Modelo Analítico de Governança da Inovação Colaborativa em Inteligência Artificial Aplicada à Segurança Pública

Ricardo Rodrigues Barcelar[1], **Josiel Maimone de Figueiredo**[1], **Thiago Meirelles Ventura**[1]

[1]Instituto de Computação – Universidade Federal de Mato Grosso (UFMT)
CEP 78060-900 – Cuiabá – MT – Brasil

ricardo.barcelar@sou.ufmt.br, {josiel, thiago}@ic.ufmt.br,

alvaro.junior1@ufmt.br

Abstract. *This article proposes an analytical governance model to guide the collaborative development of Artificial Intelligence solutions in public security through public-academic partnerships. The research, qualitative in nature, is based on a literature review and documentary analysis of standards such as ISO/IEC 27001, ISO/IEC 42001, and the NIST AI RMF, in addition to Brazilian legislation on innovation and intellectual property. The model is structured on a risk management foundation and four pillars: information security, AI lifecycle management, intellectual property, and legal compliance. The proposal seeks to align technological innovation with transparency, responsible governance, and technological autonomy.*

Resumo. *Este artigo propõe um modelo analítico de governança para orientar o desenvolvimento colaborativo de soluções de Inteligência Artificial na segurança pública em parcerias público-acadêmicas. A pesquisa, de natureza qualitativa, fundamenta-se em revisão bibliográfica e análise documental de normas como ISO/IEC 27001, ISO/IEC 42001 e o NIST AI RMF, além da legislação brasileira de inovação e propriedade intelectual. O modelo estrutura-se em uma base de gestão de riscos e quatro pilares: segurança da informação, gestão do ciclo de vida da IA, propriedade intelectual e conformidade legal. A proposta busca alinhar a inovação tecnológica à transparência, à governança responsável e à autonomia tecnológica.*

1. Introdução

O setor público, em especial a área de segurança, enfrenta uma contínua pressão por modernização e eficiência. Nesse cenário, a inovação de processo surge como um caminho estratégico para a otimização dos serviços estatais frequentemente apoiados por tecnologias digitais [OECD/Eurostat 2018].

A Inteligência Artificial (IA), especialmente em sua forma generativa, surge como uma ferramenta capaz de impulsionar essa inovação através da automatização de rotinas administrativas, do atendimento ao cidadão e, consequentemente, liberando os agentes públicos para as atividades que demandam interação humana e julgamento complexo.

Resultados de pesquisas anteriores sobre a implementação de IA na segurança pública destacam os riscos associados à aquisição de tecnologias desenvolvidas pelo setor privado. A literatura analisa os desafios da opacidade algorítmica, também conhecidas

na engenharia de software como ”caixas-pretas”, os vieses discriminatórios embutidos nos dados de treinamento e enfatiza a necessidade de transparência, responsabilidade e diretrizes éticas no uso dessas tecnologias [Vivian et al. 2024]. Em outra perspectiva, estudos demonstram um aumento na proteção da propriedade intelectual (PI) em relação às aplicações de IA, incluindo produtos voltados ao setor da segurança pública [Ning 2024].

Diante das limitações impostas pela dependência de tecnologias externas e do frequente desalinhamento com as necessidades públicas, parcerias público-acadêmicas (PPAs) são instrumentos capazes de fomentar a autonomia tecnológica do Estado e assegurar que a IA seja concebida de forma responsável e com respeito às normas legais.

Nesse sentido, tem-se a premissa de que o modelo de parceria proposto pode aprimorar o desenvolvimento de soluções de IA no setor público ao integrar inovação, cooperação estratégica e controle sobre o processo. Normas como as séries ISO 27001 e ISO 42001 e frameworks como o NIST AI RMF, oferecem parâmetros para uma governança auditável e ética. Nesse contexto, a propriedade intelectual em ambientes colaborativos é compreendida como um mecanismo estratégico para proteger e, ao mesmo tempo, difundir soluções tecnológicas voltadas ao interesse do poder público.

