



UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE ENGENHARIA DO CONHECIMENTO
CURSO DE ESPECIALIZAÇÃO EM INTELIGÊNCIA E INOVAÇÃO APLICADAS NO
ENFRENTAMENTO AO CRIME ORGANIZADO

Carlos Eduardo Conceição Silva
Fabrício Ferrão Rodrigues

**A fragmentação de informações na Segurança Pública: os desafios para a Governança
de dados e a efetividade da análise criminal**

Florianópolis
2026

Carlos Eduardo Conceição Silva

Fabício Ferrão Rodrigues

A fragmentação de informações na Segurança Pública: os desafios para a Governança de dados e a efetividade da análise criminal

Trabalho de Conclusão de Curso submetido ao curso de Especialização em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado, do Centro Tecnológico da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de especialista em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado.

Orientadora: Dra. Patrícia de Sá Freire
Coorientador: Rivaldo de Almeida Arruda

Florianópolis

2026

Silva, Carlos Eduardo Conceição

A fragmentação de informações na Segurança Pública: os desafios para a Governança de dados e a efetividade da análise criminal / Carlos Eduardo Conceição Silva, Fabrício Ferrão Rodrigues ; orientador, Patrícia de Sá Freire, coorientador, Rivaldo de Almeida Arruda, 2026.

63 p.

Monografia (especialização) - Universidade Federal de Santa Catarina, Centro Tecnológico, Curso de Especialização em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado, Florianópolis, 2026.

Inclui referências.

1. Ciências Sociais. 2. Governança de Dados. 3. Segurança Pública. 4. Análise Criminal. I. Rodrigues, Fabrício Ferrão . II. Freire, Patrícia de Sá . III. Arruda, Rivaldo de Almeida . IV. Universidade Federal de Santa Catarina. Especialização em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado. V. Título.

Carlos Eduardo Conceição Silva

Fabício Ferrão Rodrigues

**A fragmentação de informações na Segurança Pública: os desafios para a Governança de dados
e a efetividade da análise criminal**

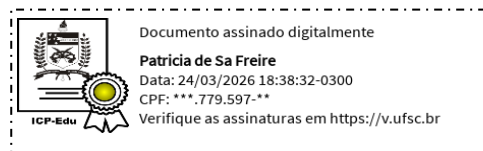
Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do título de especialista em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado e aprovado em sua forma final pelo Curso de Especialização em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado.

Florianópolis, 12 de março de 2026.



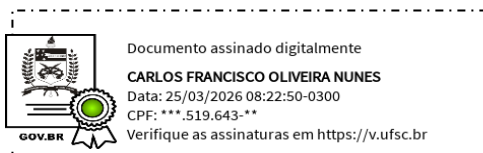
Coordenação do Curso

Banca examinadora



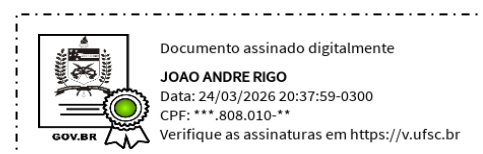
Profa. Patrícia de Sá Freire, Dra.

Orientadora



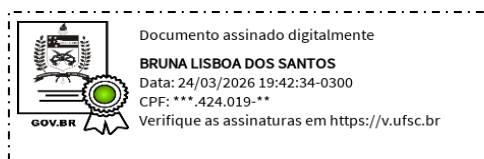
Carlos Francisco Oliveira Nunes, Dr.

Universidade Federal de Santa Catarina



João André Rigo, Msc.

Universidade de Lisboa/UL



Bruna Lisboa dos Santos, Esp.
Universidade de Caxias do Sul

Resumo

Este artigo científico investiga a fragmentação de dados criminais no Brasil e como essa realidade se torna um obstáculo crítico para a governança de segurança pública e a eficácia das análises policiais. O objetivo geral desta pesquisa é analisar os impactos da fragmentação de dados criminais na governança de dados e na efetividade da análise criminal. Especificamente, o trabalho busca levantar o histórico da gestão desses dados, investigar entraves institucionais, tecnológicos e legais, identificar boas práticas de interoperabilidade e analisar como a desarticulação interfere na tomada de decisão estratégica. A metodologia adotada é uma revisão integrativa de literatura, estruturada conforme o modelo PICO (População, Interesse, Contexto) e as diretrizes do PRISMA 2020. A busca abrangeu bases científicas como Scopus e Web of Science, além de literatura cinza, incluindo teses, relatórios técnicos e portarias normativas. Ao final do processo, foram incluídos 18 estudos, analisados qualitativamente por meio da análise de conteúdo de Bardin. Os resultados demonstram que a fragmentação é um fenômeno historicamente condicionado, sustentado por barreiras institucionais (competição entre agências e cultura de "ilhas de dados"), tecnológicas (infraestrutura desarticulada e heterogeneidade de sistemas) e legais (lacunas normativas e insegurança jurídica no compartilhamento). Tais obstáculos degradam a qualidade e a confiabilidade das informações, mantendo a segurança pública em uma dinâmica reativa em vez de proativa. Identificaram-se boas práticas, como o SUSP, SINESP, ENCCLA e REDE-LAB, que evidenciam que a interoperabilidade não é apenas uma conectividade técnica, mas uma realização de governança multinível que exige engenharia institucional, jurídica e técnica para transformar dados em inteligência pública acionável.

Palavras-chave: governança de dados, interoperabilidade, análise criminal.

Abstract

This scientific article investigates the fragmentation of criminal data in Brazil and how this reality becomes a critical obstacle to public safety governance and the effectiveness of police analysis. The general objective of this research is to analyze the impacts of criminal data fragmentation on data governance and the effectiveness of criminal analysis. Specifically, the study seeks to survey the history of data management, investigate institutional, technological, and legal barriers, identify best practices for interoperability, and analyze how disarticulation interferes with strategic decision-making. The methodology adopted is an integrative literature review, structured according to the PICo model (Population, Interest, Context) and PRISMA 2020 guidelines. The search encompassed scientific databases such as Scopus and Web of Science, as well as gray literature, including theses, technical reports, and normative ordinances. At the end of the process, 18 studies were included and qualitatively analyzed using Bardin's content analysis. The results demonstrate that fragmentation is a historically conditioned phenomenon sustained by institutional barriers (competition between agencies and a culture of "data islands"), technological barriers (disjointed infrastructure and system heterogeneity), and legal barriers (normative gaps and legal uncertainty in data sharing). Such obstacles degrade the quality and reliability of information, keeping public safety in a reactive rather than proactive dynamic. Best practices were identified, such as SUSP, SINESP, ENCCLA, and REDE-LAB, which highlight that interoperability is not merely technical connectivity but a realization of multi-level governance that requires institutional, legal, and technical engineering to transform data into actionable public intelligence.

Keywords: data governance, interoperability, criminal analysis

1. INTRODUÇÃO

O dado, enquanto elemento estruturante da sociedade contemporânea, converteu-se em ativo estratégico para o exercício do poder político, econômico e social (Cassiolato, 2025; Siqueira, 2025). Vivencia-se uma nova ordem civilizatória marcada pela interconectividade global e pela emergência do conhecimento como fator preponderante de desenvolvimento. Nesse contexto, a capacidade de coletar, tratar e transformar dados em informação e conhecimento qualificado passou a definir a posição de liderança das nações e organizações no sistema-mundo, configurando o que Cristóvam e Souza (2024) denominam de colonialismo digital.

A hegemonia contemporânea, portanto, não mais se funda exclusivamente na posse de recursos naturais, mas na aptidão de gerir fluxos informacionais e mediar processos de decisão baseados em evidências (Cassiolato, 2025; Siqueira, 2025).

A centralidade dos dados na formulação de políticas públicas introduz uma nova dimensão de soberania e de segurança nacional. Sua manipulação, armazenamento e circulação tornaram-se temas estratégicos para os Estados, demandando marcos regulatórios capazes de assegurar integridade, interoperabilidade e proteção contra interferências externas (Cristóvam & Souza, 2024). A governança de dados, nesse sentido, transforma-se em recurso territorial e em instrumento para a segurança pública, condicionando a capacidade estatal de regular sistemas complexos e de orientar políticas intersetoriais (Cristóvam, Souza, 2024; Cassiolato, 2025; Siqueira, 2025).

A literatura contemporânea sobre Governança Multinível Pública (Kempner-Moreira, Freire e Souza, 2022) reconhece que a efetividade da ação pública depende da articulação de fluxos decisórios e informacionais entre diferentes níveis e atores institucionais. No campo da segurança pública, essa premissa assume importância singular. O recrudescimento da violência e a crescente sofisticação das organizações criminosas exigem estratégias baseadas em inteligência e cooperação, apoiadas em sistemas de dados integrados e confiáveis (FBSP, 2024).

No entanto, pesquisas recentes (Lima, 2008; Durante, 2009; Lira, Caballero e Nascimento, 2022) apontam a persistência de um modelo fragmentado de produção e tratamento de dados criminais no Brasil, marcado por baixa interoperabilidade entre instituições e ausência de padronização de registros e classificações.

Essa desarticulação entre os órgãos do sistema de defesa social¹ compromete a qualidade e a confiabilidade dos dados coletados, tratados e analisados no contexto criminal e para a formulação de políticas públicas. Segundo Lima (2008), a coexistência de sistemas autônomos e a falta de comunicação entre bases de dados geram redundâncias, lacunas e inconsistências que prejudicam a articulação estratégica e, por consequência, a governança desses dados.

Para fins de delimitação analítica neste estudo, o conceito de 'dados criminais' transcende os meros registros de ocorrência policial. Amparado na necessidade de uma governança multinível, entende-se por dados criminais o conjunto de registros provenientes de instituições policiais (civis e militares), órgãos de justiça (Ministério Público e Judiciário), sistema prisional, e sistemas de inteligência e controle financeiro (como o COAF e a Receita Federal). Essa inclusão ampla justifica-se teoricamente, pois a análise criminal contemporânea depende da intersectorialidade dessas diversas fontes operando em rede.

O problema não se limita à dimensão tecnológica, mas reflete fragilidades institucionais e culturais que afetam a governança dos dados, entendida por Silva, Couto e Freire (2017), como o conjunto de princípios, estruturas e mecanismos destinados a garantir a qualidade, a integridade e o uso responsável do conhecimento nas organizações. Sob essa perspectiva, a fragmentação dos dados criminais pode ser compreendida como um obstáculo à própria governança desses dados (Freire, 2021; Kempner-Moreira et al., 2022; Nunes, 2025), que, no caso da segurança pública, é fundamental para consolidar práticas de análise criminal orientadas por evidências e para aprimorar o processo decisório das forças de segurança (Boba, 2005; Azevedo, Riccio, Ruediger, 2011).

Diante desse cenário, emergem duas constatações centrais. A primeira é a necessidade de compreender a governança de dados criminais como mecanismo estruturante da eficiência das forças de segurança pública. E a segunda é a urgência de superar os entraves tecnológicos e institucionais que impedem a interoperabilidade dos sistemas para a governança de dados criminais.

