www.revistaft.com.br

Revista FT | ISSN 1678-0817 | v.30, n.164, 2026 | DOI: 10.69849/jyb2f436

Governança preditiva de força de trabalho em segurança pública na era da inteligência artificial: arquitetura em nuvem e IA generativa para otimização de escalas, prontidão operacional e gestão estratégica do efetivo

Predictive workforce governance in public safety in the era of artificial intelligence: cloud architecture and generative AI for shift optimization, operational readiness, and strategic staffing management

Alisson Schmidt Diniz

RESUMO:

A gestão do efetivo operacional em polícias, corporações militares e órgãos de segurança governamental é um dos problemas estruturais mais difíceis da administração pública. A dependência de sistemas legados fragmentados e de planilhas eletrônicas estáticas gera baixa transparência administrativa, lentidão na mobilização de tropas, erros na apuração de direitos e na concessão de folgas regulamentares, aumento de gastos com horas extras e desgaste físico e psicológico dos agentes. Este artigo propõe um modelo conceitual e arquitetural de Governança Preditiva de Força de Trabalho (Workforce Governance) que integra computação em nuvem (SaaS/IaaS), ciência de dados e inteligência artificial (IA) preditiva e generativa. O modelo é organizado em três camadas: (i) ingestão de dados e automação em nuvem, que centraliza e padroniza informações de disponibilidade, folha de pagamento e competências táticas especializadas (atiradores de precisão, pilotos, condutores táticos e peritos, entre outras); (ii) inteligência analítica e predição, com modelos estatísticos e de aprendizado de máquina (ARIMA e regressão multilinear sazonal) e arquitetura de Geração Aumentada por Recuperação (RAG), voltada a antecipar lacunas no efetivo, simular picos de demanda em eventos críticos e identificar sinais precoces de fadiga e estresse operacional; e (iii) interface e visualização para decisão, com painéis gerenciais atualizados em tempo real e organizados em torno do Índice de Prontidão da Tropa (IPT). Uma simulação de mobilização emergencial em cenário de Alerta de Segurança Nacional, feita com dados sintéticos, indicou redução superior a 80% no retrabalho burocrático e queda do tempo de recomposição das equipes de horas para minutos. Por fim, o trabalho analisa a conformidade ética e legal do modelo diante da Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/2018) e do Projeto de Lei nº 2.338/2023, que trata da regulação da IA no Brasil, com atenção à Avaliação de Impacto Algorítmico (AIA), à prevenção de vieses discriminatórios e à supervisão humana, em alinhamento com as referências internacionais ISO/IEC 42001 e NIST AI RMF.

Palavras-chave: Governança Preditiva. Força de Trabalho. Inteligência Artificial. Arquitetura em Nuvem. Prontidão Operacional. Segurança Pública.

ABSTRACT:

Managing operational staff in police forces, military corporations and government security agencies is one of the most difficult structural problems in public administration. Reliance on fragmented legacy systems and static spreadsheets leads to poor administrative transparency, slow troop mobilization, errors in calculating entitlements and regulatory time

off, higher overtime costs, and physical and psychological strain on officers. This paper proposes a conceptual and architectural model of Predictive Workforce Governance that combines cloud computing (SaaS/IaaS), data science, and predictive and generative artificial intelligence (AI). The model is organized in three layers: (i) cloud data ingestion and automation, which centralizes and standardizes availability, payroll and specialized tactical skills data (such as snipers, pilots, tactical drivers and crisis negotiators); (ii) analytics and prediction, using statistical and machine learning models (ARIMA and seasonal multiple regression) and Retrieval-Augmented Generation (RAG) to anticipate staffing gaps, simulate demand peaks during critical events and detect early signs of fatigue and operational stress; and (iii) decision interface and visualization, with real-time management dashboards built around a Troop Readiness Index (TRI). A simulated emergency mobilization under a National Security Alert, run on synthetic data, indicated a reduction of more than 80% in bureaucratic rework and cut the time needed to reassemble specialized teams from hours to minutes. Finally, the paper examines the model's ethical and legal compliance under the Brazilian General Data Protection Law (LGPD) and Bill No. 2,338/2023 on AI regulation, focusing on Algorithmic Impact Assessments (AIA), bias prevention and human oversight, in line with ISO/IEC 42001 and the NIST AI RMF.

Keywords: Predictive Governance. Workforce Management. Artificial Intelligence. Cloud Architecture. Operational Readiness. Public Safety.

