compreendida como a abertura e a clareza dos processos decisórios da máquina que permitem auditoria e compreensão humana, e mitigar o risco crônico de vieses discriminatórios, caracterizados como distorções sistemáticas que replicam preconceitos históricos e impactam desproporcionalmente grupos vulneráveis, no seio da Corporação. Tais desafios demandam uma resposta institucional imediata, sob pena de a modernização tecnológica gerar mais insegurança jurídica do que eficiência no policiamento ostensivo.

Diante dessa encruzilhada institucional e legal, e considerando a urgência de balizar a aquisição de novos equipamentos pelo Departamento Geral de Administração (DGA) e pelo Departamento-Geral de Operações (DGO), o problema de pesquisa que norteia este estudo é:

como a PMPA pode implementar soluções de IA em suas atividades-meio e fim, garantindo a transparência algorítmica e a supervisão humana efetiva, em conformidade com o marco legal emergente e mitigando vieses discriminatórios?

O objetivo geral desta pesquisa é analisar como a PMPA pode implementar soluções de IA em suas atividades-meio e fim, garantindo a transparência algorítmica e a supervisão humana efetiva, em conformidade com o marco legal emergente e mitigando vieses discriminatórios, propondo diretrizes de governança alinhadas ao marco regulatório nacional e às necessidades institucionais. Para guiar essa investigação, estabelecem-se as seguintes questões norteadoras: (I) Quais dispositivos do marco legal e regulatório incidem sobre o uso de IA pela PMPA? (II) Quais os riscos éticos e operacionais decorrentes da opacidade algorítmica e da automatização de decisões no contexto das atividades-meio e fim? (III) Quais parâmetros de auditabilidade e transparência podem ser propostos para a aquisição e emprego de sistemas de IA pela PMPA?

Operacionalmente, essas questões correspondem aos seguintes objetivos específicos: (I) mapear quais dispositivos do marco legal e regulatório incidem sobre o uso de IA pela PMPA; (II) identificar os riscos éticos e operacionais decorrentes da opacidade algorítmica e da automatização de decisões no contexto das atividades-meio e fim; e (III) propor parâmetros de auditabilidade e transparência para a aquisição e emprego de sistemas de IA pela PMPA.

A justificativa deste trabalho repousa em três dimensões complementares. Do ponto de vista da relevância social, a implementação não regulada de IA na segurança pública representa um risco direto aos direitos fundamentais do cidadão paraense. Algoritmos enviesados podem direcionar abordagens policiais de forma discriminatória, replicando desigualdades históricas sob uma aparência de objetividade matemática, o que compromete a igualdade e a dignidade da pessoa humana.

No plano da relevância institucional, a ausência de diretrizes claras expõe o policial militar e a Corporação a graves riscos jurídicos. Quando um sistema de IA direciona uma abordagem sem fundamentação transparente, o agente de segurança fica exposto a uma responsabilidade que não pode gerir, podendo resultar na nulidade de provas, na responsabilização civil do Estado e no comprometimento da imagem da Corporação. Sob essa ótica, a participação da PMPA na formulação da EPIA transcende o formalismo administrativo, revelando-se imperativa para a segurança jurídica das operações, garantindo que modelos treinados com dados de outras realidades não sejam impostos à tropa sem adaptação.

Por fim, quanto à relevância acadêmica, o estudo preenche uma lacuna literária ao propor uma ponte entre o marco regulatório nacional emergente e as especificidades operacionais de uma Polícia Militar na região amazônica. A pesquisa contribui com a produção de conhecimento aplicado, oferecendo parâmetros concretos de governança algorítmica que podem servir de referencial para outras corporações estaduais que enfrentam dilemas semelhantes de modernização tecnológica e controle jurídico.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 O marco regulatório e a classificação de riscos na segurança pública

A regulação da IA no Brasil transita da reflexão acadêmica para a imperatividade jurídica, estabelecendo parâmetros inegociáveis para as forças de segurança. O PL nº 2.338/2023 representa o ponto de inflexão desse processo, adotando uma arquitetura regulatória policêntrica baseada na classificação de riscos. Essa lógica se concretiza ao categorizar as tecnologias conforme seu potencial ofensivo. No seu Art. 17, o projeto elenca como sistemas de alto risco aqueles utilizados para investigação criminal e segurança pública, especificamente os destinados a avaliações individuais de riscos, identificação biométrica e estudo analítico de crimes (Brasil, 2023).

Conforme destacam Santos et al. (2025), a autonomia decisória conferida a essas tecnologias, enquadradas na categoria de alto risco, exige um regramento rigoroso, sob pena de a eficiência operacional ceder lugar à insegurança jurídica. Essa categorização não é meramente retórica; ela impõe aos fornecedores e operadores um regime jurídico rigoroso de governança, que inclui documentação técnica detalhada, registro automático de operações e, sobretudo, a obrigatoriedade de Avaliação de Impacto Algorítmico (AIA), instrumento de avaliação prévia dos riscos sociojurídicos da automação, antes da colocação do sistema em funcionamento.

Nessa mesma esteira regulatória, a Portaria do Ministério da Justiça e Segurança Pública (MJSP) nº 961/2025 atua como norma setorial de imposição imediata aos órgãos de segurança. O ato normativo é claro ao condicionar o uso de soluções de IA à proporcionalidade e ao dever de prevenção de riscos. O seu Art. 11 estabelece uma vedação contundente ao uso de identificação biométrica à distância em tempo real em espaços públicos, ressalvadas apenas hipóteses estritas, como autorização judicial prévia para instrução de inquéritos, busca de vítimas ou pessoas desaparecidas, flagrantes de crimes graves, recaptura de evadidos e cumprimento de mandados de prisão (Brasil, 2025a).

A normatização consagra, no parágrafo único do Art. 10, o princípio da supervisão humana efetiva, equivalente ao *meaningful human control* da doutrina internacional (Santos et al., 2025): sempre que houver risco de lesão a direitos fundamentais, o agente de segurança revisará o resultado da inferência algorítmica (Brasil, 2025). Na doutrina militar, esse dever de revisão não cria uma nova obrigação, mas reafirma a manutenção do princípio da responsabilidade hierárquica. A máquina não pode ser o sujeito da ação policial; sua inferência deve ser tratada como elemento informativo submetido ao crivo do comandante de operação.