Nesse cenário, em que a governança de dados criminais emerge como dimensão estratégica para o Estado, a Segurança Pública figura como um dos campos mais sensíveis à

¹Embora o marco legal e normativo brasileiro (como o Art. 144 da CF), bem como a literatura recente utilize predominantemente o termo 'Segurança Pública', este estudo opta epistemologicamente pelo conceito de 'Defesa Social'. Enquanto a 'segurança pública' remete a uma atuação estatal frequentemente isolada e voltada ao patrulhamento preventivo e repressivo, o paradigma da 'Defesa Social' se alinha à Governança Multinível Pública (Kempner-Moreira et al., 2022), abrangendo um ecossistema interinstitucional de inteligência, justiça e tecnologia interagências.

ausência de integração informacional. A incapacidade de articular bases de dados entre instituições policiais, órgãos de justiça e sistemas de inteligência revela um descompasso entre o volume de informações disponíveis e sua efetiva utilização para subsidiar decisões estratégicas (Lima, 2008; Durante, 2009).

Essa condição reflete uma lacuna de governança que ultrapassa a questão técnica e adentra o campo institucional, jurídico e cultural, demonstrando a fragilidade de mecanismos colaborativos e de interoperabilidade entre níveis e atores que produzem, tratam, analisam e interpretam dados criminais. Embora existam avanços como a criação do Sistema Único de Segurança Pública (SUSP) no Brasil, ainda prevalecem, de modo geral, modelos fragmentados, nos quais diferentes sistemas coexistem de forma isolada, dificultando a consolidação de uma política de segurança orientada por evidências e pela análise inteligente de dados (Nunes, 2025; Kempner-Moreira, Freire e Souza, 2022).

Essa fragmentação não apenas compromete a confiabilidade das análises criminais, mas também limita a capacidade do Estado de responder de maneira integrada e eficiente às dinâmicas complexas da criminalidade contemporânea (Silva, 2024). Assim, este estudo propõe-se a investigar esse cenário e, para isso, pretende-se responder à seguinte questão de pesquisa: **Como a fragmentação de dados criminais entre diferentes órgãos do sistema de defesa social compromete a governança de dados e a efetividade da análise criminal?**

Para responder a essa questão, este estudo tem por objetivo geral analisar os impactos da fragmentação de dados criminais para a governança de dados e efetividade da análise criminal.

Para alcançar este objetivo geral, delimitam-se os objetivos específicos a seguir:

- (i) levantar o histórico da produção, gestão e governança de dados criminais na literatura;
- (ii) investigar os entraves institucionais, tecnológicos e legais que dificultam a governança de dados e as suas consequências;
- (iii) investigar a evolução da análise criminal de segurança pública, incluindo a gestão de estatísticas integradas;
- (iv) identificar boas práticas de interoperabilidade e governança de dados criminais;
- (v) analisar como a fragmentação de dados interfere na qualidade, confiabilidade e integridade das informações geradas para a tomada de decisão estratégica em segurança pública.

A relevância teórica desta pesquisa reside na necessidade de aprofundar a compreensão sobre a governança de dados criminais como fenômeno situado no campo da

Governança Multinível Pública (MultiGov). Embora as bases conceituais da Governança Multinível estejam consolidadas no debate sobre políticas públicas (Kempner-Moreira, Freire & Souza, 2022; Freire, 2021), ainda são escassos os estudos que analisam sua aplicação aos fluxos informacionais e decisórios da Segurança Pública.

Além disso, a literatura sobre governança de dados na administração pública tende a privilegiar dimensões técnicas e tecnológicas, negligenciando fatores sociopolíticos e culturais que condicionam a efetividade da governança (Neves, 2024; Zilli, 2022). Este estudo, ao incorporar a lente teórica da Governança Multinível de Dados (MultiGov-Data), propõe uma ampliação epistemológica do conceito, compreendendo a governança de dados criminais como um sistema de interdependências entre atores, níveis e políticas.

Assim, a investigação contribui para preencher uma lacuna na literatura ao propor uma articulação entre governança de dados, governança pública e análise criminal, fortalecendo o corpo teórico sobre governança orientada por evidências e inteligência institucional no Estado brasileiro (Nunes, 2025; Kempner-Moreira, 2022).

Ainda, ao investigar os impactos dessa fragmentação, o estudo oferece evidências concretas sobre os obstáculos institucionais, tecnológicos e culturais que dificultam a governança de dados criminais no país. Sua contribuição prática consiste em subsidiar o aperfeiçoamento das políticas públicas de segurança baseadas em evidências, oferecendo recomendações para o fortalecimento da interoperabilidade informacional, da inteligência analítica e da coordenação multinível no âmbito do SUSP, no caso do Brasil.

Espera-se, assim, que os resultados desta pesquisa contribuam para consolidar uma cultura de governança colaborativa e de uso estratégico dos dados na segurança pública brasileira.

2. PROCEDIMENTOS METODOLÓGICOS

Este estudo caracteriza-se como uma revisão integrativa de Literatura para investigar a fragmentação dos dados criminais e seus impactos na governança e efetividade da análise criminal no sistema de defesa social brasileiro (Whittemore e Knafl, 2005; Creswell, 2014; Denzin e Lincoln, 2018).

2.1 Procedimentos para Condução da Revisão Integrativa da Literatura

A condução desta revisão integrativa segue as diretrizes apresentadas no Cochrane Handbook for Systematic Reviews of Interventions (versão 6.5, 2019), adaptadas ao contexto das Ciências Sociais Aplicadas. O método foi estruturado com base nas seis etapas clássicas da revisão integrativa propostas por Souza, Silva e Carvalho (2010) e na sistematização de Whitemore e Knafl (2005), assegurando rigor, transparência e reprodutibilidade do processo.

Portanto, este artigo trata-se de uma investigação de caráter integrativo, cujo objetivo é analisar os impactos da fragmentação de dados criminais sobre a governança de dados e a efetividade da análise criminal no Brasil. A revisão buscou preencher uma lacuna identificada na literatura, referente à ausência de estudos que articulem os entraves institucionais, tecnológicos e legais à interoperabilidade dos dados criminais no contexto brasileiro.

Para isso, a questão de pesquisa foi delineada segundo o modelo PICO (População, Interesse, Contexto), conforme recomendações da Cochrane (2019):

Quadro 01 - Pergunta PICO

Elemento	Definição
P – População	Sistemas de dados criminais fragmentados
I – Interesse (Intervenção)	Governança e cooperação de dados criminais
Co – Contexto	Sistemas de defesa social

Fonte: Autores

Assim, como apresentado na introdução deste artigo, a pergunta a ser respondida por essa pesquisa é: Como a fragmentação de dados criminais entre diferentes órgãos do sistema de defesa social compromete a governança de dados e a efetividade da análise criminal? Essa questão orientou o processo de busca, seleção, análise e síntese dos estudos incluídos na revisão.

2.2 Estratégia de Busca e Fontes de Dados

A busca foi conduzida de forma sistemática e reprodutível, abrangendo fontes nacionais e internacionais. As bases consultadas incluem Scopus e Web of Science. Foi considerada também a literatura cinzenta, com inclusão de dissertações, teses e documentos institucionais

(BDTD e relatórios técnicos) que serão explicitados a posteriori. Além disso, excluíram-se desta revisão anais de eventos e não foram realizadas buscas manuais em eventos ou contatos com especialistas.

Para a busca sistematizada nas bases Scopus e Web of Science, os descritores empregados foram validados a partir dos termos controlados DeCS/MeSH e da construção da seguinte string de busca:

*data AND (governance OR cooperation) AND fragment AND crim**

A busca foi realizada em 17 de outubro de 2025 e a elaboração da estratégia de busca reflete diretamente as dimensões do protocolo PICO. O elemento População (P - Sistemas de dados criminais) foi contemplado pelos termos *data* e *crim**; o Interesse (I - Governança e cooperação) orientou a inclusão de *(governance OR cooperation)*; e o Contexto (Co - sistemas fragmentados de defesa social) materializou-se na inclusão do termo *fragment*.

A variação de sintaxe e o uso de operadores booleanos (AND, OR) e de truncamento (como o uso do asterisco em *crim**) justificam-se pela necessidade de adequação aos algoritmos de indexação específicos da Scopus e Web of Science. Isso garante a captura de variações semânticas da palavra *crime* ou *criminal*, conforme preconizado pelas diretrizes da Cochrane (2019) para revisões sistemáticas e integrativas.

Justifica-se a inclusão do termo “cooperação” porque em busca exploratória realizada previamente foi observado o uso do termo em contexto de governança. Assim, optou-se por excluir manualmente os artigos que porventura falem de cooperação fora do contexto desta pesquisa.

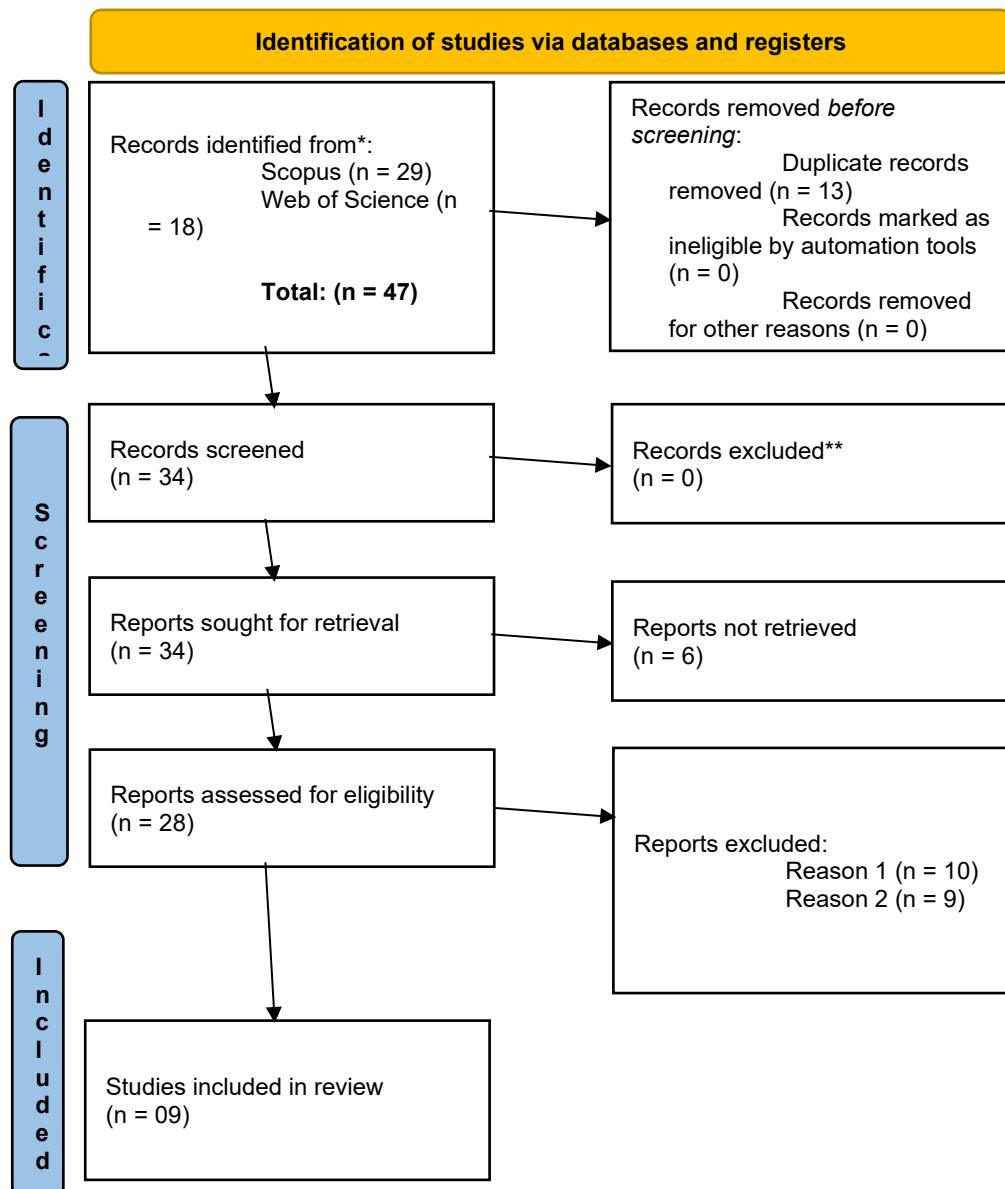
Os critérios de elegibilidade para a busca sistematizada foram definidos para garantir a pertinência e a qualidade dos estudos selecionados:

1. Tipos de estudos: artigos empíricos, qualitativos, quantitativos, mistos e teórico-analíticos publicados em periódicos científicos e anais de eventos científicos;
2. Contexto: Sistema de segurança pública, governança de dados criminais e interoperabilidade entre órgãos do sistema de defesa social.
3. Exclusão: textos sem acesso integral ou que fogem ao contexto da governança e fragmentação de dados criminais.