Considerando que a literatura ainda aborda de forma limitada modelos de governança que articulem segurança pública, academia e inovação tecnológica, este estudo busca responder à questão de como estruturar um modelo capaz de orientar a inovação em segurança pública com base em parcerias público-acadêmicas. O objetivo central é propor um modelo analítico que direcione o desenvolvimento colaborativo de soluções de IA, contemplando gestão de riscos, governança técnica, conformidade legal e estratégias de propriedade intelectual orientadas ao bem público.

2. Referencial Teórico

A inovação em segurança pública demanda não apenas novas tecnologias, mas também novos métodos de organização e aplicação prática. Segundo o Manual de Oslo, a inovação de processo envolve a adoção de formas novas ou substancialmente otimizadas de organizar a produção ou a distribuição [OECD/Eurostat 2018]. No setor público, essa transformação deve ser orientada por princípios de geração de benefícios à sociedade, responsabilidade e legalidade, indo além busca por eficiência [Ramírez-Alujas 2011].

Nesse contexto, a Inteligência Artificial (IA) surge como um instrumento com grande potencial, mas sua implementação bem-sucedida depende de um modelo de governança baseado na gestão de riscos, segurança e aderência à normas legais.

A literatura sobre inovação pública tem progressivamente se aproximado de abordagens colaborativas. A inovação colaborativa é o método mais eficaz para resolver problemas complexos e envolve a colaboração entre atores públicos, privados e a sociedade civil [Sorensen and Torfing 2016]. Diferentemente de modelos tradicionais, a colaboração promove a apropriação conjunta das soluções e, consequentemente, gera resultados mais robustos e sustentáveis.

A parceria público-acadêmica, discutida neste artigo, é a materialização desse modelo, configurando-se como um arranjo institucional que explora a coprodução como um mecanismo essencial para a inovação pública efetiva [Baretta et al. 2024]. Embora promissora, a operacionalização da inovação colaborativa em projetos de IA impõe de-

safios de governança, que podem ser agrupados em duas dimensões principais e interdependentes: a técnico-gerencial e a jurídico-estratégica.

A primeira dimensão refere-se à necessidade de um arcabouço robusto para gerenciar a tecnologia em si. A governança de IA evoluiu de um debate sobre princípios éticos abstratos [Sistla 2024] para a implementação de sistemas de gestão auditáveis. A abordagem baseada em risco, definida em frameworks como o NIST AI RMF, defende que o nível de governança deve acompanhar a relevância e o impacto da aplicação [Trisnawati 2024]. Para operacionalizar essa gestão, normas como a ISO/IEC 27001 e a ISO/IEC 42001 fornecem a estrutura técnica e processual para assegurar a segurança dos dados e a rastreabilidade do ciclo de vida da IA, transformando intenções em práticas organizacionais auditáveis [Ashraf and Mustafa 2024, Almeida et al. 2020].

A segunda dimensão desponta-se quando a colaboração substitui a aquisição. O problema deixa de ser a auditoria de ”caixas-pretas” de fornecedores privados [Vivian et al. 2024] e passa a ser a governança de um ativo co-criado. Nesta nova perspectiva, a Propriedade Intelectual (PI) torna-se um aspecto muito relevante. Com a ascensão da IA generativa, os regimes tradicionais de PI são desafiados, demandando arranjos contratuais inovadores para definir titularidade e direitos de uso [Silva et al. 2025]. A PI deixa de ser uma barreira e torna-se uma ferramenta de política pública, cujo desenho determinará se a inovação será um ativo restrito ou um bem público replicável.