No plano estratégico, o Plano Brasileiro de Inteligência Artificial (PBIA 2024-2028) direciona a política nacional para a "IA para o bem de todos", enfatizando a soberania tecnológica, a nuvem soberana e o desenvolvimento de modelos em português baseados em dados nacionais (Brasil, 2024). Nesse escopo, destacam-se os Grandes Modelos de Linguagem (LLMs, do inglês Large Language Models), sistemas treinados para compreender e gerar texto complexo. Contudo, por trás dessa visão de soberania tecnológica, a adoção irrestrita desses sistemas de IA carrega riscos que ecoam o contexto militar. Ao analisarem as operações de defesa, Santos et al. (2025) apontam que a autonomia algorítmica pode gerar insegurança jurídica e riscos de desumanização. Na segurança pública brasileira, o cenário não é diferente: os desafios se concentram no *accountability gap* (vácuo de responsabilidade), na falta de transparência algorítmica e na dificuldade de assegurar a supervisão humana efetiva quando a decisão impacta a liberdade individual.

No contexto paraense, o Decreto nº 4.690/2025 busca alinhar as especificidades locais ao criar o Grupo de Trabalho para a Estratégia Paraense de Inteligência Artificial (EPIA) (Pará, 2025a). Conforme Dal Pizzol (2025), a ausência de canais institucionais diretos na formulação de políticas tecnológicas gera insegurança jurídica e compromete a adaptação ética do Direito às inovações. A omissão da Polícia Militar na composição do Grupo de Trabalho reproduz essa lacuna: dessa forma, a segurança pública paraense fica sem voz ativa na regulamentação de tecnologias aplicáveis às suas atividades-meio e fim.

O Plano Brasileiro de Inteligência Artificial (PBIA 2024-2028) destaca a soberania tecnológica e o desenvolvimento de modelos baseados em dados nacionais (Brasil, 2024), o que, por extensão, exige dados da criminalidade do Pará. O risco, nesse caso, não é institucional, mas operacional: modelos treinados sem a lógica do policiamento de fronteira e sem a experiência do atendimento primário em áreas de difícil acesso, previstos no Manual de Policiamento Ostensivo Geral da PMPA (Pará, 2024), podem ser implantados com parâmetros inadequados, dificultando a supervisão humana efetiva exigida pela Portaria MJSP nº 961/2025 (Brasil, 2025a) e comprometendo tanto a eficiência quanto a legalidade das ações da

tropa.

2.2 Ética, viés algorítmico e o impacto nas polícias militares

A crença na neutralidade tecnológica revela-se uma premissa equivocada no contexto da segurança pública. Dal Pizzol (2025) assevera que o Direito e a técnica não são neutros nem imparciais; ambos podem contribuir para a manutenção de exclusões e desigualdades. Na atividade policial militar, os algoritmos de IA são alimentados por dados históricos que, invariavelmente, carregam os vieses estruturais da sociedade e das próprias instituições de segurança.

Conforme Costa e Oliveira (2025), o viés algorítmico atua como a causa do problema: o sistema não possui preconceito intencional, mas reflete e automatiza os padrões falhos presentes em sua base de dados. Quando esse viés se materializa no mundo real, gerando tratamento desigual ou restrição de direitos a grupos específicos, ele se converte no efeito, denominado viés discriminatório.

Nesse cenário, a discriminação se manifesta com força total. Não se trata apenas de uma falha matemática, mas da perpetuação automatizada de preconceitos: quando o modelo é treinado com dados que refletem uma atuação policial histórica enviesada, a máquina repete e amplia essa desigualdade, impactando desproporcionalmente as populações que já estão na margem do sistema (Costa; Oliveira, 2025).

Se os registros de prisões e abordagens em um determinado BPM historicamente registram de forma desproporcional determinadas comunidades periféricas, um sistema preditivo alimentado por esses dados direcionará mais policiamento para essas mesmas áreas, criando um ciclo de retroalimentação discriminatório. Na ciência da computação e na sociologia algorítmica, conforme O'Neil (2016 ***apud*** Dal Pizzol, 2025), esse fenômeno é denominado feedback loop (ciclo de retroalimentação): o resultado gerado pela máquina retorna como dado de entrada, o que amplifica de forma contínua o erro original.

O debate em torno desse tipo de viés algorítmico ganhou força após os questionamentos levantados sobre o sistema COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*), adotado pelo judiciário nos Estados Unidos. Conforme Teixeira (2021), a ferramenta do judiciário de Wisconsin apresentava viés racial inequívoco, classificando réus negros como de maior risco de reincidência em comparação aos brancos, mesmo em perfis criminais semelhantes. A empresa desenvolvedora, a Northpointe, teve enormes dificuldades em explicar o funcionamento do algoritmo no caso específico de Eric Loomis, revelando, conforme Costa e Oliveira (2025), a fragilidade do Estado diante da

opacidade privada.

No Brasil, a adoção de tecnologias de reconhecimento facial já resultou em prisões e abordagens equivocadas documentadas pelo Miniguia para juristas sobre o uso de tecnologias de reconhecimento facial na segurança pública, elaborado de forma coletiva pela Campanha Tire Meu Rosto da Sua Mira, conduzida pela organização Conectas Direitos Humanos, e pela Escola de Ativismo (Campanha Tire Meu Rosto da Sua Mira; Escola de Ativismo, 2022). O documento registra casos no Distrito Federal, Rio de Janeiro, Bahia e Piauí, em que pessoas foram submetidas a detenções injustas, condução coercitiva interestadual e restrição de liberdade por erro algorítmico advindo dessas tecnologias IA, o que expõe a limitação técnica e a gravidade ética de se delegar poder de coerção a sistemas matemáticos imperfeitos.

Para Santos et al. (2025), os impactos éticos da automação baseada em IA envolvem o risco de desumanização e a consequente perda de dignidade das pessoas submetidas a decisões automatizadas. Quando a inferência algorítmica sugere a restrição da liberdade de um cidadão, tornando-a como uma variável matemática, a responsabilidade pela decisão final, contudo, ainda recai sobre o agente de segurança, que não pode se eximir de sua obrigação de julgamento sob alegação de automatização.