2.3 Processo de Seleção e Extração dos Estudos

A triagem dos resultados seguiu o fluxo PRISMA 2020, com dupla checagem independente e um terceiro revisor para resolução de divergências. O gerenciamento das referências foi realizado com auxílio dos softwares Rayyan e Mendeley. A seguir, apresenta-se o fluxo PRISMA e os artigos selecionados na etapa sistematizada, além da indicação da literatura cinza levantada:

Figura 01 – PRISMA 2020



Fonte: Adaptado de Page MJ, et al. (2021)

A seguir, apresentam-se os 09 registros resgatados da busca sistematizada:

Quadro 02 - Artigos Resgatados na Busca Sistematizada

Autor(es)	Ano	Título	Revista	DOI
Orji	2015	Multilateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation?	2015 7th International Conference On Cyber Conflict - Architectures In Cyberspace (Cycon)	*
Ra e Kim	2019	Racialized perceptions of the police Measuring the dimensions of juveniles' perceptions of the police	Policing-An International Journal Of Police Strategies & Management	10.1108/PIJPSM-11-2017-0144
Omelicheva e Markowitz	2021	When Does the Crime-Terror Nexus Fail to Materialize? Drug Trafficking, Militants, and the State in Russia	Journal Of Global Security Studies	10.1093/jogss/ogz078
Wagenaar et al.,	2015	Overcoming Conflicting Logics of Care and Justice: Collaborative Innovation in Dealing with Habitual Offenders in the Netherlands	Collaborative Governance And Public Innovation In Northern Europe	10.2174/97816810801301150101
Lili et al.,	2024	Enhancing Security, Economy, and Education: A Policy Analysis of the Indonesia-Malaysia Border Region	Lex Scientia Law Review	10.15294/lslr.v8i2.11039
Aplin	2022	The policing, investigation and governance of 'Rogue Trader' fraud: Whose responsibility?	Police Journal	10.1177/0032258X211020038
Breuil, Siegel e van Uhm	2022	Smoke and Mirrors: Empirical Research into the Illegal Trade in Tobacco Products in Europe	*	10.1007/978-3-030-67802-9_3
Yagunov	2020	THE UKRAINIAN PRISON AND PROBATION POLICY (1991 – 2020): GENERALIZATION OF MODULATIONS AND ASSESSMENT OF KEY INDICATORS	Evropsky Politicky a Pravni Diskurz	10.46340/eppd.2020.7.5.15
Meyerhoff Nielsen et al.,	2017	Georgia on my mind: A study of the role of governance and cooperation in online service delivery in the caucasus	Lecture Notes in Computer Science	10.1007/978-3-319-64677-0_7

Fonte: Dados da pesquisa; Elaboração: Autores, 2025.

2.3.1 Estratégia de busca da Literatura Cinza

Para minimizar o viés de publicação, esta revisão incluiu a busca de literatura cinza utilizando descritores diferentes dos aplicados nas bases principais ao passo que também

utilizou termos livres e palavras-chave, tendo como foco a busca manual e dirigida em repositórios institucionais, visando capturar documentos de alta relevância prática, como portarias e relatórios técnicos, que não seguem o sistema de indexação de periódicos científicos.

Os descritores empregados foram validados a partir dos termos controlados DeCS/MeSH para Segurança Pública: Segurança Pública, Policiamento, com os seguintes termos livres: Inteligência Policial, Integração de Forças de Segurança, Segurança baseada em evidências, Combate ao Crime Organizado. DeCS/MeSH para Interoperabilidade: Interoperabilidade de Dados, Sistemas de Informação, com os seguintes termos livres: Intercâmbio de dados, Integração de sistemas. DeCS/MeSH para Governança de Dados: Gestão de Informação, Acesso à Informação, Governança Digital. Termos Livres: Qualidade do dado, Intermediação de dados, Governança colaborativa, conforme quadro 3 a seguir.

Quadro 03: Tesouros, descritores e termos livres.

Tesouro	Temática	Descritores / Termos Controlados	Termos Livres
DeCS/MeSH	Segurança Pública	Segurança Pública; Policiamento.	Inteligência Policial; Integração de Forças de Segurança; Segurança baseada em evidências; Combate ao Crime Organizado.
DeCS/MeSH	Interoperabilidade	Interoperabilidade de Dados; Sistemas de Informação.	Intercâmbio de dados; Integração de sistemas.
DeCS/MeSH	Governança de Dados	Gestão de Informação; Acesso à Informação; Governança Digital.	Qualidade do dado; Intermediação de dados; Governança colaborativa.

Fonte: Dados da pesquisa; Elaboração: Autores, 2025.

Os descritores empregados foram validados a partir dos termos controlados DeCS/MeSH e por meio da construção da seguinte *string* de busca:

("Segurança Pública" OR "Policiamento") AND ("Interoperabilidade" OR "Integração de Sistemas") AND ("Governança de Dados" OR "Gestão da Informação")

Os critérios de elegibilidade para a busca da literatura cinza foram:

1. Tipos de estudos: artigos empíricos, qualitativos, quantitativos, mistos e teórico-analíticos, publicados em periódicos científicos, anais de eventos científicos, repositórios institucionais e de organizações, portais governamentais assim como documentos disponíveis nesses bancos de dados.

2. Contexto: Sistema de segurança pública, governança de dados criminais e interoperabilidade entre órgãos do sistema de defesa social.
3. Exclusão: textos sem acesso integral ou que fogem ao contexto da governança e fragmentação de dados criminais integrados ao setor público.

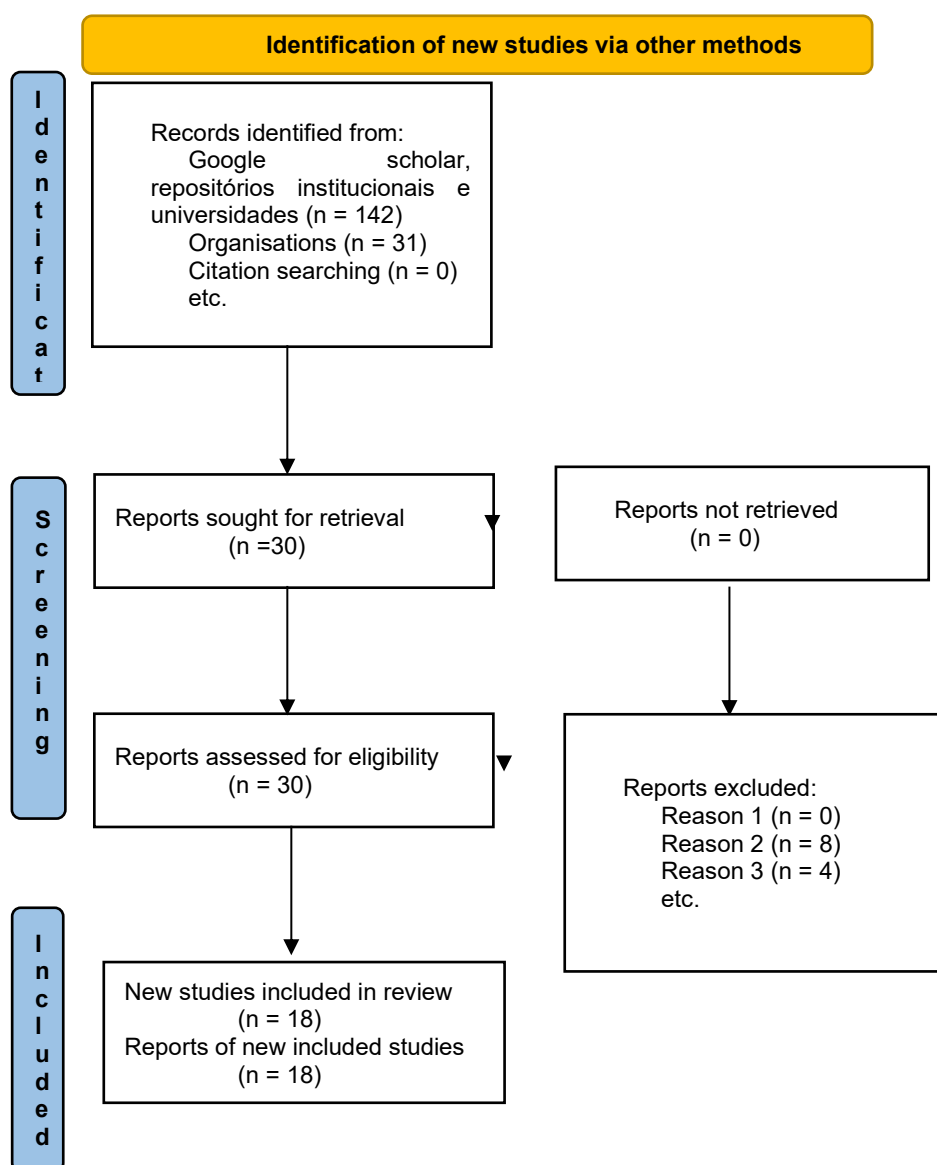
Para a busca manual em portais governamentais e organizações foram utilizadas, além dos termos livres, algumas palavras-chave como: integração de sistemas, troca de informações, interconexão de dados, sistemas interoperáveis, interoperabilidade informacional, políticas de segurança, inteligência policial, defesa social, gestão da segurança pública, segurança pública baseada em evidências, prevenção da criminalidade, gestão da informação, administração de dados, qualidade do dado, governança digital. Esse procedimento foi fundamental para localizar registros em sites da web institucionais, onde os descritores controlados nem sempre capturam as nomenclaturas das portarias e normativas recentes.

A busca foi estendida para sites da *web* de órgãos oficiais e instituições de pesquisa (Ministério da Justiça, IPEA e Fórum Brasileiro de Segurança Pública), sendo crucial para incluir documentos de natureza normativa (portarias) e estatística (anúários), que não estão sistematizados em bases acadêmicas, mas que fundamentam a prática da segurança pública no Brasil.