Ainda sobre à dimensão jurídico-estratégica, o licenciamento em ambientes colaborativos fornecem as bases para um modelo de licenciamento que equilibre proteção, uso e difusão da tecnologia [Bogers et al. 2013]. Em vez de licenças restritivas ou totalmente abertas, modelos adaptáveis ou duais são frequentemente necessários para conciliar os diferentes interesses dos parceiros. Essa análise justificaria a proposta de uma política de licenciamento dual, capaz de equilibrar o interesse público de ampla reutilização da tecnologia pelo Estado com o potencial de exploração comercial por meio de spin-offs universitárias, garantindo a sustentabilidade e o reinvestimento na parceria.

Outras pesquisas sobre inovação e colaboração no setor público demonstram que o sucesso de parcerias depende de fatores como a clareza de papéis, o compartilhamento de metas e a existência de mecanismos de governança estruturada [Gil-García et al. 2019]. Todas essas condições podem ser consolidadas para orientar a inovação na segurança pública, mediante o uso de Inteligência Artificial em parcerias público-acadêmicas.

3. Metodologia

A pesquisa adota uma abordagem qualitativa, voltada à análise conceitual e teórica, sem uso de mensurações numéricas. O objetivo é exploratório e propositivo, buscando articular conhecimentos de Governança de IA, Gestão da Inovação, Segurança da Informação, Propriedade Intelectual e legislação, com foco na criação de um modelo analítico de governança. O estudo investiga a interface entre sistemas de gestão de IA (como a ISO/IEC 42001) e estratégias de PI em parcerias público-acadêmicas.

Os procedimentos técnicos baseiam-se em pesquisa bibliográfica e documental: a primeira sustenta o referencial teórico e a identificação de lacunas; a segunda permite examinar normas e frameworks que fundamentam o modelo. A construção do modelo analítico ocorreu em três etapas sequenciais e integradas, descritas a seguir.

3.1. Delimitação do Estudo

Embora os princípios gerais de inovação e governança de IA possam ser amplamente aplicados, este trabalho delimita seu escopo à proposição de um modelo para parcerias público-acadêmicas entre universidades e órgãos de segurança pública.

Tal escolha fundamenta-se nas particularidades da proposta apresentada, pois diferentemente de parcerias com o setor privado, as parcerias público-acadêmicas operam sob um alinhamento de interesses focado na geração de valor público e conhecimento científico e não apenas no lucro. Mais importante, são regidas por um arcabouço jurídico específico, entre eles, o Marco Legal de Ciência, Tecnologia e Inovação, que estabelece regras próprias para a colaboração e para a gestão da propriedade intelectual. Portanto, o modelo proposto ao final foi desenhado para ser aderente a este contexto.

3.2. Levantamento e Análise Bibliográfica

A fundamentação teórica deste artigo foi construída a partir de uma revisão da literatura focada nos eixos centrais da pesquisa. Utilizou-se primariamente a base de dados Google Scholar para identificar os trabalhos mais influentes e recentes sobre governança de IA, inovação colaborativa no setor público e os desafios da propriedade intelectual em tecnologia. A seleção das fontes priorizou artigos publicados em periódicos com revisão por pares, anais de conferências e obras de referência consolidadas.

3.3. Análise Documental

A segunda etapa envolveu uma análise documental dos seguintes documentos:

- ISO/IEC 42001:2023 (Tecnologia da Informação, Inteligência Artificial, Sistema de Gestão);
- ISO/IEC 27001:2022 (Segurança da Informação, Cibersegurança e Proteção da Privacidade; Sistemas de Gestão da Segurança da Informação);
- NIST AI Risk Management Framework (AI RMF 1.0);
- Lei do Software (Lei nº 9.609/98);
- Lei de Direitos Autorais (Lei nº 9.610/98);
- Lei da Propriedade Industrial (Lei nº 9.279/96);
- Marco Legal de Ciência, Tecnologia e Inovação (Lei nº 13.243/16);

Para a análise destes documentos foi realizada uma análise de conteúdo temática, buscando extrair conceitos, princípios, processos e controles que poderiam ser aplicados aos desafios de uma parceria público-acadêmica. O foco foi identificar elementos básicos para a governança, como os requisitos para análise de impacto, gestão do ciclo de vida do sistema de IA, definição de papéis e responsabilidades, e tratamento de riscos.