Sob a ótica normativa, o Estatuto dos Policiais Militares do Estado do Pará (Lei Estadual nº 5.251/1985) corrobora essa premissa ao estabelecer que a responsabilidade pelos atos praticados no exercício da função é pessoal e direta (Art. 10), cabendo ao comandante a responsabilidade pela regularidade do serviço sem que isso exima o subordinado de sua responsabilidade direta (Art. 11). Nesse sentido, o ordenamento jurídico militar pressupõe uma cadeia de responsabilidades estritamente humana, não admitindo, por lógica e por direito, a transferência ou a diluição dessa atribuição decisória para uma máquina.

Apesar dessa clareza legal, a opacidade dos sistemas de IA introduz um severo desafio probatório na apuração do nexo causal. Em caso de uma abordagem injusta direcionada por erro do algoritmo, a tentativa de eximização da culpa torna-se uma realidade processual: o policial militar alega ter sido induzido pela inferência da máquina, o comandante atribui o vício à limitação técnica do modelo adquirido, e o desenvolvedor privado, responsável pela falha lógica, escapa da jurisdição militar amparado pelo segredo industrial. Essa dificuldade concreta de individualizar a conduta e mensurar a falha, mesmo existindo um sujeito responsável na lei, configura o que a doutrina denomina accountability gap (vácuo de responsabilidade), deixando o cidadão lesado sem reparação ágil e o Estado exposto a lides intermináveis (Santos et al., 2025).

2.3 Transparência algorítmica e o dever de explicabilidade

A opacidade dos sistemas de IA, definida como a impossibilidade de acesso e compreensão da lógica interna de processamento dos algoritmos, representa o principal obstáculo para a sua legitimidade democrática na segurança pública. Redes neurais profundas operam de forma tão complexa que nem mesmo seus desenvolvedores conseguem rastrear com precisão a rota lógica que levou o sistema a uma determinada inferência (Nagata, 2024). Na literatura técnica, conforme Teixeira (2021), essa condição é definida como o problema da caixa preta (*black box*), em que os dados de entrada e os resultados de saída são conhecidos, mas o processo decisório interno é inescrutável. No Estado de Direito, o cidadão tem o direito inafastável de saber os fundamentos de uma decisão que lhe afeta a esfera jurídica, princípio este que entra em choque direto com a lógica da caixa preta corporativa.

A transparência algorítmica, compreendida como a abertura e a clareza dos processos decisórios da máquina, permitindo auditoria e compreensão humana, exige atenção em duas dimensões essenciais para as atividades-meio e fim da PMPA: a do código-fonte (software aberto) e a da lógica decisória (explicabilidade). Teixeira (2021) defende que softwares adquiridos com recursos públicos devem possuir código aberto, permitindo auditorias independentes e mitigando a dependência tecnológica do Estado em relação a grandes corporações tecnológicas. Como exemplo de governança, cita-se a Carta de Algoritmo da Nova Zelândia, (Nova Zelândia, 2020 ***apud*** Teixeira, 2021), em que órgãos públicos comprometem se a documentar o funcionamento dos algoritmos em linguagem simples, revisá-los periodicamente e fornecer canais de apelação aos afetados pelas decisões automatizadas.

No setor público brasileiro, coube ao Judiciário a iniciativa de fixar os primeiros limites éticos e técnicos para o uso da IA. A Portaria CNJ nº 271/2020 do Conselho Nacional de Justiça (CNJ) (Brasil, 2020a) regulamentou o uso da IA em seu âmbito e, complementando-a, a Resolução nº 332/2020 do Conselho Nacional de Justiça (CNJ) (Brasil, 2020b) estabeleceu parâmetros rígidos de ética, transparência e auditabilidade para o Judiciário (Teixeira, 2021), norma recentemente revogada e substituída pela Resolução CNJ nº 615/2025 do Conselho Nacional de Justiça (CNJ) (Brasil, 2025b), que mantém e aprofunda a exigência de transparência e auditabilidade algorítmica.

Na segurança pública, porém, a realidade é diferente: as polícias militares estaduais ainda operam sem a mesma estrutura normativa. Esse cenário começou a mudar recentemente com a edição da Portaria MJSP Nº 961/2025 (Brasil, 2025a), que dedicou seção específica às

soluções de inteligência artificial, impondo a obrigatoriedade de supervisão humana efetiva sobre inferências algorítmicas de risco, a exigência de transparência e registros de log, que constituem o histórico automatizado e imutável das operações do sistema, além de vedar o uso de tecnologias que resultem em lesão à vida ou em vigilância biométrica indevida.

Na prática, para a PMPA, o cumprimento desses preceitos ultrapassa o campo das recomendações éticas e caminha para se consolidar como exigência legal. O Art. 8º do PL nº 2.338/2023 assegura à pessoa afetada o direito de solicitar explicações sobre a decisão automatizada, incluindo informações sobre a racionalidade do sistema, os dados processados, os critérios utilizados e, quando aplicável, a ponderação adotada pelo modelo (Brasil, 2023).

Caso a PMPA utilize sistemas inescrutáveis, torna-se materialmente impossível exercer o direito de defesa do cidadão e inviabiliza a revisão hierárquica do ato policial, uma vez que o comandante não pode avaliar a legalidade ou a proporcionalidade de uma ação cujos critérios de disparo estão ocultos na estrutura lógica do algoritmo. Isso viola o princípio do devido processo legal e o da ampla defesa.

Para conter a opacidade algorítmica em sistemas de IA, a doutrina e o cenário regulatório em estruturação no país, representado pelo PL nº 2.338/2023 (Brasil, 2023), em tramitação, e na Portaria MJSP nº 961/2025 (Brasil, 2025a), já vigente, tornam obrigatórios os protocolos de governança algorítmica. No cenário da segurança pública, tais protocolos são definidos como o conjunto de diretrizes e procedimentos técnicos que asseguram a supervisão humana efetiva, a transparência decisória e a auditabilidade dos sistemas (Brasil, 2025a; Dal Pizzol, 2025). O propósito desses mecanismos, conforme Dal Pizzol (2025), é coibir que a automação suplante a responsabilidade ética do profissional, assegurando que a tecnologia funcione como instrumento subordinado ao controle hierárquico e que o agente humano se mantenha no núcleo das decisões sobre direitos fundamentais.