2.3.2 Processo de seleção e extração dos estudos da literatura cinza

A triagem dos resultados seguiu o fluxo PRISMA 2020 (Figura 2) com os mesmos critérios de seleção e extração das bases principais.

Figura 2: Fluxograma PRISMA 2020



Fonte: Adaptado de Page MJ, et al. (2021)

No processo de identificação foram detectados 173 trabalhos, dos quais 142 estão disponíveis no Google Scholar, nos repositórios institucionais e de universidades como Catálogo de Teses e Dissertações da CAPES, no portal de periódicos da CAPES. 31 obras em *sites* organizacionais como Ministério da Justiça, Polícia Federal, Fórum Brasileiro de Segurança Pública e Diário Oficial da União. Nessa fase foi realizada leitura flutuante com foco nos títulos e resumos, sendo descartados documentos sem aderência aos temas de integração, interoperabilidade ou governança de dados criminais.

Em seguida foi realizada a recuperação de 30 estudos (*Reports sought for retrieval*), os quais apresentavam aderência direta aos critérios de inclusão. Desses, todos foram efetivamente recuperados em sua integridade para a etapa de avaliação de elegibilidade.

Os 30 relatórios recuperados foram avaliados para elegibilidade (*assessed for eligibility*) por meio de leitura integral. Nesta fase, aplicaram-se rigidamente os critérios de exclusão, resultando na exclusão quantificada baseada nas seguintes categorias: (i) Inadequação temática ou ausência de aderência ao recorte analítico do sistema de defesa social (n=8); e (ii) Fuga ao contexto do setor público brasileiro (n=4). Essa categorização explícita confere robustez e mitiga impressões de subjetividade no processo seletivo, em conformidade com o método PRISMA 2020. Ao final do processo de seleção, foram incluídos 18 estudos (n=18), os quais foram selecionados para a síntese qualitativa. A amostra final caracteriza-se pela diversidade de fontes, englobando artigos científicos, dissertações recentes (2024), relatórios institucionais de referência e atos normativos vigentes do Ministério da Justiça e Segurança Pública (MJSP).

Foram obtidos os seguintes resgates: 02 do repositório de teses e dissertações da CAPES; 03 do portal de Periódicos da CAPES; 01 do repositório da Fundação Getúlio Vargas (FGV); 01 do repositório do Ministério da Justiça; 01 do repositório da Sociedade Brasileira de Computação; 07 do Fórum Brasileiro de Segurança Pública. Além disso, foi acessado o Diário Oficial da União na busca de documentos normativos onde foram selecionadas 03 (três) portarias pertinentes ao tema. O quadro 4 especifica os locais de busca, o quantitativo de documentos selecionados e as instituições responsáveis:

Quadro 4: Resgates bibliográficos por banco de dados e instituição

Banco de Dados / Repositório	Número de Resgates	Instituição Integrante/Responsável
Repositório de Teses e Dissertações	02	CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior)
Portal de Periódicos	03	CAPES
Repositório Fundação Getúlio Vargas (FGV)	01	FGV
Repositório Ministério da Justiça	01	Ministério da Justiça e Segurança Pública
Repositório da Sociedade Brasileira de Computação	01	SBC (Sociedade Brasileira de Computação)
Fórum Brasileiro de Segurança Pública	07	FBSP
Diário Oficial da União (DOU)	03	Imprensa Nacional / Governo Federal (Busca de documentos normativos/portarias)

Fonte: Dados da pesquisa; Elaboração: Autores, 2025.

Os critérios de escolha priorizaram a interoperabilidade e a governança de dados. A leitura foi organizada de forma sistemática: os documentos foram avaliados para elegibilidade mediante leitura íntegra, sendo excluídos aqueles sem densidade técnica. O material foi analisado e transformado em argumento através da técnica de síntese qualitativa que será demonstrada à frente.

Por fim, no quadro 5, estão descritos os documentos levantados a partir da busca da literatura cinza:

Quadro 05 - Documentação Resgatada na literatura cinza

Tipo do Documento	Título	Autor(es) e ano	Revista/Base/Instituição	Justificativa
Dissertação	A Segurança pública brasileira no contexto Pós-88: Desafios da integração.	Silva, Marcos Paulo Hiath 2024.	Instituto de Pesquisa Economical Aplicada (IPEA).	Aborda a necessidade da superação da fragmentação institucional considerando essencial para que as políticas de segurança e de inteligência atinjam a eficácia necessária
Dissertação	Uma Plataforma para Promover a Interoperabilidade entre Órgãos de Segurança Pública	Nunes, Diogo Cirne.	Programa de Pós-graduação em Tecnologia da Informação da Universidade Federal do Rio Grande do Norte	Aborda a necessidade de automatização de procedimentos na área de segurança pública, que historicamente dependem de processos manuais e isolados, dificultando a cooperação e a eficiência entre as diferentes agências (como polícias civil, militar e órgãos de perícia)
Livro	Anuário Brasileiro de Segurança Pública	Fórum Brasileiro de Segurança Pública, 2022.	Fórum Brasileiro de Segurança Pública	Panorama da análise de dados e informações mais recentes sobre Segurança Pública
Artigo	A inteligência Policial e a cooperação interagências no combate ao crime organizado nas fronteiras	Gomes, Rodrigo Carneiro	Revista Brasileira de Ciências Policiais	Destaca o papel da Inteligência de Estado e avalia sua adequação para promover a integração interinstitucional na faixa de fronteira, visando à proteção nacional, à defesa e, principalmente, à repressão e inibição do crime organizado transfronteiriço
Artigo	Segurança pública baseada no uso de dados	Silveira, C. T.	Brazilian Journal of Business	Defesa de um modelo de segurança pública orientado por dados e análise criminal
Artigo	Governança Digital e	ARAÚJO FILHO, F. G.	Anais do XIII latin american symposium on	Inovação por meio da Heurística investigativa,

	Investigação Patrimonial: Uma Heurística para Identificação de Grupos Econômicos	de; ISHIKAWA, E.	digital government (lasdigov),	governança digital e cooperação interinstitucional.
Artigo	Convergências e divergências metodológicas das bases de dados penitenciários no Brasil.	FERREIRA, Carolina Cutrupi	Livro Estatística de Segurança Pública: Produção e uso de dados criminais no Brasil (Fórum Brasileiro de Segurança Pública)	Aborda a complexidade e os desafios na coleta, organização e interpretação dos dados sobre a população prisional brasileira
Artigo	Segurança pública na era do Big Data: mapeamento e diagnóstico da implementação das novas tecnologias no combate à criminalidade	AMARAL, Thiago Bottino do; VARGAS, Daniel; PRATES, Fernanda	Repositório Fundação Getúlio Vargas	Analisa a incorporação de Big Data e ferramentas analíticas na segurança pública brasileira, discutindo potencial de cruzamento massivo de bases (policiais, judiciais, sociais)
Livro (Plano de ação)	ENCCLA 2023: estratégia nacional de combate à corrupção e à lavagem de dinheiro.	Ministério da Justiça e Segurança Pública	Repositório Ministério da Justiça e Segurança Pública	Execução da Interoperabilidade institucional e informacional
Artigo	Interoperabilidade informacional entre sisbin e ministério público e aplicação pelo órgão ministerial de conhecimentos oriundos da atividade de inteligência – estágio atual e desafios.	RODRIGUES, Luiz Cláudio de Queiroz	Revista Brasileira de Inteligência	As dificuldades na concretização da interoperabilidade informacional entre o Sisbin e o Ministério Público
Artigo	Democracia, transparência e inovação como ferramentas de accountability: O papel do Fórum Brasileiro de Segurança Pública	Vasconcelos, F.T.R.	Fórum Brasileiro de Segurança Pública	Produção, padronização e divulgação de estatísticas criminais
Artigo	Inteligência Artificial na segurança	Furtado, V.	Fórum Brasileiro de Segurança Pública	Apresenta conceitos básicos de IA e aplicações em segurança pública (predição

	pública: conceitos, perspectivas e desafios			de crime, reconhecimento de padrões, análise de redes, apoio à investigação).
Artigo	Modernização dos modelos de policiamento: uso das estatísticas na segurança pública para além da análise dos registros de ocorrência na polícia (DF - 2015 a 2018)	Durante, M. and Ribeiro, A. and Viana, M. and Barbosa, T.	Fórum Brasileiro de Segurança Pública	Argumenta que a modernização do policiamento passa por abandonar o uso meramente contábil dos registros de ocorrência e adotar análise criminal qualificada, com foco em padrões espaciais, temporais e contextuais dos crimes.
Artigo	Notas sobre a qualidade dos dados de homicídios no Brasil	Borges, D.	Fórum Brasileiro de Segurança Pública	Falta de integração entre polícia, IML e saúde que geram sub ou má notificação de homicídios.
Artigo	Sobre as estatísticas criminais no Rio de Janeiro (1908-2020): uma breve história e um testemunho	Misse, M.	Fórum Brasileiro de Segurança Pública	Reconstrói, em perspectiva histórica, a formação e transformação das estatísticas criminais no Rio de Janeiro, mostrando como categorias, métodos e instituições foram mudando ao longo do século XX e início do XXI.
Portaria	Portaria MJSP nº 847	Ministério da Justiça e Segurança Pública	Diário Oficial da União	Criação do Sistema Nacional de Inteligência para Enfrentamento ao Crime Organizado (Orcrim)
Portaria	Portaria SNJ nº 242	Secretariado Nacional de Justiça (SNJ) do Ministério da Justiça	Diário Oficial da União	Instituiu a Rede Nacional de Laboratórios de Tecnologia contra Lavagem de Dinheiro (REDE-LAB), assegurando a cooperação, compartilhamento de técnicas e dados entre órgãos de combate à lavagem de dinheiro, como Polícias, Ministérios Públicos e Receita Federal
Portaria	Portaria MJSP nº 145	Ministério da Justiça e Segurança Pública	Diário Oficial da União	Atribui à Rede-Lab a natureza de Programa de Articulação Institucional. Fortalece a colaboração entre os laboratórios de tecnologia do MJSP e outras instituições, visando aprimorar a segurança pública.

Fonte: Dados da pesquisa; Elaboração: Autores, 2025.

Além da perspectiva teórica, a seleção dos trabalhos buscou trazer uma concepção pragmática à investigação. O material selecionado cobre desde a teoria acadêmica da integração até a implementação prática por meio de portarias e sistemas de inteligência, além de contribuir no estabelecimento de uma visão escalar (global-local), administrativa, normativa e operacional do tema. Assim, foram escolhidas obras que descrevem a realidade estrangeira e a local, trabalhos que atribuem uma visão ampla de governança de dados não somente à sua perspectiva tecnológica, mas também institucional e regulatória. Buscou-se incluir teoria e aplicabilidade, por meio da demonstração de pesquisas empíricas que descrevem a operacionalização da governança de dados em segurança pública depositadas em sites de organismos internacionais, portais governamentais, repositórios institucionais de ONGs e fóruns.

A extração dos dados foi conduzida por meio de uma planilha eletrônica padronizada baseada no Quadro 7.3.a do Cochrane Handbook, contemplando: autor, ano, objetivo, tipo de estudo, instrumentos utilizados, principais achados e limitações. Ainda, a planilha foi complementada conforme a técnica de análise de conteúdo de Bardin (2016). Para esta etapa, a planilha contemplou também variáveis relacionadas à governança, interoperabilidade e restrições institucionais nos dados criminais.