3.4. Síntese e Construção do Modelo

A terceira etapa consistiu na consolidação das informações coletadas de diversas fontes, com o objetivo de construir um modelo analítico de governança. Os desafios e lacunas identificados na revisão da literatura forneceram os requisitos que o modelo deve atender, estabelecendo sua base conceitual.

Paralelamente, a análise documental permitiu extrair os processos e controles que compõem a estrutura operacional do modelo, enquanto a literatura sobre propriedade intelectual e inovação colaborativa definiu o pilar dedicado às estratégias de licenciamento e difusão. Além disso, foram consideradas as exigências e oportunidades presentes na legislação brasileira, reforçando a aplicabilidade do modelo no contexto nacional.

4. Resultados e Discussões

Esta seção apresenta o modelo analítico proposto e discute suas implicações teóricas e práticas.

4.1. Modelo Analítico de Governança (MAG)

O modelo visa oferecer uma estrutura que permita o desenvolvimento conjunto de soluções que apliquem inteligência artificial, respeitando diretrizes éticas, legais e técnicas. A proposta está estruturada sobre uma base fundacional de gestão de riscos e sustentado por quatro pilares interdependentes, conforme ilustrado na Figura 1.

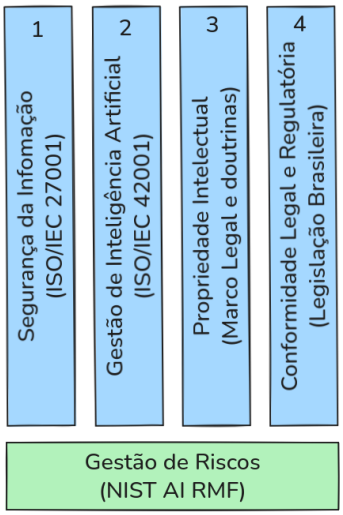

Figure 1. Esquematização do MAG

Complementarmente à arquitetura visual apresentada, a descrição do modelo especifica cada componente, pormenorizando referências, objetivos, atores, artefatos entregáveis e resultados esperados de cada pilar.

Base Fundacional: Gestão de Riscos

- Referência: NIST AI RMF
- Objetivo: Mapear e mitigar riscos associados ao uso de IA em operações de segurança pública.
- Atores Envolvidos: Comitê Gestor da Parceria (Secretaria de Segurança, universidades), analistas de risco, setor de TI das forças de segurança.
- Entregáveis: Matriz de risco para IA em segurança; plano de mitigação de vieses; diretrizes de uso responsável.
- Resultados Esperados: Redução de falhas críticas; conformidade ética; maior confiabilidade institucional das tecnologias aplicadas.

Pilar 1: Segurança da Informação

- Referência: ISO/IEC 27001:2023
- Objetivo: Proteger dados sensíveis como dados de ocorrências, imagens, registros biográficos, entre outros usados em sistemas de IA, além da infraestrutura de execução das soluções;

- Atores Envolvidos: DPO da Secretaria de Segurança; Gestores de Infraestrutura; Gestor de Dados das forças de segurança; Coordenadores do projeto (Secretaria de Segurança e Universidade);
- Entregáveis: Política de segurança da informação adaptada à segurança pública; Acordos interinstitucionais de dados; Relatório de Impacto à Proteção de Dados Pessoais para sistemas policiais.
- Resultados Esperados: Segurança da infraestrutura de execução; prevenção de uso de dados indevidos; conformidade com LGPD; aumento da confiança pública em soluções tecnológicas policiais.