3 METODOLOGIA

3.1 Tipo da pesquisa

A presente pesquisa classifica-se, quanto à natureza, como aplicada, por buscar gerar conhecimentos direcionados à solução de problemas concretos e imediatos da PMPA, especificamente no tocante à conformidade legal de suas aquisições tecnológicas. A abordagem de pesquisa selecionada é a qualitativa, uma vez que analisa aspectos éticos, jurídicos e sociais que não podem ser quantificados ou reduzidos a tratamento estatístico isolado (Gil, 2017).

Do ponto de vista de seus fins, a pesquisa se mostra exploratória e descritiva: exploratória por aprofundar-se em um arcabouço normativo recentíssimo e em fase de consolidação (PL nº 2.338/2023, Portaria MJSP nº 961/2025, Resolução CNJ nº 615/2025 e Decreto Paraense nº 4.690/2025), e descritiva por detalhar os riscos e as características da IA na segurança pública, com foco nas especificidades da Polícia Militar do Pará. Quanto aos meios ou procedimentos técnicos, enquadra-se como uma pesquisa bibliográfica e documental. Essa matriz classificatória respalda-se em Gil (2017), para quem a pesquisa aplicada e exploratória viabiliza a compreensão de fenômenos recentes, e em Demo (2009), que destaca a pertinência da abordagem qualitativa na interpretação de questões ético-sociais.

3.2 Lócus da pesquisa

A delimitação espacial concentrou-se na realidade institucional da Polícia Militar do Pará (PMPA). O lócus abrange as unidades responsáveis pelas atividades-fim, especificamente as unidades operacionais no Estado, compostas por Batalhões de Polícia Militar (BPM), Companhias Independentes de Polícia Militar (CIPM) e os centros de comando e controle (CIOp/NIOp), dentre outros, alinhando-se estritamente ao escopo operacional discutido ao longo do estudo. Esse recorte justifica-se pela necessidade de analisar os impactos éticos e jurídicos da automação algorítmica na rotina real da tropa paraense, considerando as particularidades da segurança pública no Estado do Pará.

3.3 Fontes de dados

A investigação ocorreu por meio de pesquisa bibliográfica e documental, tendo como universo analítico a produção científica e normativa sobre IA no campo da segurança pública e seus reflexos institucionais na Polícia Militar do Pará (PMPA). A delimitação temporal abrangeu o período de 2021 a 2025, recorte que acompanhou a maturação do debate regulatório nacional até a edição das normas mais recentes.

O corpus bibliográfico foi composto por artigos científicos, teses, dissertações e livros, extraídos de repositórios institucionais de teses (como o Lume da UFRGS), plataformas de periódicos científicos (como sistemas OJS e Zenodo) e bases de indexação acadêmica (Google Scholar). O recorte temporal das publicações restringiu-se a esse mesmo período, selecionando-se obras de rigorosa relevância sobre o tema.

Já o corpus documental abrangeu normas jurídicas, manuais institucionais, relatórios de campanhas e notas públicas, extraídos de acervos e repositórios oficiais. Para a legislação

federal e normas do Poder Judiciário, utilizaram-se os portais do Senado Federal, do Planalto e do Conselho Nacional de Justiça. Para as normas estaduais e documentos da PMPA, acessou se o Diário Oficial do Estado do Pará e o portal oficial da corporação. Relatórios técnicos e notas públicas foram obtidos nos sítios eletrônicos da Defensoria Pública do Rio de Janeiro, da Agência Pará e do Comitê Gestor da Internet no Brasil (CGI.br).

3.4 Procedimentos de coleta de dados

Os procedimentos de coleta adequaram-se à tipologia das fontes. Na vertente bibliográfica, rastrearam-se repositórios acadêmicos e bases indexadoras mediante os descritores "Inteligência Artificial", "Segurança Pública", "Transparência Algorítmica" e "Regulação", restringindo a seleção às produções alinhadas ao escopo policial militar. No âmbito documental, consultaram-se os portais oficiais (Senado Federal, CNJ e site da PMPA), empregando filtros de data e tema para isolar as normas e manuais em vigor, e em seguida efetuando-se o download da legislação e dos manuais publicados no período delimitado.

3.5 Técnicas empregadas na análise dos dados

O material foi examinado mediante análise crítica de conteúdo, conforme propõe Moraes (1999), técnica voltada a superar a descrição literal dos textos e inferir sentidos sobre as condições de produção das mensagens. O percurso analítico dividiu-se em três fases: (1) pré análise, com organização e leitura flutuante; (2) exploração, com codificação e isolamento temático em eixos (regulatório, ético e de transparência); e (3) interpretação, cruzando as inferências normativas com a rotina operacional da PMPA.

Como forma de controle crítico, as inferências foram contrastadas com os princípios constitucionais da Administração Pública, evitando vieses de confirmação. Dada a natureza bibliográfica e documental da investigação, sem sujeitos ou dados nominativos, a submissão ao Comitê de Ética tornou-se dispensável, em conformidade com a Resolução CNS nº 510/2016. Registre-se, como limitação do estudo, a inexistência de dados primários internos à PMPA, o que circunscreveu as conclusões ao cenário normativo, deixando de cobrir as especificidades de infraestrutura dos batalhões locais.

4 RESULTADOS E DISCUSSÃO

A análise dos dados documentais aponta o enquadramento da segurança pública como setor de alto risco ou risco excessivo no marco regulatório emergente como resultado imediato e mais severo para a PMPA. O PL nº 2.338/2023, em seu Art. 15, veda o uso de sistemas de

identificação biométrica à distância em tempo real pelo poder público ressalvadas as hipóteses estritas de persecução penal individualizada com autorização judicial, busca de vítimas, crime em flagrante com pena superior a dois anos e cumprimento de mandados de prisão (Brasil, 2023).