2.4 Análise dos Dados

A análise dos documentos levantados pela busca sistematizada acrescida da literatura cinza garante uma revisão sólida e contextualizada para o contexto brasileiro. A síntese dos achados seguiu abordagem qualitativa, com base na análise de conteúdo de Bardin (2016).

2.4.1 Pré-análise

Durante a primeira etapa, procedeu-se à leitura flutuante de todo o material coletado na pesquisa. Realizou-se a seleção dos documentos mais relevantes para os objetivos propostos, definindo-se o corpus a ser analisado, com base em critérios de representatividade e pertinência temática. Também foram estabelecidos objetivos analíticos e elaborados indicadores para orientar a categorização dos dados, seguindo as recomendações metodológicas de Bardin (2016).

2.4.2 Exploração do material

Na etapa seguinte, promoveu-se a codificação minuciosa dos dados extraídos do material documental e bibliográfico. Foram identificadas e agrupadas unidades de registro (como temas, palavras-chave, expressões representativas e acontecimentos recorrentes) e suas respectivas unidades de contexto. O material foi categorizado em diferentes eixos analíticos, o que permitiu agrupar sentidos convergentes e divergentes, organizando o conteúdo de acordo com o roteiro temático previamente definido na pré-análise.

Os dados levantados na literatura foram organizados nas categorias:

- (1) fragmentação e Governança Multinível;
- (2) entraves institucionais, tecnológicos e legais;
- (3) impactos na efetividade da análise criminal; e
- (4) boas práticas e modelos de interoperabilidade,

Para garantir a transparência da análise de conteúdo, as unidades de registro (termos e expressões representativas extraídas dos textos) foram agrupadas por similaridade semântica e aderência temática. O Quadro 6 detalha os códigos utilizados e suas definições operacionais, demonstrando como foram agregados para formar as quatro categorias analíticas do estudo:

Quadro 6 - Estrutura de Categorização da Análise de Conteúdo

Categorias Analíticas	Unidades de Registro (Termos e Expressões)	Critério de Agrupamento
1. Fragmentação e Governança Multinível	"Ilhas de dados"; "Desarticulação"; "Baixa interoperabilidade"; "Competição institucional"; "Trabalho isolado".	Trechos que descrevem o isolamento informacional, a falta de cooperação estruturada entre as agências e a ausência de uma arquitetura de governança integrada no sistema de defesa social.
2. Entraves institucionais, tecnológicos e legais	"Insegurança jurídica"; "Lacunas normativas"; "Retenção defensiva"; "Heterogeneidade de sistemas"; "Infraestrutura desarticulada"; "Cultura resistente".	Identificação das barreiras normativas (como a ausência de lei específica e tensões de privacidade), defasagens de infraestrutura de TI e resistências culturais que impedem a conexão dos bancos de dados.
3. Impactos na efetividade da análise criminal	"Dinâmica reativa"; "Baixa aplicabilidade"; "Redundância"; "Retrabalho"; "Perda de confiabilidade"; "Qualidade do dado".	Consequências práticas da desarticulação, resultando em dados de baixa qualidade que limitam a capacidade proativa das polícias e prejudicam o planejamento estratégico baseado em evidências.
4. Boas práticas e modelos de interoperabilidade	"Redes colaborativas"; "Padronização de procedimentos"; "Compartilhamento informacional"; "Plataformas integradas" (ex: SINESP, ENCCLA, REDE-LAB).	Relatos de plataformas, normativas ou arranjos institucionais voltados à superação da fragmentação, que promovem a integração e a inteligência interagências

2.4.3 Interpretação e tratamento dos resultados

Por fim, na terceira etapa, os dados categorizados foram submetidos a uma análise interpretativa detalhada. A equipe de pesquisa buscou realizar inferências controladas, correlacionando os achados.

O tratamento dos resultados privilegiou a reflexão crítica sobre o sentido das mensagens, o contexto de produção e os impactos dos resultados para o objeto de estudo, garantindo um diálogo rigoroso entre os dados e a literatura analisada. A síntese permitiu a triangulação dos resultados, reforçando a compreensão dos obstáculos e das dimensões sociopolíticas envolvidas na governança de dados criminais (Silva, Couto e Freire, 2017).

2.5 Aspectos Éticos e Coprodução TransHumana

A revisão não envolve dados primários, respeitando a integridade e a atribuição dos autores originais. Todo o processo foi documentado por todos os revisores e validado conforme Cochrane (2019).

Por fim, acusa-se o uso ético de ferramentas de Inteligência Artificial (ChatGPT Plus Modelos 5 e 4) para estruturação do texto e identificação de insights na etapa de interpretação. O uso da IA seguiu as diretrizes propostas por Freire e Marques (2023), na obra Coprodução TransHumana.

3. RESULTADOS

A seguir apresentam-se os resultados desta pesquisa.

3.1 O Histórico da Produção, Gestão e Governança de Dados Criminais na Literatura

A gestão da segurança pública, ao longo de sua história, tem sido marcada pela evolução das estratégias de controle social e pelo crescente reconhecimento da informação criminal como um ativo essencial para a tomada de decisão estratégica. A evolução institucional no campo da segurança pública, especialmente no início do século XXI, levou a uma redefinição das práticas de policiamento. Historicamente, as abordagens policiais eram frequentemente mais isoladas, focadas na função, estrutura e controle dentro da sociedade democrática. Contudo, o avanço de tecnologias e da informação legitimou a colaboração interagencial e a coleta de inteligência

como a melhor abordagem para combater ameaças criminosas ou terroristas (Sedgwick, Callahan e Hawdon, 2020: p.3).

Este modelo contribuiu para o surgimento de ações integradas e como uma nova abertura para o trabalho conjunto, distanciando o modelo anteriormente utilizado, baseado em ações isoladas por cada um dos órgãos de segurança pública (Sedgwick, Callahan e Hawdon, 2020: p.14).

Essa necessidade crescente de coordenação, impulsionada pelo crescimento dos problemas de segurança transnacionais, coincidiu com a ascensão da sociedade da informação, caracterizada pela hiperconectividade contínua e pela produção ininterrupta de dados. Neste novo contexto, a informação passou a ser vista como um ativo central, capaz de gerar valor e subsidiar ações estratégicas. A emergência do *Big Data* transformou radicalmente a capacidade de análise, sendo definida não apenas pelo seu volume massivo, mas principalmente pela capacidade de pesquisa, agregação e referência cruzada desses grandes conjuntos de dados por algoritmos. Assim, a gestão de segurança pública começou a se mover para as estratégias de “política criminal atuarial” ou policiamento da informação, onde o dado é usado para extrair *insights* relevantes, prever atividades criminosas futuras e orientar a tomada de decisão estratégica, prometendo inovações na prevenção de crimes. (Amaral, Vargas, Prates, 2023: p. 18, p. 23)

Apesar do imenso potencial do *Big Data* para otimizar a segurança pública e baratear custos operacionais, os desafios de governança de dados se tornaram o ponto crítico na transição para um modelo estratégico. A ausência de uma legislação unificada, como observado no contexto do México, leva a uma fragmentação regulatória que enfraquece a consistência legal e a colaboração interinstitucional (Covarrubias, 2025: p. 2).

No campo da segurança, essa fragmentação é manifesta no campo prático onde as instituições frequentemente operam em “ilhas” de dados, tratando suas bases como uma fortaleza que não deve ser compartilhada, resultando em resistência institucional. Essa falta de integração é vista pelos próprios agentes como um problema institucional, ligado a disputas de poder sobre as informações, e não apenas à falta de tecnologia, impedindo a interoperabilidade necessária para análises eficazes. A gestão do crime, portanto, reflete um complexo processo de evolução, onde o controle social é crescentemente mediado pela tecnologia, mas fragilizado pela desorganização e pela falta de coordenação no uso desse novo ativo. (Amaral, Vargas, Prates, 2023: p. 109, 111)

3.2 O Policiamento Tradicional e a Emergência da Informação como Elemento de Controle

Historicamente, a função, a estrutura e o controle policial foram temas centrais nas sociedades ocidentais. No contexto brasileiro, o debate sobre grupos criminais e a ordem social em presídios remonta, pelo menos, aos anos 1980, com a emergência das "falanges", que posteriormente originaram os modelos atuais de Organizações Criminosas. (Viana, Rocha, Ribeiro, 2023: p. 3)

A produção de dados, inicialmente, estava intrinsecamente ligada à atividade policial e judicial, focando no controle e na repressão. Contudo, desde cedo, pressões institucionais moldaram a forma como a polícia opera. (Sedgwick, Callahan e Hawdon, 2020: p. 14)

A transição democrática no Brasil, marcada pela Constituição de 1988, estabeleceu um novo marco para a segurança pública, definindo-a como dever do Estado, direito e responsabilidade de todos. Sob o novo paradigma da Segurança Pública, os estados se tornaram os principais responsáveis pela gestão das polícias Civil e Militar. Essa estrutura constitucional implementou uma separação de papéis, atribuindo o patrulhamento ostensivo a cargo da Polícia Militar e a atividade investigativa sob responsabilidade da Polícia Civil, mas não integrou suas práticas, o que, historicamente, resultou em mecanismos de disputas entre as corporações. (Amaral, Vargas, Prates, 2023: p. 43, p. 45)

As primeiras tentativas de gestão e organização de dados em nível nacional surgiram como respostas às crises de violência de grande repercussão. Durante o período compreendido entre o final dos anos 90 e o início dos anos 2000, apesar dos esforços lentos para elaborar uma Política Nacional de Segurança Pública, o sequestro do ônibus 174, em junho de 2000, precipitou a publicação do primeiro Plano Nacional de Segurança Pública. Embora fosse um plano dispersivo, representou uma virada democrática e o reconhecimento da responsabilidade do Governo Federal sobre a matéria, firmando um compromisso com a agenda de Direitos Humanos, mais especificamente na área de Segurança Pública. (Amaral, Vargas, Prates, 2023: p. 46)

3.3 A Institucionalização da Gestão de Dados e o Policiamento Orientado por Problemas

Ao longo dos anos 2000 pode ser observado o avanço do reconhecimento da importância de políticas de segurança baseadas em análise criminal e uso sistemático de dados. Nesse período, o policiamento orientado por dados consolidou suas bases na ideia de que a análise do crime permite respostas mais eficientes e resolutivas para a prevenção criminal (Silveira, 2024: p. 3). A análise criminal, por sua vez, foi definida como o uso de métodos para planejar ações

e políticas de segurança, envolvendo a obtenção, organização, análise e interpretação de dados para tirar conclusões (Senasp, 2021: p. 5).