Pilar 2: Gestão do Sistema de IA

- Referência: ISO/IEC 42001:2023
- Objetivo: Garantir governança do ciclo de vida de soluções de IA aplicadas à segurança.
- Atores Envolvidos: Comitê de Governança de IA (misto), equipes técnicas das forças de segurança, universidades parceiras.
- Entregáveis: Política de IA para segurança; Política de Curadoria e Tratamento de Dados para Mitigação de Viés; Avaliação de impacto; Documentação e auditoria de modelos aplicados a decisões operacionais.
- Resultados Esperados: Rastreabilidade e auditabilidade das decisões; governança ativa do ciclo de vida do modelo; processos formais de validação e monitoramento.

Pilar 3: Propriedade Intelectual

- Referência: Marco Legal de CTI, Silva et al. (2025), Bogers et al. (2013)
- Objetivo: Definir titularidade e uso de tecnologias de IA desenvolvidas em parcerias, como sistemas de classificação, análise criminal, reconhecimento facial, entre outros.
- Atores Envolvidos: NITs universitários; assessorias jurídicas das Secretarias de Segurança Pública; Procuradorias-Gerais.
- Entregáveis: Cláusulas de PI em acordos de parceria; contratos de uso público e comercial de tecnologias desenvolvidas.
- Resultados Esperados: Reutilização pública das soluções; fomento à inovação em segurança; segurança jurídica nas transferências de tecnologia.

Pilar 4: Conformidade Legal e Regulatória

- Referência: LGPD, Lei do Software, Marco Legal da Inovação;
- Objetivo: Assegurar que o uso de IA em segurança pública esteja em conformidade com direitos fundamentais e normas brasileiras.
- Atores Envolvidos: Comitês de ética; DPOs; assessorias jurídicas das secretarias e universidades.
- Entregáveis: Pareceres jurídicos sobre uso de IA; Pareceres de conformidade; políticas de responsabilização civil; termos de uso em plataformas públicas.
- Resultados Esperados: Redução de riscos legais; legitimação institucional; respeito à privacidade e aos direitos civis nas operações com IA.

A operacionalização do MAG, conforme ilustra a Figura 2, inicia-se com a Estruturação da Governança e Acordos Jurídicos. Nela, os Pilares 1 (Segurança da Informação), 3 (Propriedade Intelectual) e 4 (Conformidade Legal) atuam de forma integrada para produzir os documentos fundacionais que formalizam a parceria. Embora o Acordo de Parceria seja o instrumento central, ele é sustentado por um conjunto de artefatos, como os pareceres de conformidade, as cláusulas de PI, entre outros documentos que juntos garantem a segurança jurídica e informacional da colaboração.