Conforme Lima, D'ornellas e Pessoa (2025), a classificação rigorosa dessas tecnologias é imperativa para coibir que a eficiência operacional se sobreponha à dignidade humana. Essa restrição é estendida para as instituições estaduais de segurança pública pela Portaria MJSP nº 961/2025 (Art. 11), que condiciona a legalidade dessas soluções de inteligência artificial ao emprego de recursos do Fundo Nacional de Segurança Pública (FNSP) e reitera as hipóteses excepcionais de uso (Brasil, 2025a). Na prática da PMPA, o cenário é de estrita vedação legal quando vinculada ao custeio federal: qualquer aquisição de sistemas de identificação biométrica em tempo real fora das exceções descritas é ilícita e, nos termos do Art. 15 da própria Portaria MJSP nº 961/2025, sujeitará os responsáveis ao rigor das sanções nas esferas administrativa, civil e criminal (Brasil, 2025a).

Cercada por essas restrições normativas, a PMPA deve reorientar seus investimentos em tecnologia para garantir que sua modernização não resulte em nulidades judiciais, insegurança jurídica ou desperdício de recursos públicos. Em vez de buscar câmeras com varredura facial massiva para as ruas dos municípios paraenses, o que configuraria risco excessivo, a Corporação pode priorizar a implementação de sistemas de Inteligência Artificial (IA) voltados às atividades-meio, como o apoio logístico e a gestão documental, visto que tais funções apresentam menor potencial de lesão a direitos fundamentais e maior aceitação ética.

Contudo, a aplicação dessas tecnologias em atividades-fim, como o policiamento ostensivo, permanece como uma possibilidade institucional legítima, desde que estritamente condicionada aos parâmetros da Portaria do Ministério da Justiça e Segurança Pública (MJSP) nº 961/2025. Um exemplo é o uso de Processamento de Linguagem Natural no tratamento de áudio do rádio do Núcleo Integrado de Operações (NIOp) para triagem de ocorrências por nível de risco, prática já adotada com sucesso pela Polícia Militar de São Paulo (Costa; Oliveira, 2025).

Nesse cenário, a inferência algorítmica não resulta em restrição imediata da liberdade do cidadão, mas no direcionamento de recursos logísticos, configurando uma aplicação de menor risco jurídico e alto valor operacional. Consoante Dal Pizzol (2025), há uma tensão evidente ao condenar a opacidade algorítmica dos modelos preditivos de segurança e, ao mesmo tempo, aceitar a IA na esfera administrativa. Essa fronteira não é demarcada pela eficiência da ferramenta, mas pela salvaguarda constitucional, visto que o poder de restringir a

liberdade alheia exige um julgamento moral e ético que o algoritmo, desprovido de empatia, é incapaz de reproduzir.

Na automação de rotinas de apoio, como a triagem de documentos internos ou a gestão de frotas (atividades-meio), na hipótese de a PMPA adotar tais modelos, o algoritmo não tem qualquer ingerência sobre a liberdade individual. Já no direcionamento do policiamento ostensivo preditivo (atividade-fim), a inferência da máquina recai de forma imediata e restritiva sobre o corpo e a liberdade do cidadão abordado, potencialmente eliminando o filtro da deliberação humana.

Paralelamente à classificação de risco, a análise dos impactos éticos e operacionais evidencia um cenário ainda mais complexo, centrado no viés discriminatório sistêmico e na opacidade decisória. Dal Pizzol (2025) e Costa e Oliveira (2025) convergem de maneira incisiva para a problemática do *feedback loop*. Sistemas de policiamento preditivo, ao processarem os dados massivos captados por bodycams, Veículos Aéreos Não Tripulados (VANTs) e plataformas como o Sinesp, tendem a replicar a seletividade penal histórica das instituições. Na prática, se um modelo for treinado com Boletim de Atendimento Policial Militar (BAPM) que registram de forma desproporcional abordagens em comunidades periféricas, a máquina direcionará mais policiamento para essas áreas, validando estatisticamente o próprio preconceito e gerando mais prisões, que alimentarão o sistema novamente.

Caso a PMPA implemente modelos preditivos para despacho de viaturas de um BPM via Centro Integrado de Operações (CIOp) na Região Metropolitana de Belém, e esse modelo for treinado com dados viciados das últimas décadas, a resultante será um policiamento ostensivo desproporcional em periferias, contrariando o princípio da igualdade e a própria doutrina de Direito Fraterno, que impõe ao Direito uma adaptação ética e solidária às inovações tecnológicas, evocada por Dal Pizzol (2025). A solução não é a rejeição tecnológica, mas a imposição da "supervisão humana efetiva", ou seja, a obrigação do agente de segurança de revisar e, se necessário, reverter a inferência algorítmica antes da tomada de decisão que impacte direitos fundamentais, conforme preconiza o Art. 10 da Portaria MJSP nº 961/2025 (Brasil, 2025a).

O operador e seu comandante não podem se tornar meros validadores de *scores* de risco, ou seja, as pontuações probabilísticas geradas pelo algoritmo que classificam indivíduos ou áreas conforme seu potencial de ameaça. Por essa razão, a inferência da IA deve ser tratada como um elemento informativo subsidiário, jamais como prova ou ordem autônoma. O policial militar deve ter a prerrogativa e o dever de rejeitar a recomendação do algoritmo

quando a realidade de campo demonstrar sua inadequação, respondendo, entretanto, por essa decisão dentro da cadeia de comando.

Nessa dinâmica, a tecnologia auxilia o policial militar no cruzamento de dados da ocorrência, mas a deliberação ética sobre a abordagem permanece exclusivamente humana.O respeito à dignidade da pessoa humana exige que a empatia e o julgamento moral situacional, traços próprios da atuação policial, prevaleçam sobre a frieza da probabilidade estatística. Ao garantir essa prevalência, impedindo que a máquina substitua o discernimento tático do operador, preserva-se não apenas a liberdade do cidadão, mas a própria integridade da responsabilidade hierárquica no emprego da força.

Somado à seletividade algorítmica, a PMPA poderá enfrentar outro risco crítico: o "efeito caixa preta" (*black box*) nas aquisições de sistemas de IA, caracterizado pela compra de tecnologias cuja lógica decisória interna é inacessível ao órgão público, geralmente blindada sob a proteção do segredo industrial do fornecedor. Nagata (2024) e Teixeira (2021) demonstram que as polícias frequentemente adquirem sistemas proprietários cuja arquitetura lógica é protegida por segredo industrial, fator que inviabiliza a auditoria algorítmica externa e o direito de explicação do afetado. Essa opacidade algorítmica representa um sério entrave contratual e gerencial para a organização policial militar.