1 INTRODUÇÃO

Polícias, corporações militares e demais órgãos de segurança pública enfrentam hoje um desafio considerável na gestão do seu pessoal. A criminalidade contemporânea, marcada por organizações transnacionais conectadas, por crises socioambientais recorrentes e por ameaças cada vez mais complexas à ordem pública, exige capacidade de resposta rápida, alocação precisa de especialistas e alto grau de prontidão. Apesar disso, grande parte dos departamentos de polícia e das secretarias de segurança, no Brasil e no exterior, ainda trabalha com rotinas administrativas antigas, muito burocratizadas e dependentes de processos manuais ou de planilhas que não se comunicam com os sistemas operacionais.

A separação entre as bases de dados de Recursos Humanos (RH), as folhas de pagamento, os sistemas de atendimento de emergência (Computer-Aided Dispatch, CAD) e os bancos de registros policiais (Records Management Systems, RMS) faz com que as cadeias de comando tenham pouca visibilidade sobre o próprio efetivo (NICE PUBLIC SAFETY, 2024; POLICE1 BRANDFOCUS, 2024). No dia a dia de batalhões e delegacias, quem monta a escala raramente sabe, de forma atualizada, quais agentes estão de fato disponíveis, quantas horas cada um trabalhou nos últimos dias, quantas folgas compensatórias acumulou ou quando vencem suas licenças e certificações. Esse descompasso entre a demanda das ruas e o planejamento do pessoal produz problemas operacionais e financeiros.

Do ponto de vista orçamentário, a dificuldade de prever e ajustar as escalas leva a uma alocação reativa do efetivo e ao uso frequente de horas extraordinárias ou de diárias operacionais (DHO). Além de elevar os gastos com pessoal, esse modelo distribui mal a carga de trabalho. É comum que operadores táticos essenciais estejam de folga ao mesmo tempo durante picos sazonais de criminalidade ou, ao contrário, que os mesmos agentes sejam convocados repetidamente para turnos dobrados, o que contribui para exaustão física, estresse crônico e casos de síndrome de burnout.

O problema se agrava na alocação de pessoal especializado em unidades de pronto emprego, como os Batalhões de Operações Especiais (BOPE/CHOQUE), os Gabinetes de Segurança Institucional e os Centros de Operações Integradas. Nessas unidades, mobilizar uma tropa diante de uma crise grave ou de uma catástrofe exige reunir, ao mesmo tempo, competências técnicas muito específicas. Em poucos minutos, o comando precisa formar equipes com atiradores de precisão (snipers), pilotos de aeronaves, condutores táticos, negociadores de crise, peritos em explosivos e operadores de tecnologias de menor potencial ofensivo, todos com certificação válida. Sem uma base centralizada e sem ferramentas capazes de cruzar automaticamente essas qualificações com as restrições legais de escala, a formação das equipes fica lenta, o que prejudica o gerenciamento da crise (PERRY et al., 2013).

Diante desse quadro, o uso de inteligência artificial generativa, computação em nuvem e ciência de dados na Governança Preditiva de Força de Trabalho (Workforce Governance) deixa de ser apenas uma modernização desejável e passa a ser uma necessidade institucional. O presente trabalho parte da seguinte pergunta de pesquisa: de que forma uma arquitetura em nuvem, integrada a modelos preditivos e de IA generativa, pode tornar proativa a gestão de efetivo em polícias e corporações militares, otimizando escalas, prevenindo a fadiga e assegurando prontidão operacional, sem descuidar dos limites éticos e legais?

2 REVISÃO DE LITERATURA

A literatura acadêmica e os relatórios de organismos multilaterais apontam o esgotamento dos modelos tradicionais de gestão de pessoal na segurança pública. Os sistemas convencionais de Recursos Humanos foram pensados para ambientes

industriais ou para burocracias relativamente estáveis e têm dificuldade em lidar com a variação, muitas vezes imprevisível, das demandas operacionais da área. Segundo relatório da Organização para a Cooperação e Desenvolvimento Econômico (OECD, 2025), o setor público ainda encontra obstáculos para ampliar o uso de tecnologias emergentes. O documento indica que cerca de metade das iniciativas de IA generativa e analítica em governos não passa da fase de prova de conceito (PoC) ou fracassa por causa da baixa qualidade dos dados, da permanência de silos entre setores e da falta de regras consolidadas de governança de dados.