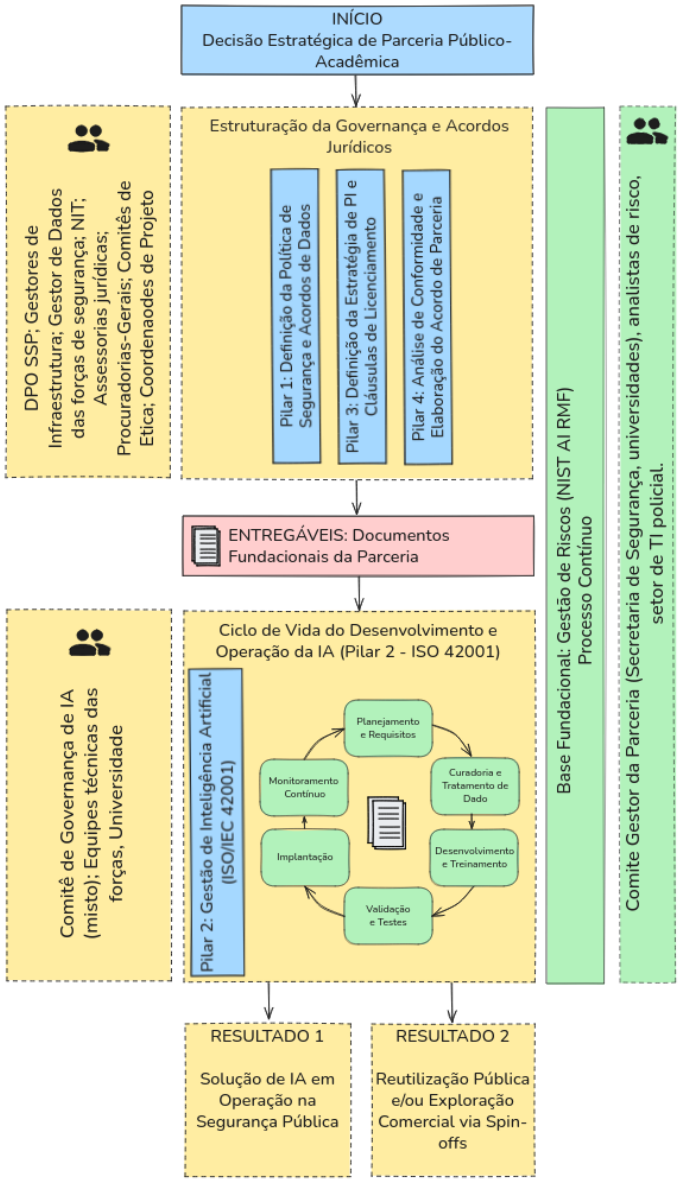

Figure 2. Fluxo de Operacionalização do MAG

Uma vez que esta base de governança está estabelecida, o processo avança para o Ciclo de Vida do Sistema de IA, governado pelo Pilar 2. Esta etapa não possui um único entregável, mas artefatos de governança como a Política de Curadoria de Dados, as avaliações de impacto e a documentação e auditoria do modelo. Esses documentos são produzidos ao longo das fases de desenvolvimento, validação e monitoramento, assegurando a rastreabilidade e a gestão responsável da tecnologia.

Todo o processo é supervisionado pela Gestão de Riscos. Finalmente, com a solução em operação, os resultados estratégicos do Pilar 3 são ativados, completando o ciclo de geração de valor público.

4.2. Discussão

O modelo proposto oferece uma arquitetura de governança que, ao materializar a inovação colaborativa na segurança pública, substitui a abordagem convencional de aquisição de tecnologia. Conforme aponta a teoria de Torfing (2016), a colaboração entre atores distintos é o método mais eficaz para gerar inovações legítimas e sustentáveis. O MAG serve como uma estrutura institucional para essa colaboração, transformando a parceria de uma mera declaração de intenções em um processo gerenciável.

Isso dialoga diretamente com os achados de Gil-García et al. 2019, que identificam a clareza de papéis e a governança estruturada como determinantes do sucesso em parcerias públicas. O modelo proposto responde a essa necessidade ao utilizar as normas ISO 27001 e 42001 (Pilares 1 e 2) não apenas como checklists técnicos, mas como frameworks que forçam a definição de processos, responsabilidades, envolvendo atores essenciais de ambas as instituições como o DPO e coordenadores do projeto (Pilar 1) para elaborar o Relatório de Impacto à Proteção de Dados e um Comitê gestor misto (Pilar 2) para definir a Política de Curadoria de Dados e Mitigação de Viés. Ao fazer isso, o modelo supera o paradigma da 'caixa-preta', onde os processos internos da tecnologia são opacos e inacessíveis [Vivian et al. 2024], por uma abordagem na qual a transparência se torna um atributo intrínseco ao desenvolvimento em coprodução [Baretta et al. 2024].

No contexto da segurança pública, o pilar de segurança da informação (ISO 27001) ganha especial relevância em projetos que envolvem o tratamento de dados sensíveis, aliado a preocupação com a proteção do ambiente de execução dos sistemas.