Ao licitar sistemas de IA, a PMPA deve exigir, como parâmetro de transparência e critério obrigatório de habilitação, a abertura do código-fonte ou, ao menos, a disponibilização de documentação técnica exaustiva que garanta a auditabilidade externa e a explicabilidade da decisão. Conforme Teixeira (2021), a dependência tecnológica do Estado em relação a fornecedores privados, cujos modelos de negócio frequentemente blindam o código como segredo industrial, só é mitigada pela exigência de software aberto. O autor defende que, mesmo contrariando a lógica corporativa privada, a Administração Pública deve priorizar o código aberto para viabilizar auditorias independentes, garantir a transparência algorítmica e minimizar vieses discriminatórios ocultos.

Sob a ótica do Art. 8º do PL nº 2.338/2023, o direito à explicação impõe ao Estado o dever de explicitar a racionalidade da decisão automatizada. É institucionalmente insustentável que a PMPA tenha que responder a um habeas corpus argumentando que o sistema não pode ser explicado por restrições de propriedade intelectual da empresa contratada. A Nota Pública do CGI.br (2023) reforça que a regulação deve observar a assimetria entre atores, protegendo os menores desenvolvedores nacionais, mas não pode abrir mão da transparência quando o bem jurídico tutelado é a liberdade do cidadão. A Tabela 1 resume todos os riscos mapeados e as leis que os baseiam.

Tabela 1 – Mapeamento de Riscos Algorítmicos e Parâmetros Regulatórios Aplicáveis à PMPA

RISCO IDENTIFICADO	DESCRIÇÃO FÁTICA	PARÂMETRO LEGAL/REGULATÓRIO CORRESPONDENTE
Vigilância Massiva	Uso de reconhecimento facial em tempo real em espaços públicos sem autorização judicial	Art. 15, PL nº 2.338/2023; Art. 11, Portaria MJSP nº 961/2025
Viés Discriminatório	Direcionamento de tropa baseado em dados históricos viciados	Art. 12, PL nº 2.338/2023; Nota Pública CGI.br (2023)
Opacidade Decisória	Sistemas *black box* sem possibilidade de explicação da inferência	Art. 8º, PL nº 2.338/2023; Resolução CNJ nº 615/2025 (analogia)
Ausência de Supervisão Humana Efetiva	Decisões algorítmicas autônomas sem revisão crítica do agente de segurança, gerando risco de desumanização da ação policial	Art. 10, Portaria MJSP nº 961/2025; Art. 3º, VII, Resolução CNJ nº 615/2025 (analogia)
Lacuna de Responsabilização	Impossibilidade de imputar dolo/culpa pela decisão da máquina	Art. 27, PL nº 2.338/2023; Santos et al. (2025)

Fonte: Elaborado pelos autores (2025), com base na classificação de riscos de Dal Pizzol (2025).

Para além dos entraves jurídicos e operacionais, a PMPA não teve representação institucional na formulação da estratégia paraense de inteligência artificial. Isso porque o Decreto nº 4.690/2025, que instituiu o Grupo de Trabalho para a Estratégia Paraense de Inteligência Artificial (EPIA), deixou a Corporação de fora de sua composição original, reservando a vaga apenas ao Corpo de Bombeiros Militar do Pará (CBMPA) (Pará, 2025a). Essa ausência ganha relevância porque o PBIA 2024-2028 insiste na necessidade de uma IA sustentável e adaptada ao contexto local, como o amazônico, e prevê investimentos pesados em infraestrutura de dados.

Ficar de fora desse debate cria um descompasso direto entre as diretrizes estaduais e a realidade operacional da Corporação. O PBIA prioriza modelos nacionais e LLMs, e é justamente a PMPA que detém o acervo mais rico de dados de segurança com particularidades amazônicas. Sem a presença da instituição nas discussões da EPIA, aumenta

consideravelmente a chance de a regulamentação ignorar as demandas da tropa e as especificidades da criminalidade no Estado, sobretudo porque a classificação da segurança pública como área de alto risco no futuro marco regulatório nacional (PL nº 2.338/2023) exige protocolos de governança específicos que só a PMPA pode operacionalizar.

Diante disso, a saída é a PMPA assumir uma postura proativa e apresentar propostas ao Grupo de Trabalho. A sugestão é a criação de um subcomitê de segurança pública na EPIA e a adoção da Avaliação de Impacto Algorítmico (AIA) como parâmetro obrigatório de auditabilidade voltado à atividade policial militar, para garantir que a inovação no Estado caminhe junto com a supervisão humana e a proteção dos direitos fundamentais.

5 CONCLUSÃO

O objetivo geral desta pesquisa foi analisar como a PMPA pode implementar soluções de IA em suas atividades-meio e fim, garantindo a transparência algorítmica e a supervisão humana efetiva, em conformidade com o marco legal emergente e mitigando vieses discriminatórios. Retomando o problema de pesquisa, questionava-se: como a PMPA pode utilizar soluções de IA em suas atividades-meio e fim de maneira compatível com a transparência algorítmica, a supervisão humana efetiva e em conformidade com o marco legal emergente, mitigando vieses discriminatórios? A resposta construída ao longo deste estudo demonstra que a viabilidade jurídica e operacional dessas tecnologias está estritamente condicionada à adoção de uma governança institucional robusta, capaz de subordinar a eficiência da máquina aos direitos fundamentais e à doutrina de emprego da tropa.

Verificou-se que a implementação de soluções de IA pela PMPA não apenas se mostra viável, mas também estratégica para o aprimoramento das atividades-meio e fim. Ainda assim, sua implementação depende da observância rigorosa da arquitetura de riscos proposta pelo PL nº 2.338/2023 e das limitações da Portaria MJSP nº 961/2025 (Brasil, 2025a). Nesse contexto, a classificação da segurança pública como setor de alto risco restringe práticas experimentais e exige a realização da Avaliação de Impacto Algorítmico e veda, de forma contundente, práticas de vigilância massiva, como o reconhecimento facial em tempo real em espaços públicos, ressalvadas as hipóteses legais. Essa vedação impõe ao Departamento Geral de Administração (DGA) e aos setores de aquisição da Corporação o dever de reformular seus editais e termos de referência, sob pena de nulidade dos contratos e responsabilização dos gestores.