Na gestão de escalas e de força de trabalho (Workforce Management, WFM), estudos realizados em centrais de controle policial e salas de atendimento de emergência (PSAP/911/190) mostram que a adoção de plataformas com recursos preditivos representa uma mudança importante em relação aos modelos anteriores (NICE PUBLIC SAFETY, 2024). Os sistemas tradicionais de escala (duty management) apenas registram os turnos já cumpridos, enquanto as soluções de WFM mais recentes aplicam métodos estatísticos a séries históricas para prever o volume de chamados e a gravidade das ocorrências. Modelos como o ARIMA de Box-Jenkins (AutoRegressive Integrated Moving Average), a suavização exponencial e a regressão multilinear sazonal permitem identificar padrões de demanda no tempo e no espaço, antecipar picos de incidência criminal e ajustar o tamanho do contingente à demanda observada (NICE PUBLIC SAFETY, 2024; POLICE1 BRANDFOCUS, 2024).

No Brasil, levantamento do Núcleo de Inteligência Artificial (NIA), vinculado à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (MGI), divulgado em conjunto com o Observatório Brasileiro de Inteligência Artificial (OBIA/NIC.br), traça um retrato da maturidade tecnológica do setor público (MENDES GAYA LOPES DOS SANTOS et al., 2026). Segundo o estudo, a adoção de ferramentas de IA chegou a 49% dos órgãos do Poder Executivo Federal pesquisados, índice superior ao do nível estadual (28%) e ao do setor empresarial (13%). Os principais obstáculos à expansão são a falta de profissionais com formação em ciência de dados e aprendizado de máquina, apontada por 170 órgãos, e a insuficiência de recursos orçamentários, citada por 187. O relatório menciona ainda iniciativas como o Projeto INSPIRE, com investimento previsto de R$ 390 milhões em quatro anos, voltado ao fortalecimento da infraestrutura pública de

dados, à interoperabilidade entre sistemas e à soberania digital (MENDES GAYA LOPES DOS SANTOS et al., 2026).

Na área de Ciência da Computação, trabalhos apresentados em eventos da Sociedade Brasileira de Computação (SBC) propõem modelos de governança adaptados ao setor público e às parcerias entre governo e universidades. Barcelar, Figueiredo e Ventura (2025) defendem que a implantação de soluções de IA na segurança pública deve se apoiar em quatro pilares: segurança da informação, gestão do ciclo de vida do modelo, propriedade intelectual e autonomia tecnológica, e conformidade legal. O modelo proposto pelos autores segue normas internacionais como a ISO/IEC 27001 (segurança da informação), a ISO/IEC 42001 (sistemas de gestão de inteligência artificial) e o NIST AI Risk Management Framework (AI RMF), de modo que a inovação não avance sem governança nem aumente a exposição das instituições a riscos cibernéticos.

A literatura jurídica e sociológica, por sua vez, alerta para os riscos do uso pouco cuidadoso de algoritmos preditivos pelas agências de aplicação da lei (Law Enforcement Agencies, LEAs). Trabalhos publicados no Minnesota Journal of Law & Inequality (SPITLER, 2026) e em outros fóruns (ROY; NEETU; SINGH, 2025; BRAYNE, 2020) mostram que sistemas alimentados por dados históricos marcados por vieses institucionais tendem a reproduzir e ampliar padrões de discriminação e de policiamento excessivo sobre comunidades vulneráveis. Ferguson (2017), ao tratar do policiamento orientado por grandes volumes de dados (big data policing), e as análises de O'Neil (2016) e Chouldechova (2017) reforçam que algoritmos opacos, tidos como neutros, podem transformar correlações estatísticas frágeis em justificativas automáticas para abordagens arbitrárias. Por isso, a Governança Preditiva da Força de Trabalho deve manter distância da vigilância invasiva e de previsões sobre o comportamento individual, concentrando-se na otimização logística e administrativa do pessoal do Estado, com transparência e possibilidade de auditoria dos algoritmos (SPITLER, 2026; PINTO, 2025).

3 ARQUITETURA PROPOSTA

A solução proposta se baseia em uma arquitetura nativa em nuvem (cloud-native), implantada em modelo SaaS/IaaS privado e de acordo com os requisitos de segurança cibernética aplicáveis ao governo (CJIS/SISP/ISO 27001). O

objetivo é integrar as bases operacionais e administrativas que hoje funcionam de forma isolada e transformar dados de escala e de pessoal em informação útil para a tomada de decisão em tempo real. A arquitetura se divide em três camadas interdependentes, descritas a seguir.