No plano político, o segundo Plano Nacional de Segurança Pública, ambicionava reformar as instituições e implementar o Sistema Único de Segurança Pública (SUSP), buscando integrar a troca de informações entre as instituições de segurança. Embora o Plano tenha sido precocemente abandonado, em ato contínuo foi lançado o Programa Nacional de Segurança Pública com Cidadania (Pronasci), que enfatizava o caráter preventivo, o papel dos municípios e o investimento em formação policial (Amaral, Vargas, Prates, 2023: p. 46, p. 48)

Paralelamente, em um contexto internacional, pressões externas também influenciavam a gestão de dados. Nos Estados Unidos, a partir dos ataques de 11 de setembro de 2001, houve uma crescente popularidade do policiamento comunitário e de forças-tarefa multiagências, impulsionada por políticas que legitimavam a colaboração entre as instituições e o desenvolvimento da inteligência (Sedgwick, Callahan e Hawdon, 2020: p. 3)

A produção de dados criminais se tornou mais técnica, e o gerenciamento começou a se estruturar, passando por algumas etapas:

a) Definição Conceitual de Dados e Conhecimento: Conceitualmente, o dado é a quantidade de registros sobre determinado crime. A informação é o resultado do tratamento do dado (ex.: quantidade de crimes comparada ao período anterior). O conhecimento é a interpretação dessa informação, analisando o contexto e variáveis para orientar as ações do gestor (Silveira, 2024: p. 3).

b) Criação de Estruturas Nacionais de Dados: A partir de 2011, são priorizadas as políticas de segurança sobre as fronteiras, evidenciando a orientação da política de segurança para o modelo da segurança nacional, período em que é aprovada a lei que criou o Sistema Nacional de Informações de Segurança Pública, Prisionais e sobre Drogas, o Sinesp, porém não apresentava estrutura sólida e, portanto, se mostrou ineficaz na alteração de estruturas. (Amaral, Vargas, Prates, 2023: p. 48)

c) Aprimoramento na Busca dos Dados Produzidos por Organizações Criminosas: O crescimento e a expansão de facções como o Primeiro Comando da Capital (PCC) geraram a necessidade de produção e rastreamento de dados por diversas instituições. Utilizando o estado de Minas Gerais como exemplo, entre 2009 e 2018, o número de membros conhecidos do PCC, rastreados por diferentes órgãos (Ministério Público de Minas Gerais, Polícia Militar de Minas Gerais, Centro Integrado de Inteligência de Segurança Pública e Polícia Civil de Minas Gerais),

multiplicou-se exponencialmente, saindo de 72 em 2009 para 2.330 em 2018 (Gráfico 1, em Viana, Rocha, Ribeiro, 2023: p. 22).

3.4 O Advento do Big Data e os Novos Desafios de Governança

A partir da virada dos anos 2010, o campo da segurança pública foi impactado pela emergência do *Big Data* e da inteligência artificial (IA), que prometem otimizar a segurança e baratear custos operacionais (Amaral, Vargas, Prates, 2023: p. 36)

Através da análise automatizada do *Big Data*, é possível extrair grandes quantidades de dados por algoritmos, visando resultados e benefícios, sendo essa análise menos sobre os dados em si e mais sobre a capacidade de pesquisa, agregação e referência cruzada de grandes conjuntos (Amaral, Vargas, Prates, 2023: p. 36).

No Brasil, a integração dessas tecnologias ganhou forma com programas como o Sinesp Big Data, o Sinesp Geo Inteligência, o Sinesp Tempo Real e o Sinesp Busca, introduzidos através do projeto piloto “Em Frente Brasil”. O objetivo de ferramentas sob a ótica do *Big Data* é facilitar o acesso às fichas criminais, boletins de ocorrências e informações sobre focos de criminalidade, permitindo o combate à criminalidade difundido ao longo do território nacional por meio do compartilhamento de informações entre estados (Amaral, Vargas, Prates, 2023: p. 27-28).

3.4.1 A Governança e a Regulação dos Dados

O aumento massivo na produção e no tratamento de dados tornou a questão da governança uma preocupação central, especialmente com relação à regulação legal e à garantia de direitos.

a) Marco Legal: Embora a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) exclua de seu escopo o tratamento de dados realizado para fins de segurança pública e persecução penal, ela determina a necessidade de uma legislação específica para disciplinar o uso de dados pessoais por órgãos de segurança. Esse direcionamento garante aderência ao devido processo legal e aos princípios estruturantes da proteção de dados. Em paralelo, o Supremo Tribunal Federal consolidou, em 2020, a proteção de dados pessoais como direito fundamental autônomo, status posteriormente positivado pela Emenda Constitucional nº 115, de fevereiro de 2022 (Amaral, Vargas, Prates, 2023: p. 30-31).

b) Governança Fragmentada: Apesar dos avanços legais e tecnológicos, a gestão de dados é cronicamente prejudicada pela fragmentação institucional. Em contextos como o Rio de Janeiro, a divisão histórica entre Polícia Militar (ostensiva) e Polícia Civil (investigativa)

resultou na criação de bancos de dados separados, falta de comunicação, tarefas redundantes e competição institucional por recursos e prestígio, o que impede a atuação preventiva (Amaral, Vargas, Prates, 2023: p. 30-31).

3.4.2 O Conceito de Dado como Ativo e a Qualidade da Informação

O histórico da gestão de dados evoluiu para a necessidade de estabelecer uma cultura de dados nas organizações de segurança. Ainda que com certa resistência através das gerações, os Agentes de segurança da alta gestão passaram a encarar o dado como um ativo organizacional, capaz de gerar valor e subsidiar ações estratégicas (Amaral, Vargas, Prates, 2023: p. 27-28).

No entanto, a falta dessa cultura de dados, combinada com a fragmentação, leva a problemas de qualidade da informação. O Delegado Civil 1 (citado em Amaral, Vargas, Prates., 2023: p. 117) afirma que a polícia "trata muito mal o dado" e que, sem um processo de governança e qualidade de gerenciamento do dado, a coleta massiva resultará em "lixo", impedindo análises eficazes, mesmo com cientistas de dados qualificados.

A governança eficaz exige não apenas o compartilhamento, mas a interoperabilidade, ou seja, que sistemas diferentes se comuniquem usando uma linguagem comum para que os dados migrados possam ser lidos e utilizados pelas diversas instituições. A uniformização nacional de dados é vista como essencial para superar a grande disparidade tecnológica entre as polícias civis dos estados. (Policia Militar 3, Delegada Civil 3, citados Amaral, Vargas, Prates, 2023: p.108-109).

Uma recente sistematização de dados ocorreu com o Plano Nacional de Segurança Pública e Defesa Social (PNSP) 2021-2030, que estabeleceu indicadores e metas com foco no direcionamento de esforços baseado em dados. Além disso, em 2024, o Ministério da Justiça e Segurança Pública conseguiu superar limitações técnicas para agrupar 28 indicadores estatísticos de segurança, um avanço possível pela Lei do Sinesp (Silveira, 2024: p. 4, p.10).

O histórico revela uma evolução constante: da produção de dados rudimentares ligada à repressão e à segurança nacional, passando pela institucionalização de modelos de gestão orientados por problemas e pela criação de sistemas de informação nacionais (SUSP/SINESP), até chegar ao desafio atual de gerenciar o volume e a complexidade do *Big Data* em um cenário legalmente sensível. Contudo, a governança de dados é o elo fraco dessa cadeia, uma vez que as relações de confiança pessoal e as disputas institucionais continuam a prevalecer sobre a

coordenação e a integração efetiva das bases de dados, resultando na fragmentação de informações que compromete a efetividade das ações de Segurança Pública.

3.5 Entraves institucionais, legais e tecnológicos à governança

Ao levar em consideração os estudos analisados nesta investigação, percebe-se que o estabelecimento da governança de dados criminais na segurança pública não se apresenta como uma tarefa exercida com facilidade pelos gestores de segurança, tampouco se mostra uma prática amplamente aplicada e difundida pelo sistema de defesa social. Realidade que se observa não somente no Brasil, mas também em diversas partes do mundo. Empecilhos de caráter regulatório, burocráticos e barreiras tecnológicas contribuem para um lento caminhar na geração, manejo e governança dos dados criminais.

O continente europeu com o advento da União Europeia e o estabelecimento de uma governança multinível apresentou-se como um exemplo de integração interestatal por meio de cooperação interinstitucional. Porém, com a instauração do Brexit precisou ter seus mecanismos de cooperação revisados e reestruturados ante a nova realidade de ausência do Reino Unido do bloco comum (Loik, 2020).

Loik (2020) investigou o impacto estratégico do *Brexit* nos interesses de segurança interna da Europa. O estudo concluiu que a saída do Reino Unido da União Europeia traria consequências negativas para a cooperação e a segurança interna, levando à fragmentação interinstitucional, contribuindo para um significativo retrocesso nas opções de policiamento internacional e cooperação policial transfronteiriça. Observa-se, então, entraves como fragmentação da cooperação, disputa por jurisdição legal e ocorrência de exigências rigorosas de interoperabilidade de dados entre o Reino Unido e a União Europeia (UE)

O Reino Unido passa por uma remodelagem em sua política de governança enfrentando barreiras que resultam de sua saída da União Europeia. Perdeu seu voto em questões da Europol e precisa celebrar acordos de cooperação especial, ainda assim, necessita de reestruturação para estabelecer uma continuidade operacional das agências de segurança que tiveram uma interrupção cooperativa com órgãos e legislações vinculadas à UE. Em relação às barreiras legais, o Reino Unido necessita desvincular-se de leis da União Europeia, sobretudo, no que diz respeito aos direitos fundamentais e ao compartilhamento de dados internacionais, mas, para isso, precisa combater a resistência dos países europeus. A interoperabilidade de dados antes existente sob a vigília da União Europeia carece de ser intensificada restabelecendo altos padrões e qualidade de proteção de dados sobretudo ante a ameaça do terrorismo. Diante disso,

a governança na segurança interna *pós-Brexit* é travada pela tensão entre o interesse operacional mútuo em combater o terrorismo e o crime organizado transnacional e a posição jurídica inflexível da União Europeia em manter a supervisão supranacional sobre os direitos fundamentais e a proteção de dados (Loik, 2020).

Lothian (2024) aborda um problema de segurança interestatal que deixa mares e oceanos internacionais vulneráveis à criminalidade. Em sua pesquisa sobre o Tratado do Alto Mar ou Acordo BBNJ (Acordo sobre a Conservação e Uso Sustentável da Biodiversidade Marinha em Áreas Além da Jurisdição Nacional), destaca o descaso no controle de crimes ambientais em alto mar decorrente da fragilidade regulatória nas áreas além da jurisdição nacional (ABNJ). Aponta dificuldades no âmbito regulatório, institucional e tecnológico existentes antes da ocorrência do acordo implementado pela Organização das Nações Unidas.

A autora revela que a inércia legislativa resultou em uma fragmentação do quadro legal e institucional internacional para a governança do alto mar. Isso favorecia os crimes ambientais marítimos transnacionais como poluição com despejo de lixo, dragagem, extração de recursos, mineração ilegal, mas também a atuação de organizações criminosas por meio do tráfico ilícito de pessoas, narcóticos, armas ou resíduos, ação de piratas, roubos e contrabando de cargas ilícitas. Assim, a área além da jurisdição nacional (ABNJ) era um alvo principal para os crimes transnacionais devido ao quadro legal internacional fracionado e à falta de coordenação e cooperação entre as estruturas de governança e institucionais.

Lothian (2024) ainda cita algumas barreiras institucionais existentes que dificultam uma cooperação e integração como uma estrutura de governança fragmentada onde a proteção das áreas em alto mar era realizada por diversificadas organizações e órgãos globais, regionais e setoriais, cada um com mandatos e prioridades específicos, mas nenhum tendo um foco central.