Percebe-se que a adoção dessas soluções de IA pela PMPA não depende somente da eficiência técnica dos sistemas empregados. A discussão desenvolvida ao longo do estudo mostrou que a utilização de ferramentas pouco transparentes pode criar obstáculos para a

fiscalização da própria atividade policial, sobretudo quando não existem mecanismos mínimos de auditabilidade. Por esse motivo, entende-se como necessária a preferência por sistemas explicáveis, além da previsão contratual de acesso à documentação técnica, abertura de código e outras formas de verificação dos modelos utilizados pela Corporação. A superação do efeito caixa preta não é apenas uma exigência ética, mas um imperativo de controle interno, permitindo que a Corregedoria-Geral e o Centro de Inteligência (C.INT) realizem auditorias eficazes sobre os critérios empregados nas inferências automatizadas.

A questão da supervisão humana também apareceu como um ponto sensível da pesquisa. No contexto da atividade policial militar, a inferência produzida pelo sistema não pode substituir a decisão tomada pelo responsável pela ação. Dessa forma, a necessidade de registrar esse limite em normativa interna surge como medida importante para preservar a responsabilidade hierárquica e evitar o afastamento humano do processo decisório. A Portaria MJSP nº 961/2025 corrobora essa premissa ao exigir o meaningful human control, o que na prática operacional significa que o comandante da fração ou o policial militar na ponta do atendimento (BAPM) mantém a prerrogativa e o dever de rejeitar a recomendação da máquina quando esta conflitar com a realidade tática do terreno.

No plano governativo, o estudo indicou que a PMPA precisa participar das iniciativas estaduais relacionadas à governança da IA. A presença da Corporação no Grupo de Trabalho da EPIA pode auxiliar na construção de modelos mais compatíveis com as demandas e particularidades da segurança pública no Estado do Pará. A exclusão atual do Decreto nº 4.690/2025 representa um risco estratégico, pois modelos treinados sem a expertise do policiamento ostensivo nas especificidades amazônicas tendem a gerar falsos positivos e a comprometer a credibilidade do Sistema Nacional de Informações de Segurança Pública (Sinesp) em nossa região.

O atendimento aos objetivos específicos reforça esse quadro. O mapeamento legal deixou evidente que o uso de IA em espaços públicos sofre bloqueios rigorosos. Ao dissecar os riscos, ficou patente como o viés algorítmico e o feedback loop discriminatório comprometem a ética e a operacionalidade da tropa. E a saída apontada pela pesquisa é direta: a proposição de transparência via abertura de código e a adoção de Avaliações de Impacto como parâmetros de auditabilidade, garantindo o direito à explicação. Tais medidas operacionalizam a escada de objetivos traçada na introdução, transformando conceitos abstratos de regulação em Procedimentos Operacionais Padrão (POP) exequíveis pelos Batalhões de Polícia Militar (BPM) e Companhias Independentes.

Diante do exposto, a conclusão é contundente. A modernização da PMPA, dissociada dos parâmetros éticos e do controle jurídico, configura violação de direitos em vez de sua prevenção. A máquina não decide o destino da ação policial. No dia a dia da tropa, a hierarquia, a disciplina e a dignidade da pessoa humana não podem ficar subordinadas à eficiência algorítmica. Para materializar esse controle na prática, o estudo aponta a urgência de uma pesquisa aplicada que construa um modelo normativo interno de Avaliação de Impacto Algorítmico, focado na realidade das Operações Policiais Militares no Pará. Somente através dessa vigilância epistemológica e normativa a inovação tecnológica deixará de ser um risco jurídico para se consolidar como uma ferramenta legítima de defesa social.

REFERÊNCIAS

AMORIM, Tarcya. Polícia Militar do Pará apresenta inovações tecnológicas e práticas sustentáveis na COP30. **Agência Pará**, Belém, 14 nov. 2025. Disponível em: https://www.agenciapara.com.br/noticia/72505/policia-militar-do-para-apresenta-inovacoestecnologicas-e-praticas-sustentaveis-na-cop30. Acesso em: 08 maio 2026.

BRASIL. Ministério da Ciência, Tecnologia e Inovação. **Plano Brasileiro de Inteligência Artificial (PBIA) 2024-2028**: IA para o bem de todos. Brasília, DF: MCTI, 2024. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/planobrasileiro-de-inteligencia-artificial-pbia-_vf.pdf. Acesso em: 08 maio 2026.

BRASIL. Ministério da Justiça e Segurança Pública. **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**, Brasília, DF, 2025a. Disponível em: https://www.gov.br/mj/ptbr/assuntos/noticias/portaria-do-mjsp-regulamenta-uso-de-tecnologia-em investigacoes-criminais-e-inteligencia-de-seguranca-publica/portaria-no961-de-24-de junho-de-2025. Acesso em: 09 maio 2026.

BRASIL. Conselho Nacional de Justiça. **Resolução nº 615, de 11 de março de 2025**. Estabelece diretrizes para o desenvolvimento, utilização e governança de soluções desenvolvidas com recursos de inteligência artificial no Poder Judiciário. **Diário Oficial da União**, Brasília, DF, 2025b. Disponível em: https://atos.cnj.jus.br/files/original155530202503146 7d4517244566.pdf. Acesso em: 10 maio

2026.

BRASIL. Senado Federal. **Projeto de Lei nº 2.338, de 2023**. Dispõe sobre o uso da Inteligência Artificial. Brasília, DF, 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 12 maio 2026.

BRASIL. Conselho Nacional de Justiça. **Portaria nº 271, de 20 de agosto de 2020**. Dispõe sobre a organização e o funcionamento do Departamento de Gestão de Dados e Estatística do Conselho Nacional de Justiça e dá outras providências. **Diário Oficial da União**, Brasília, DF, **2020a**. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3424. Acesso em: 14 maio 2026.

BRASIL. Conselho Nacional de Justiça. **Resolução nº 332, de 25 de agosto de 2020**. Estabelece diretrizes para o desenvolvimento, utilização e governança de soluções desenvolvidas com recursos de inteligência artificial no Poder Judiciário. **Diário Oficial da União**, Brasília, DF, **2020b**. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3435. Acesso em: 16 maio 2026.