No tocante a gestão de riscos, o modelo parte da premissa de que a governança de IA vai além da ética baseada em princípios, exigindo mecanismos de operacionalização [Sistla 2024]. A Base Fundacional (NIST AI RMF) e o Pilar 2 (ISO 42001) funcionam como um mecanismo que converte princípios em práticas auditáveis, como a avaliação de impacto e a mitigação de vieses. É a formalização desses processos e a geração de artefatos, como a Política de Curadoria de Dados e os logs de auditoria, que justificam o resultado esperado de rastreabilidade e auditabilidade.

A inclusão do Pilar 4 (Conformidade Legal e Regulatória) expande a noção de risco para além da perspectiva técnica, abrangendo a responsabilidade civil, a conformidade com a LGPD e a aderência aos marcos legais de inovação. Essa conformidade é operacionalizada pela atuação das assessorias jurídicas, que produzem pareceres de legalidade e políticas de responsabilização para garantir que o resultado esperado de confiança institucional seja construído sobre uma base juridicamente segura. Em soluções aplicadas à segurança pública, como aplicações de classificação de ocorrências e reconhecimento de padrões criminais, a confiança institucional torna-se ainda mais crítica, exigindo mecanismos robustos de responsabilização, explicabilidade e controle.

Quanto à gestão da propriedade intelectual, o modelo propõe tratá-la como um instrumento de política de inovação que busca responder a desafios, como aqueles relacionados a IA generativa, que suscita questionamentos sobre os regimes tradicionais de titularidade de dados de treinamento, modelos e resultados. Diante disso, o modelo sug-

ere arranjos de licenciamento inovadores, entendidos aqui como modelos adaptáveis, como o licenciamento dual, capazes de assegurar a gestão clara e segura dos direitos de uso ao definir contratualmente as permissões que a legislação atual deixa em aberto [Silva et al. 2025].

A fundamentação teórica para esta abordagem encontra-se diretamente na análise de Bogers et al. (2013) sobre a importância de licenças flexíveis para o sucesso de parcerias de inovação. O estudo sustenta a adoção da política de licenciamento dual (Pilar 3) como uma estratégia para gerenciar a propriedade intelectual em contextos colaborativos, cuja negociação, envolvendo o Núcleo de Inovação Tecnológica (NIT) da universidade e a Procuradoria-Geral do Estado, é formalizada através das cláusulas de PI nos acordos de parceria.

Tal política resolve o impasse inerente à parceria ao separar a titularidade da tecnologia das licenças de uso. Por um lado, o Estado recebe uma licença governamental não exclusiva, garantindo seu direito irrestrito de uso e modificação de forma a maximizar o valor público, como preconiza Ramírez-Alujas (2011). Por outro lado, ao reter a titularidade da propriedade intelectual, a universidade mantém a prerrogativa de oferecer licenças comerciais a terceiros, como spin-offs, viabilizando a exploração comercial e criando um ciclo virtuoso de reinvestimento.

Assim, o MAG não apenas governa a criação da tecnologia, mas sua socialização e sustentabilidade, assegurando que o conhecimento gerado com recursos públicos cumpra sua função social e fomente o ecossistema de inovação. Essa estrutura de licenciamento, formalizada nas cláusulas de PI é o que garante a segurança jurídica, enquanto a licença governamental não exclusiva assegura a reutilização pública e a possibilidade de licenciamento comercial viabiliza o fomento à inovação e ao reinvestimento.

5. Considerações Finais

Embora o Modelo Analítico de Governança apresente uma proposta estruturada e alinhada às melhores práticas internacionais, sua aplicação ainda não foi testada em estudos de caso concretos. Além disso, a adoção plena das normas técnicas sugeridas pode depender do nível de maturidade institucional e dos recursos disponíveis na administração da segurança pública.