No tocante à realidade brasileira, Rocha (2020), ao analisar a Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA), considera o surgimento dessa rede de articulação como uma implicação dos entraves institucionais, legais e tecnológicos à governança no contexto do enfrentamento à corrupção e à lavagem de dinheiro. Esses obstáculos resultaram em fragmentação das ações estatais. No âmbito institucional, assegura que antes da ENCCLA ocorria competição e falta de articulação entre as agências que assim não cooperavam, conflito de atribuição entre diversos órgãos, ausência de coordenação estratégica única por parte do Estado, favorecendo a eclosão de ações segmentadas e isoladas. Os entraves legais apontados pelo autor indicam a insuficiência de leis para lidar com a complexidade dos crimes de corrupção, lacunas na legislação já existente e insegurança jurídica. Os obstáculos tecnológicos estão ligados à governança de dados, refletindo a

incapacidade de gerenciar e compartilhar informações de forma eficiente: dificuldade de acesso a bancos de dados, carência de padronização tecnológica, inovação e capacitação para novas tecnologias. A ENCCLA surge para enfrentar essas barreiras e otimizar o combate à crimes complexos.

Amaral, Vargas e Prates (2023) destacam em seus estudos que os obstáculos institucionais à governança estão ligados à cultura organizacional, à gestão de recursos humanos e à falta de coordenação entre as agências onde se observa a existência de ilhas de dados com escassez de integração e compartilhamento de informações, somada à falta de cultura de dados, sendo que esses não são vistos como um ativo institucional capaz de gerar valor. Destacam-se, igualmente, o despreparo e a resistência dos agentes de segurança às novas tecnologias. No que tange às barreiras legais indica a ausência de uma regulação específica para o uso de dados pelas forças de segurança e na proteção dos direitos fundamentais, contribuindo para insegurança jurídica no manejo das informações criminais. Os entraves tecnológicos incluem desde a escassez de equipamentos até a capacidade de processamento, integração e qualificação dos dados, como a ocorrência de desatualização tecnológica, pouca infraestrutura para *big data*, dificuldades no processo de governança, qualidade e gerenciamento para garantir a acurácia dos dados.

Rodrigues (2022) demonstra o funcionamento da interoperabilidade informacional entre o Sistema Brasileiro de Inteligência (Sisbin) e o Ministério Público (MP) analisando o intercâmbio de dados, informações e conhecimentos entre determinadas agências integrantes do Sisbin e o *Parquet* ressaltando sua importância, mas alertando para ausência de normas e regulações para o estabelecimento dessa relação. O autor considera que existem leis esparsas e jurisprudências que norteiam a cooperação com órgãos específicos do Sisbin, como o COAF, no entanto, esclarece que a ausência de um arcabouço legislativo abrangente gera insegurança jurídica e limita a atuação harmônica das instituições dificultando a ampla cooperação entre Inteligência e Ministério Público. A principal barreira institucional é a falta de uma estrutura formal que promova a cooperação coesa entre os órgãos com mecanismos regulatórios que normatizem a interoperabilidade informacional entre o Sisbin e o Ministério Público.

A falta dessa normatização acaba restringindo a atuação desses órgãos e enfraquece o enfrentamento à criminalidade organizada, ao terrorismo e à espionagem. Os obstáculos legais e normativos criam insegurança jurídica e impedem a utilização efetiva dos produtos de Inteligência. Como exemplo do efeito da ausência de base legal tem-se a seguinte situação: se um membro do *Parquet* decidir integrar o conhecimento gerado pelo Sisbin diretamente aos autos de um procedimento judicial, fatalmente sobreviria uma alegação de nulidade processual

pela defesa e o produto de inteligência gerado seria desconsiderado e assim desperdiçado. Em suma, a ausência de um mecanismo institucional que padronize a interoperabilidade é o entrave central, levando a leis esparsas e genéricas que geram insegurança jurídica e restrição no uso de informações vitais para a segurança do Estado (Rodrigues, 2022).

Nunes (2022) considera que as instituições de segurança isoladamente realizam uma diversidade de práticas e ainda sofrem com a falta de mecanismos de colaboração automatizados entre as agências. Ressalta a ocorrência de uma complexidade de dados e de uma heterogeneidade de sistemas, além da indisponibilidade de recursos computacionais. Corroborando com as ideias de Amaral, Vargas e Prates (2023), o autor traz à tona a insegurança jurídica no manejo dos dados provocada por uma incipiente regulação, muitas vezes gerando dúvidas de quais informações podem ser compartilhadas entre as instituições.

Gomes (2022), atribuindo semelhanças com as afirmações estabelecidas por Amaral, Vargas e Prates (2023), considera que os entraves institucionais à governança dos dados criminais estão ligados à cultura organizacional, à disputa de poder e à gestão de recursos humanos. Afirma a existência de uma cultura de isolamento e resistência onde a integração é dificultada pela falta ou diversidade de cultura organizacional e pela resistência interna dos órgãos e de seus integrantes ao esforço cooperativo. Os entraves legais considerados pelo autor estão relacionados à difusão dos dados onde a regulação contribui para o estabelecimento de um dilema entre o segredo e a transparência na vida pública, a fim de promover os direitos e garantias fundamentais dos cidadãos.

Gomes (2022) entende que empecilhos tecnológicos estão ligados à infraestrutura desarticulada e à falha na gestão e compartilhamento de informações essenciais. Antigas práticas dificultam o avanço tecnológico. Dentre essas se pode citar a feudalização ou ilha de dados, multiplicidade de sistemas onde a cooperação é dificultada pela variedade de *softwares* nas mais diversas plataformas computacionais, e pela centralização de dados, informações e sistemas.

Diante das considerações estabelecidas por Gomes (2022), essas barreiras institucionais, legais e tecnológicas, ao dificultar a governança de dados, contribuem para transformar informações estratégicas em recursos isolados e de pouca confiança com inibição do uso e acesso, favorecendo a centralização e o controle, perda e subaproveitamento de dados, persistência no estabelecimento de integrações pontuais e não sistemáticas, favorecimento de relações pessoais em detrimento das relações institucionais na condução das rotinas de procedimentos interinstitucionais. Tudo isso promovendo prejuízo à produção do conhecimento.

Silva (2024) acredita que a fragmentação impede que os dados se transformem em conhecimento de inteligência acionável e eficaz para a tomada de decisão, afetando assim a gestão e produção do conhecimento estratégico. O autor considera que a falta de integração entre os órgãos compromete a eficácia das políticas voltadas para a produção e gestão de informações estratégicas. Silva (2024), assim como Gomes (2022), esclarece que a cooperação entre agências se baseia muito na informalidade e nos contatos pessoais, ao invés de uma estrutura institucionalizada, contribuindo para restrição e perda de informações cruciais e que as barreiras tecnológicas impedem a circulação eficiente de informação. A fragmentação resulta em operações redundantes e sobrepostas, gerando sobreposição de tarefas e retrabalho, ocasionando um uso ineficiente de recursos e ampliando as falhas operacionais.

Silveira (2025) descreve algumas implicações relacionadas a uma ausência de governança de dados criminais ocasionada por barreiras de cunho institucional, legal e tecnológico. Além da baixa qualidade dos dados, outras consequências como a dificuldade de acesso, interpretação e aplicação para a formulação de estratégias eficazes. Fato que corrobora, conforme o autor, na constituição de um sistema de segurança pública que permanece reativo ao invés de proativo. Essa negligência afeta a capacidade do estabelecimento de uma qualidade, acessibilidade e aplicabilidade estratégica dos dados.

A expressão máxima dessas implicações ocorre na Venezuela em um contexto de crise e autoritarismo neopatrimonial quando o Estado fragmentado recorre a alianças com grupos armados como estratégia de sobrevivência frente à percepção de ameaça. Isso permite ao Estado manter um mínimo de governabilidade e controle territorial. Nesse sentido, práticas formais e institucionalizadas são abandonadas e o uso de dados para planejar a segurança é, portanto, substituído por negociações e tolerância de atividades ilegais (como o mercado de drogas) em troca de ordem.

Os entraves institucionais e a fragmentação do Estado fazem com que a informação oficial perca relevância estratégica, sendo substituída por alianças voláteis ocasionando a utilização de pactos ao invés de políticas. A informação e o dado são disponibilizados e transmitidos de forma analógica, sem critérios formais, com foco em interesses particulares. O dado criminal, na verdade, passa a refletir a efetividade de um pacto de tolerância e pacificação, e não a aplicação da lei ou o sucesso de políticas públicas (Zubbilaga, Hanson e Sánchez, 2022).

Com base no estudo descrito, o quadro 7 resume os entraves identificados na bibliografia apresentada.

Autor(es)	Países/Contexto	Natureza dos Entraves	Descrição
Loik (2020)	Reino Unido (UK) e União Europeia (UE) (pós-Brexit)	Legal Institucional	A saída do Reino Unido levou à fragmentação da cooperação, disputa por jurisdição legal e exigências rigorosas de interoperabilidade de dados entre o Reino Unido e a UE. O Reino Unido perdeu o direito de voto em questões da Europol e necessita celebrar acordos de cooperação especiais.
Loik (2020)	Reino Unido (UK) e União Europeia (UE) (pós-Brexit)	Legal Interoperabilidade	O Reino Unido necessita desvincular-se de leis da União Europeia, especialmente no que diz respeito aos direitos fundamentais e compartilhamento de dados internacionais. A governança é travada pela tensão entre o interesse operacional mútuo em combater o terrorismo/crime organizado transnacional e a posição jurídica inflexível da UE em manter a supervisão supranacional sobre direitos fundamentais e proteção de dados.
Rocha (2020)	Brasil (contexto ENCCLA)	Institucional	Antes da ENCCLA, ocorria competição e falta de articulação entre as agências, conflito de atribuição entre diversos órgãos, e ausência de coordenação estratégica única, favorecendo a eclosão de ações segmentadas e isoladas.
Rocha (2020)	Brasil (contexto ENCCLA)	Legal	Insuficiência de leis para lidar com a complexidade dos crimes de corrupção, lacunas na legislação existente e insegurança jurídica.
Rocha (2020)	Brasil (contexto ENCCLA)	Tecnológico	Dificuldade de acesso a bancos de dados, carência de padronização tecnológica, e falta de inovação e capacitação para novas tecnologias.
Amaral, Vargas e Prates (2023)	Brasil (contexto amplo)	Institucional	Obstáculos ligados à cultura organizacional, à gestão de recursos humanos, à falta de coordenação entre agências e à existência de "ilhas de dados". Há uma escassez de integração e compartilhamento de informações, somada à falta de cultura de dados, onde estes não são vistos como um ativo institucional. Observam-se o despreparo e a resistência dos agentes de segurança às novas tecnologias.
Amaral, Vargas e Prates (2023)	Brasil (contexto amplo)	Legal	Ausência de uma regulação específica para o uso de dados pelas forças de segurança e para a proteção dos direitos fundamentais contribui para a insegurança jurídica no manejo das informações criminais.
Amaral, Vargas e Prates (2023)	Brasil (contexto amplo)	Tecnológico	Incluem a escassez de equipamentos, baixa capacidade de processamento, desatualização tecnológica, pouca infraestrutura para <i>big data</i> , e dificuldades no gerenciamento para garantir a acurácia dos dados.
Rodrigues (2022)	Brasil (Sisbin e MP)	Legal / Normativo	Ausência de um arcabouço legislativo abrangente que normatize a interoperabilidade informacional entre Inteligência e Ministério Público. A falta de base legal gera insegurança jurídica e limita a atuação harmônica das instituições, podendo levar à alegação de nulidade processual caso produtos de inteligência sejam integrados diretamente aos autos.
Rodrigues (2022)	Brasil (Sisbin e MP)	Institucional	A principal barreira institucional é a falta de uma estrutura formal com mecanismos regulatórios para promover a cooperação coesa e padronizar a interoperabilidade entre os órgãos.
Nunes (2022)	Brasil (contexto amplo)	Tecnológico	Falta de mecanismos de colaboração automatizados, complexidade de dados, heterogeneidade de sistemas e indisponibilidade de recursos computacionais.
Nunes (2022)	Brasil (contexto amplo)	Legal	Insegurança jurídica no manejo dos dados provocada por uma regulação incipiente, que gera dúvidas sobre quais informações podem ser compartilhadas entre as instituições.