CAMPANHA TIRE MEU ROSTO DA SUA MIRA; ESCOLA DE ATIVISMO. **Miniguia para juristas sobre o uso de tecnologias de reconhecimento facial na segurança pública**. [S.l.: s.n.], 2022. Disponível em: https://defensoria.rj.def.br/uploads/arquivos/f38beb39ffe14910841966dc0fb19c11.pdf. Acesso em: 19 maio 2026.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Nota Pública sobre PL 2.338/2023 e regulação de sistemas de Inteligência Artificial no Brasil**. São Paulo: CGI.br, 2023. Disponível em: https://cgi.br/media/docs/publicacoes/4/ptbr/20260305145405/Nota_Tecnica_PL_2338_Regulacao_IA.pdf. Acesso em: 21 maio 2026.

COSTA, João Vitor Duarte da; OLIVEIRA, Janaina de. A relação entre os dilemas éticos e a utilização da inteligência artificial na segurança pública. **Interface Tecnológica**, Taquaritinga, v. 22, n. 2, p. 277-289, 2025. DOI: 10.31510/infa.v22i2.2366.

DAL PIZZOL, Dineia Anziliero. **Inteligência Artificial na Segurança Pública**: uma análise dos riscos, oportunidades e diretrizes regulatórias. 2025. Tese (Doutorado em Direito) –**Universidade Federal do Rio Grande do Sul**, Porto Alegre, 2025. Disponível em:

https://lume.ufrgs.br/handle/10183/300097 Acesso em: 24 de maio de 2026.

DEMO, Pedro. **Metodologia do conhecimento científico**. São Paulo: Atlas, 2009.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 7. ed. São Paulo: Atlas, 2017.

LIMA, Isabela Quinto; D'ORNELLAS, Maria Cristina Gomes da Silva; PESSOA, João Pedro Seefeldt. A necessidade de regulamentação da inteligência artificial militar no Brasil: impactos éticos e jurídicos. 2025. Artigo acadêmico (Bacharelado em Direito) – Universidade Federal de Santa Maria, Santa Maria, 2025. Disponível em: https://repositorio.ufsm.br/handle/1/12345. Acesso em: 25 maio 2026.

MORAES, Roque. **Análise de texto e discurso**: princípios e procedimentos. 1999. 126 f. Tese (Doutorado em Educação) – **Universidade Federal do Rio Grande do Sul**, Porto Alegre, 1999.

NAGATA, Sabrina Vettorazzi. Utilização da inteligência artificial na segurança pública e sua contribuição na Polícia Militar. **Brazilian Journal of Development**, Curitiba, v. 10, n. 6, p. e70815, 2024. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/70815. Acesso em: 28 maio 2026.

NOVA ZELÂNDIA. **Algorithm Charter**. 2020. Disponível em: https://data.govt.nz/use data/data-ethics/government-algorithm-transparency-and-accountability/algorithm-charter/. Acesso em: set. 2020. *Apud*: TEIXEIRA, Lucas de Barros. Transparência algorítmica em soluções utilizadas por governos mundo afora, e o contexto Brasil. **Interface Tecnológica**, [S.l.], v. 18, n. 1, p. 12-28, 2021.

PARÁ. Governo do Estado. **Decreto nº 4.690, de 27 de maio de 2025a**. Institui Grupo de Trabalho para elaborar propostas preliminares para a Estratégia Paraense de Inteligência Artificial (EPIA) e a estruturação de um Marco Legal Estadual da Inteligência Artificial (IA). **Diário Oficial do Estado do Pará**, Belém, PA, 30 maio 2025.

PARÁ. **Lei nº 5.251, de 31 de julho de 1985**. Dispõe sobre o Estatuto dos Policiais Militares do Estado do Pará. **Diário Oficial do Estado do Pará**, Belém, PA, 31 jul. 1985. Disponível em: https://www.pm.pa.gov.br/images/PM1/Lei_n%C2%BA_5.251_de_31_de_julho_de_1985_E

STATUTO_DOS_MILITARES_2022.pdf. Acesso em: 26 maio 2026.

PARÁ. Polícia Militar do Pará. **Manual de Policiamento Ostensivo Geral (POG)**: Volume I. Belém: PMPA, 2024. Publicado no Aditamento ao Boletim Geral nº 220 II, de 27 nov. 2024. Disponível em: https://www.pm.pa.gov.br/phocadownload/userupload/userupload/sales.44248/ADIT.%20BG%20N%20220%20II%20de%2027%20NOV%202024%20-%20MANUAL%20DE%20POLICIAMENTO%20OSTENSIVO%20GERAL%20POG.pdf. Acesso em: 4 jun. 2026.

PARÁ. Polícia Militar do Pará. **PM participa de assinatura de ordem para a instalação de 50 novos totens de segurança no estado.** Belém, 2025b. Disponível em: https://www.pm.pa.gov.br/component/content/article/80-blog/news/8387-pm-participa-deassinatura-de-ordem-para-a-instalacao-de-50-novos-totens-de-seguranca-no-estado.html. Acesso em: 5 jun. 2026.

SANTOS, Gleyciellen Borges dos; BATISTA, Mariana Vieira; FRATTARI, Marina Bonissato. A utilização de inteligência artificial nas operações militares e os limites jurídicos à luz do Direito Internacional Humanitário. **Revista do Ministério Público Militar**, Brasília, a. 52, n. 48, p. 245-304, 2º sem. 2025. DOI: 10.5281/zenodo.17869820.

TEIXEIRA, Lucas de Barros. Transparência algorítmica em soluções utilizadas por governos mundo afora, e o contexto Brasil. **Interface Tecnológica**, [S.l.], v. 18, n. 1, p. 12-28, 2021. DOI: 10.31510/infa.v18i1.1083.

VIRGOLINO, Bianca. PMPA avança na utilização de câmeras corporais. **Polícia Militar do Pará**, Belém, 18 jan. 2024. Disponível em: https://www.pm.pa.gov.br/component/content/article/80-blog/news/5647-pmpa-avanca-nautilizacao-de-cameras-corporais-por-militares-da-corporacao.html. Acesso em: 08 jun 2026.