Pesquisas futuras podem explorar a implementação prática do modelo em parcerias reais, de modo a avaliar sua efetividade. Sugere-se o desenvolvimento de estudos de caso que demonstrem a aplicação dos artefatos (como a Matriz de Risco e as Cláusulas de PI) em cenários específicos, bem como a definição de roteiros de adaptação com um MAG mínimo para organizações com menor maturidade técnica. Por fim, outros trabalhos podem aprofundar as metodologias de curadoria de dados (Pilar 2), detalhando o uso do conhecimento acadêmico na mitigação ativa de vieses em dados policiais sensíveis, indo além do compliance formal das normas.

Em um campo tão sensível quanto a segurança pública, o uso de IA requer uma governança rigorosa para controlar riscos como vieses discriminatórios e violações à privacidade. O MAG é, portanto, proposto como uma estrutura orientada por valores públicos que oferece essa base de controle colaborativa e juridicamente segura. Ao integrar normas técnicas, princípios legais e arranjos institucionais de coprodução, o modelo

articula a segurança técnica, jurídica e estratégica, visando ampliar a legitimidade e a eficácia das inovações em IA.

Ao promover parcerias público-acadêmicas ancoradas em governança transparente, o modelo contribui para a autonomia tecnológica da segurança pública e para a disseminação de soluções éticas, auditáveis e orientadas ao interesse coletivo.

References

Almeida, P., Santos Jr, C., and Farias, J. (2020). Artificial intelligence regulation: A meta-framework for formulation and governance.

Ashraf, Z. and Mustafa, N. (2024). *AI Standards and Regulations*, pages 325–352.

Baretta, J. V., Hoffmann, M. G., Militao, L., and Farias, J. S. (2024). Coproduction, public sector innovation and governance: a systematic literature review. *International Journal of Innovation Science*, 17(3):500–522.

Bogers, M., Bekkers, R., and Granstrand, O. (2013). Intellectual property and licensing strategies in open collaborative innovation. In Information Resources Management Association, editor, *Digital Rights Management: Concepts, Methodologies, Tools, and Applications*, pages 1204–1224. IGI Global Scientific Publishing, Hershey, PA.

Gil-García, J. R., Guler, A., Pardo, T. A., and Burke, G. B. (2019). Characterizing the importance of clarity of roles and responsibilities in government inter-organizational collaboration and information sharing initiatives. *Government Information Quarterly*, 36(3):101393.

Ning, W. (2024). A legal and ethical review of artificial intelligence technology in public safety management. *Applied Mathematics and Nonlinear Sciences*, 9(1):1–16.

OECD/Eurostat (2018). *Oslo Manual 2018: Guidelines for Collecting, Reporting and Using Data on Innovation*. OECD Publishing/Eurostat, Paris/Luxembourg, 4th edition.

Ramírez-Alujas, V. (2011). Sobre la aplicación y desarrollo del concepto de innovación en el sector público: estado del arte, alcances y perspectivas. *Revista Circunstancia*, (26).

Silva, T. B., Souto, M. C. B., Silveira, M. M., de Oliveira, G. A., Dultra, A. Z., Júnior, T. A., da Costa, T. M., Nelson, R. A. R. R., and Galvão, T. M. N. (2025). Intellectual property in language models: Challenges of ownership in the integration of multiple databases. *Beijing Law Review*, 16:257–272.

Sistla, S. (2024). Ai with integrity: The necessity of responsible ai governance. *Journal of Artificial Intelligence Cloud Computing*, 3:1–3.

Sorensen, E. and Torfing, J. (2016). *Collaborative Innovation in the Public Sector*, page 117–138. Cambridge University Press.

Trisnawati (2024). Artificial intelligence governance and regulation: A roadmap to developing legal policies for artificial intelligence deployment. *Journal of Governance and Administrative Reform*, 5(2):185–194.

Vivian, M., Ashrafur, R. N., Tusher, M. T., Akther, M. N., and Rayhan, R. U. (2024). Ethical implications of ai- powered predictive policing: Balancing public safety with privacy concerns. *Innovatech Engineering Journal*, 2(01):47–58.