3.1 Camada de ingestão de dados e automação em nuvem

A primeira camada é responsável pela integração e padronização dos dados da instituição. Por meio de interfaces de programação (Application Programming Interface, API) seguras e criptografadas, ligadas a um barramento de integração governamental, a plataforma se conecta de forma contínua aos sistemas de atendimento de emergência (CAD), de registros policiais (RMS), prisionais e periciais (JMS/DEMS) e de folha de pagamento e frequência das secretarias de administração. Com esses dados, a camada mantém atualizado um repositório central em nuvem (data lake), organizado nas seguintes dimensões:

• **Disponibilidade em tempo real:** registro atualizado da situação de cada agente, com turnos em andamento, folgas usufruídas, férias programadas, afastamentos de saúde, licenças-prêmio e restrições médicas temporárias ou definitivas.

• **Matriz de qualificações e certificações táticas:** cadastro individual das qualificações técnicas e operacionais de cada agente. O sistema acompanha a validade de certificações como as de atirador de precisão, piloto de aeronaves tripuladas e remotamente pilotadas (RPAS/drones), condutor tático de veículos de emergência, negociador em ocorrências com reféns, perito em artefatos explosivos, operador de tecnologias não letais e atendimento a grupos vulneráveis.

• **Regras de negócio e restrições estatutárias:** inclusão das restrições legais que se aplicam à gestão da tropa, como os limites de jornada semanal e mensal, os intervalos mínimos de descanso entre turnos (por exemplo, 24x72h e 12x36h), o teto mensal de horas extras ou DHO por batalhão e os critérios de antiguidade previstos na legislação militar ou civil.

3.2 Camada de inteligência analítica e predição

A segunda camada concentra o processamento e o apoio à decisão. A partir dos dados reunidos na camada de ingestão, utiliza algoritmos de aprendizado de máquina (machine learning) supervisionado e não supervisionado, combinados com

IA generativa baseada em RAG (Retrieval-Augmented Generation). Suas principais funções são:

• **Previsão de lacunas no efetivo:** modelos de séries temporais (ARIMA e regressão multilinear sazonal) analisam o histórico de vários anos de absenteísmo, licenças médicas sazonais e aumento de chamados por região. Com isso, o sistema indica com semanas de antecedência quais batalhões ou delegacias terão falta de pessoal e sugere ajustes na escala com o menor custo possível.

• **Simulação de demandas sazonais e eventos críticos:** simulações de Monte Carlo testam cenários de grande porte, como o policiamento de grandes eventos, as operações de verão no litoral ou desastres socioambientais. O sistema estima a quantidade de policiais necessária e sugere a composição do contingente sem desfalcar o policiamento ordinário.

• **Alerta precoce de fadiga e estresse operacional:** o sistema acompanha a carga horária acumulada por agente, a quantidade de turnos noturnos seguidos e a exposição repetida a ocorrências de alto impacto emocional. Quando um policial ultrapassa os limites definidos, o comando recebe um alerta e uma sugestão de remanejamento temporário para funções menos desgastantes.

• **Assistente conversacional com IA generativa (RAG):** interface baseada em modelos de linguagem de grande porte (LLMs) instalados em ambiente corporativo isolado, com arquitetura RAG ligada às normas internas e ao banco de dados em nuvem. Comandantes e chefes de seção podem fazer consultas em linguagem natural (por exemplo: 'listar os atiradores de precisão disponíveis na Região Metropolitana no próximo sábado que ainda não atingiram o teto de horas extras') e recebem respostas com indicação das fontes e um relatório de conformidade.

3.3 Camada de interface e visualização para decisão

A terceira camada é a interface destinada aos responsáveis pelas decisões estratégicas, como comandantes-gerais, secretários de segurança pública e chefes de gabinete militar. No lugar de relatórios em papel ou de planilhas extensas, a interface apresenta painéis (dashboards) atualizados em tempo real e organizados em torno do Índice de Prontidão da Tropa (IPT).

O IPT é um indicador composto que busca medir, de forma objetiva, a capacidade de resposta de uma unidade ou de toda a corporação em determinado momento. Para uma especialidade ou batalhão, ele é calculado pela seguinte expressão:

$$IPT = (w_1 \cdot A) + (w_2 \cdot C) + (w_3 \cdot F) + (w_4 \cdot P)$$

Em que A é a razão de disponibilidade do efetivo (relação entre policiais ativos e previstos no quadro); C é a taxa de compatibilidade de certificações (percentual do efetivo escalado com certificação válida para a missão); F é o fator de higidez, inversamente proporcional ao nível de fadiga acumulada da tropa; e P é a proximidade logística em relação ao local da ocorrência. Os pesos w_1, w_2, w_3 e w_4 são definidos pela cadeia de comando conforme a natureza da missão.

O painel exibe mapas de calor do IPT por região e período, o que permite identificar rapidamente unidades com pouca cobertura ou com excesso de pessoal e redistribuir o efetivo de forma ágil, com verificação automática das regras de escala.

4 ESTUDO DE CASO SIMULADO

Para avaliar o efeito prático da arquitetura proposta, foi feita uma simulação quantitativa com dados sintéticos que reproduzem a rotina de um Batalhão de Operações Especiais e de um Gabinete de Segurança Institucional de uma grande cidade brasileira. O cenário hipotético envolve a decretação repentina de um Alerta de Segurança Nacional diante de duas crises simultâneas: a tentativa de invasão de um prédio público estratégico, com tomada de reféns, e uma ameaça à ordem pública que exigiu a formação imediata de um grupamento tático de contenção.

No cenário tradicional, com planilhas e contatos por telefone, a equipe de planejamento do batalhão levou cerca de 5 horas e 40 minutos para levantar os operadores habilitados, conferir em arquivos físicos a validade das certificações de tiro de precisão e de negociação e contatar os agentes de folga. Nesse processo manual ocorreram 14 violações dos intervalos mínimos de descanso, 3 agentes com certificação vencida foram incluídos na escala e o primeiro grupamento chegou ao local com atraso significativo. O custo projetado com horas extras ficou 45% acima do teto previsto.

No cenário com a plataforma em nuvem, o comando acionou o sistema pelo painel executivo. O algoritmo de alocação consultou o repositório central e, em 12

minutos, gerou a lista de convocação. Todos os operadores selecionados tinham as certificações exigidas (atiradores de precisão, negociadores e condutores táticos), os agentes com fadiga elevada ou sem o descanso legal mínimo foram excluídos e os convocados receberam notificação imediata por aplicativo corporativo. O IPT resultante foi de 98,2 pontos.

A Tabela 1 resume a comparação entre os indicadores obtidos nos dois cenários.

Tabela 1 – Comparativo de Desempenho Operacional: Gestão Legada vs. Governança Preditiva em Nuvem

Indicador Operacional e Administrativo	Cenário Legado (Planilhas / Manual)	Cenário Preditivo em Nuvem (IA Proposta)
Tempo de Mobilização de Tropas Especializadas	4 a 8 horas (validação manual e contatos verbais)	Menos de 15 minutos (verificação e disparo em nuvem)
Índice de Retrabalho Burocrático em Escalas	Elevado (35% do tempo da seção de pessoal em ajustes)	Redução estimada acima de 80%, sem conflitos de agenda
Violação de Restrições Legais de Descanso / Fadiga	Frequentes (12% a 18% da escala com sobreposição indevida)	Zero violações (filtragem algorítmica automatizada)
Acurácia do Índice de Prontidão da Tropa (IPT)	Aproximada e desatualizada (defasagem de 24h a 48h)	Precisão em tempo real (atualização a cada evento do CAD/RMS)

Fonte: Dados gerados pela simulação do modelo conceitual (2026).

5 ASPECTOS ÉTICOS E LEGAIS

O uso de inteligência artificial e de processamento preditivo em corporações policiais e órgãos de segurança não pode ser avaliado apenas pelo ganho de eficiência. Por se tratar de exercício do poder estatal em área sensível, ele deve respeitar os direitos fundamentais, os princípios da administração pública (art. 37 da Constituição Federal) e as normas de tecnologia e de proteção de dados em vigor ou em discussão.

5.1 O Projeto de Lei nº 2.338/2023 e a Avaliação de Impacto Algorítmico

A discussão sobre a regulação da inteligência artificial no Brasil gira em torno do Projeto de Lei nº 2.338/2023, em tramitação no Congresso Nacional. Inspirado no

regulamento europeu (EU AI Act), o projeto adota uma abordagem baseada em risco e estabelece regras específicas para o uso de sistemas algorítmicos pelo Poder Público (PINTO, 2025). O texto classifica como de 'risco excessivo' o uso de sistemas de identificação biométrica à distância, em tempo real, em espaços públicos (art. 13, IV), proibindo-o salvo em hipóteses restritas ligadas à segurança pública, como a busca de pessoas desaparecidas e a recaptura de foragidos.

O modelo de gestão da força de trabalho aqui proposto, porém, tem natureza diferente. Ao contrário dos sistemas de vigilância biométrica voltados à população, a plataforma atua apenas na administração interna do pessoal do Estado. Mesmo assim, como trata dados sensíveis de agentes públicos e automatiza decisões que afetam direitos funcionais, ela tende a ser enquadrada como sistema de 'alto risco', sujeito às exigências dos arts. 23 e 25 do PL 2.338/2023 (PINTO, 2025).

Assim, a Avaliação de Impacto Algorítmico (AIA) passa a ser uma obrigação do gestor público antes da implantação da ferramenta. A AIA exige documentar previamente a metodologia, identificar os riscos de viés na distribuição de escalas e promoções e descrever as medidas de mitigação adotadas. Merece destaque o art. 23, § 2º, do projeto: se os riscos apontados na AIA, como vieses discriminatórios persistentes, não puderem ser eliminados ou reduzidos de forma substancial, a autoridade pública deve interromper o uso do sistema (PINTO, 2025).

5.2 Proteção de dados pessoais dos agentes (LGPD) e prevenção de vieses

Reunir dados funcionais, de saúde física e mental e de qualificação dos agentes em um repositório em nuvem exige observância da Lei Geral de Proteção de Dados Pessoais (LGPD, Lei nº 13.709/2018). O art. 4º, III, 'a', da LGPD afasta sua aplicação ao tratamento de dados realizado exclusivamente para fins de segurança pública e defesa nacional. Ainda assim, a jurisprudência do Supremo Tribunal Federal (STF) e as orientações da Autoridade Nacional de Proteção de Dados (ANPD) reconhecem que garantias como a autodeterminação informativa, a segurança e a minimização do uso de dados continuam valendo para os servidores públicos.

Para atender à LGPD, a arquitetura prevê controle de acesso baseado em papéis (Role-Based Access Control, RBAC), criptografia dos dados em trânsito e em repouso e anonimização dos registros de saúde física e psicológica na camada analítica. Somente médicos e psicólogos da corporação têm acesso aos

diagnósticos individuais; o algoritmo recebe apenas a informação de aptidão ou inaptidão para o serviço.

A mitigação de vieses discriminatórios no aprendizado de máquina também é uma preocupação central. Algoritmos treinados com históricos de escalas que reflitam práticas inadequadas, como a atribuição sistemática de turnos noturnos como punição ou a preterição de determinados agentes em cursos de especialização, tendem a repetir essas distorções (SPITLER, 2026; ROY; NEETU; SINGH, 2025). Por isso, a arquitetura prevê auditorias periódicas dos algoritmos, testes contínuos de equidade (fairness testing) e supervisão humana efetiva (human-in-the-loop), além de garantir aos agentes o direito à explicação e ao contraditório administrativo contra decisões automatizadas de escala que afetem seus direitos funcionais.

5.3 Normas internacionais de governança (ISO/IEC 42001 e NIST AI RMF)

Para dar consistência técnica e permitir auditoria, a arquitetura segue as diretrizes da ISO/IEC 42001 (sistema de gestão de inteligência artificial) e o NIST AI Risk Management Framework (NIST AI RMF), como recomendam a literatura especializada e organismos internacionais (BARCELAR; FIGUEIREDO; VENTURA, 2025; OECD, 2025). Essas normas permitem rastrear todo o ciclo de vida dos modelos preditivos, proteger o sistema contra ataques específicos, como o envenenamento de dados (data poisoning) e a injeção de instruções (prompt injection) em modelos RAG, e alinhar o projeto aos objetivos de soberania digital do Plano Brasileiro de Inteligência Artificial (PBIA).

6 CONSIDERAÇÕES FINAIS

A substituição de um modelo de gestão de efetivo fragmentado, reativo e baseado em planilhas por uma estrutura de Governança Preditiva de Força de Trabalho apoiada em inteligência artificial e computação em nuvem representa um avanço importante para as corporações policiais e os órgãos de segurança no Brasil.

A arquitetura em três camadas apresentada neste trabalho indica que é possível aumentar a eficiência operacional, com redução estimada de mais de 80% no retrabalho burocrático, mobilização mais rápida em emergências e menor uso de horas extras, sem abrir mão da saúde física e mental dos operadores e das

garantias éticas e legais. Como esses resultados vêm de uma simulação com dados sintéticos, eles ainda precisam ser confirmados em testes com dados reais.

Para secretarias de segurança, comandos militares e departamentos de polícia que pretendam adotar esse modelo, recomenda-se:

• **Criação de comitês multidisciplinares de governança de dados e IA:** formar grupos com gestores operacionais, cientistas de dados, juristas e representantes dos agentes para elaborar os planos de gestão de dados e conduzir as Avaliações de Impacto Algorítmico (AIA).

• **Implantação gradual, com projetos-piloto:** testar o modelo primeiro em unidades menores e estratégicas, como Batalhões de Operações Especiais ou centrais de atendimento de emergência, antes de estendê-lo a toda a corporação.

• **Capacitação contínua em letramento digital e ética algorítmica:** preparar comandantes e chefes de seção para o uso adequado das ferramentas analíticas, deixando claro que a decisão final continua sendo humana.

• **Soberania digital e padrões abertos:** dar preferência a soluções baseadas em padrões abertos e arquiteturas auditáveis, que mantenham os dados sob custódia do poder público e evitem a dependência de um único fornecedor (vendor lock-in).

REFERÊNCIAS

BARCELAR, Ricardo Rodrigues; FIGUEIREDO, Josiel Maimone de; VENTURA, Thiago Meirelles. **Modelo Analítico de Governança da Inovação Colaborativa em Inteligência Artificial Aplicada à Segurança Pública**. In: ESCOLA REGIONAL DE INFORMÁTICA DE MATO GROSSO (ERI-MT), 14., 2025, Pontes e Lacerda. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2025. p. 20-29.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018.

BRASIL. **Projeto de Lei nº 2.338, de 2023**. Dispõe sobre o uso da Inteligência Artificial no Brasil. Brasília: Senado Federal, 2023.

BRAYNE, Sarah. **Predict and Surveil: Data, Discretion, and the Future of Policing**. New York: Oxford University Press, 2020.

CHOULDECHOVA, Alexandra. **Fair prediction with disparate impact: A study of bias in recidivism prediction instruments**. Big Data, v. 5, n. 2, p. 153-163, 2017.

FERGUSON, Andrew Guthrie. **The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement**. New York: New York University Press, 2017.

MENDES GAYA LOPES DOS SANTOS, Renan et al. **Governança de dados na era da Inteligência Artificial. Relatório Panorama Setorial da Internet**. São Paulo: Núcleo de Informação e Coordenação do Ponto BR (NIC.br) / Observatório Brasileiro de Inteligência Artificial (OBIA), 2026.

NICE PUBLIC SAFETY. **How Police Control Rooms are Mastering Staff Scheduling with AI-Powered Workforce Management**. NiCE Public Safety & Justice, 2024.

OECD. **Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions**. Paris: OECD Publishing, 2025.

O'NEIL, Cathy. **Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy**. New York: Crown Publishing Group, 2016.

PERRY, Walter L. et al. **Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations**. Santa Monica: RAND Corporation, 2013.

PINTO, Manoel Duarte. **IA na segurança pública: Entre a eficácia operacional e o novo paradigma regulatório**. Portal Migalhas, 18 dez. 2025.

POLICE1 BRANDFOCUS. **Smart solutions for short-staffed departments: Predictive analytics in law enforcement**. Police1, 7 mar. 2024.

ROY, Apoorva; NEETU, Neetu; SINGH, Ajay Raj. **The Role of Artificial Intelligence in Predictive Policing and Its Legal Implications. In: NATIONAL SEMINAR ON ENHANCING PRIVACY PROTECTION IN THE DIGITAL AGE, 2025**. Advances in Social Science [...]. Atlantis Press, 2025. p. 95-113.

SPITLER, Aaron. **Fighting Pre-Crime?: Law Enforcement, Artificial Intelligence, and Predictive Policing Technology**. Minnesota Journal of Law & Inequality, v. 44, 27 jan. 2026.