Gomes (2022)	Brasil (contexto amplo)	Institucional	Entraves ligados à cultura organizacional, disputa de poder, gestão de recursos humanos e uma cultura de isolamento e resistência à cooperação.
Gomes (2022)	Brasil (contexto amplo)	Legal	A regulação contribui para um dilema entre o segredo e a transparência na difusão dos dados, com o objetivo de promover os direitos e garantias fundamentais dos cidadãos.
Gomes (2022)	Brasil (contexto amplo)	Tecnológico	Infraestrutura desarticulada, falha na gestão/compartilhamento de informações, "feudalização" ou ilhas de dados, multiplicidade de sistemas e centralização de dados.
Silva (2024)	Brasil (contexto amplo)	Institucional	A fragmentação impede que os dados se transformem em conhecimento de inteligência acionável e eficaz para a tomada de decisão. A cooperação entre agências é baseada na informalidade e em contatos pessoais, em vez de uma estrutura institucionalizada. A fragmentação resulta em operações redundantes, gerando sobreposição de tarefas e retrabalho.
Silva (2024)	Brasil (contexto amplo)	Tecnológico	Barreiras tecnológicas que impedem a circulação eficiente de informação.
Zubbilaga, Hanson e Sánchez (2022)	Venezuela	Institucional Político	Contexto de crise e autoritarismo neopatrimonial, onde o Estado fragmentado recorre a alianças com grupos armados. Práticas formais são abandonadas, e o planejamento da segurança é substituído por negociações e tolerância de atividades ilegais. A informação oficial perde relevância estratégica, sendo substituída por alianças voláteis.
Zubbilaga, Hanson e Sánchez (2022)	Venezuela	Tecnológico Governança	A informação e o dado são disponibilizados de forma analógica, sem critérios formais, com foco em interesses particulares.
Lothian (2024)	Áreas Além da Jurisdição Nacional (ABNJ); Governança do Alto Mar	Legal	Fragilidade Regulatória e Fragmentação do Quadro Legal. A inércia legislativa resultou em um quadro legal internacional fracionado e fragmentado para a governança do alto mar, deixando as ABNJ vulneráveis à criminalidade.
Lothian (2024)	ABNJ; Estruturas de Governança Internacionais	Institucional	Estrutura de Governança Fragmentada e Setorial. A proteção do alto mar era realizada por uma "colcha de retalhos" de organizações e órgãos globais, regionais e setoriais diversificados, cada um com mandatos e prioridades específicos, mas nenhum tendo um foco central na biodiversidade marinha.
Lothian (2024)	ABNJ; Organizações Internacionais	Institucional	Falta de Cooperação e Coordenação. Ausência de um mecanismo global ou abrangente para garantir a coordenação, consistência e coerência das ferramentas de gestão e falta de cooperação entre as estruturas de governança e institucionais
Lothian (2024)	Norte Global vs. Sul Global; ABNJ	Tecnológico	Disparidade Tecnológica. Existência de uma ampla lacuna tecnológica (entre o Norte e o Sul Global), dificultando a pesquisa, a coleta de dados e a fiscalização nas ABNJ [conversação histórica]. O acesso à informação científica e a tecnologia de ponta (como navios de pesquisa e ferramentas in situ) são caros, limitando a capacidade dos Estados em desenvolvimento de monitorar e responder ao crime marítimo.
Lothian (2024)	ABNJ; Agências de Aplicação da Lei Marítima	Tecnológico	Limitações de Capacidade Operacional para Fiscalização. As agências de aplicação da lei marítima carecem de capacidade operacional e de pessoal suficientes, bem como dos equipamentos necessários (embarcações, aeronaves) para realizar monitoramento e vigilância eficazes em alto mar, permitindo que criminosos explorem as lacunas de fiscalização.

Fonte: Dados da pesquisa; Elaboração: Autores, 2025.

3.6 Boas práticas de governança e interoperabilidade

Observa-se hoje um esforço para consolidação do policiamento orientado pela inteligência e, portanto, baseado em evidência. Diante disso, diversas ações a nível estratégico por meio de políticas públicas vêm sendo feitas em uma lenta evolução desde o estabelecimento da Constituição Federal de 1988, intensificando-se nas primeiras décadas do século XXI, com o objetivo de superar a fragmentação institucional e a falta de coordenação no setor de segurança pública. Dentre essas medidas tem-se a criação do Sistema Único de Segurança Pública (SUSP), fundado em 2018 para tentar resolver a fragmentação e promover maior integração entre os diferentes entes federativos, mas ainda enfrenta problemas relacionados à resistência cultural e à falta de interoperabilidade tecnológica.

A criação do Subsistema de Inteligência de Segurança Pública (SISP), instituído pelo Decreto nº 3.695, em 2000; a fundação da Secretaria Nacional de Segurança Pública (SENASP) que é um órgão fundamental para a formulação de políticas públicas mais abrangentes e articuladas em nível federal; o surgimento do Programa Nacional de Segurança com Cidadania (Pronasci), lançado em 2010, este programa marcou um avanço por promover a repressão e a prevenção de crimes em parceria com estados e municípios, utilizando repasses da União. Essa abordagem descentralizada impulsionou a criação de secretarias estaduais e municipais de segurança pública (Silva, 2024).

No que diz respeito às ações de interoperabilidade institucional e operacional, Silva (2024) destaca a implementação do Termo Circunstanciado de Ocorrência (TCO) por Polícias Militares (PM) e Polícia Rodoviária Federal (PRF), simplificando processos burocráticos ao acelerar o atendimento de ocorrências, reduzindo a carga de trabalho das delegacias, assim contribuindo para que as Polícias Judiciárias foquem em investigações mais complexas.

O Ministério da Justiça e Segurança Pública (MJSP) do Brasil é o responsável pela criação e coordenação de diversas redes e sistemas colaborativos que visam integrar esforços entre os entes federativos (União, Estados e Municípios) e outras instituições para enfrentar a criminalidade, alguns desses já citados nesta investigação: Sistema Único de Segurança Pública (SUSP), Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Voz (SINESP), Rede Integrada de Perfis Genéticos, Rede Nacional de Altos Estudos em Segurança Pública.

Criou a principal rede colaborativa interinstitucional, no ano de 2003, que é a ENCCLA: um modelo de rede interorganizacional criado para superar a fragmentação institucional e otimizar o uso da informação no enfrentamento a crimes complexos: combate à corrupção,

combate à lavagem de dinheiro, recuperação de ativos, enfrentamento a organizações criminosas (em sua vertente financeira). Registra mais de 90 instituições participantes oriundas dos Poderes Executivo, Legislativo, Judiciário, Ministério Público, Forças Policiais, Controladorias e Órgãos Reguladores como Conselho de Controle de Atividades Financeiras (Coaf), Advocacia-Geral da União (AGU), Controladoria-Geral da União (CGU), Receita Federal do Brasil (RFB), Polícia Federal (PF), Banco Central do Brasil (BCB) Conselho Nacional de Justiça (CNJ), Superior Tribunal de Justiça (STJ), Tribunais de Justiça e Federais, Ministério Público Federal (MPF), Ministério Público do Trabalho (MPT), Ministério Público de Contas (MPC), e diversos Ministérios Públicos Estaduais, Tribunal de Contas da União (TCU) e Tribunais de Contas Estaduais (TCEs), associações de classes (como a FEBRABAN), entidades do sistema de justiça, Banco do Brasil, entre outros (Brasil, 2022).

Por meio de plenária, definem ações anuais e a partir de então cria-se grupo de trabalho composto por múltiplos especialistas dos órgãos envolvidos. Esses grupos realizam estudos, diagnósticos, elaboram propostas legislativas, soluções em Tecnologia da Informação (TI) e outros produtos concretos. As decisões e o desenvolvimento dos trabalhos são acompanhados por instâncias de governança, como o Gabinete de Gestão Integrada (GGI), e são baseados em consenso. Ao final do ciclo, os resultados e produtos são compartilhados com o conjunto de participantes e com a sociedade (Brasil, 2022).

De acordo com Rocha (2020), na ENCCLA, a interoperabilidade é alcançada por meio da criação de sistemas eletrônicos integrados e da padronização de procedimentos, dinamizando o fluxo e o compartilhamento de informações entre as agências de repressão e controle. Destacam-se sistemas como Sistema de Investigação de Movimentações Bancárias (SIMBA), amplamente utilizado por mais de 80 instituições (Polícia Federal, Ministério Público, Polícias Civis, Justiça do Trabalho, TSE), demonstrando alta interoperabilidade tecnológica para investigações financeiras complexas, além do Cadastro de Clientes do Sistema Financeiro Nacional (CCS) que é mantido pelo Banco Central (Bacen). O CCS permite que autoridades requisitem a identificação das instituições financeiras com as quais um investigado mantém relacionamento. A capacitação também é uma preocupação em que as ações são concretizadas conforme o Programa Nacional de Capacitação e Treinamento (PNLD), que é um programa integrado e contínuo de formação de agentes públicos sobre temas prioritários (corrupção, lavagem de dinheiro, cooperação jurídica internacional), disseminando o conhecimento e fortalecendo a atuação em rede.

Ainda no contexto dos crimes financeiros, a Rede Nacional de Laboratórios de Tecnologia contra Lavagem de Dinheiro (REDE-LAB) destaca-se como um importante avanço

na promoção da interoperabilidade institucional e informativa de esfera nacional e interinstitucional. É um programa estratégico para a articulação e o combate a crimes financeiros complexos no Brasil, com um forte foco na interoperabilidade e no uso de tecnologia. Criado em 2014, pela Portaria SNJ nº 242, de 29 de setembro de 2014, surge da necessidade de integração e articulação institucional após a replicação bem-sucedida dos Laboratórios de Tecnologia contra Lavagem de Dinheiro (LAB-LD). Em 2022, a rede foi reestruturada pela Portaria MJSP nº 145, de 15 de agosto de 2022, tornando-se um programa permanente de Articulação Institucional do Ministério da Justiça e Segurança Pública (MJSP), sendo atualmente composta por 64 unidades LAB-LD, incluindo a Polícia Federal, o Ministério Público Federal, o Ministério Público Militar e as Polícias Civis e Ministérios Públicos das 27 unidades federativas (Brasil, 2014; 2022).

O programa funciona como um ambiente de cooperação e compartilhamento, buscando aperfeiçoar a atuação dos Laboratórios de Tecnologia contra a Lavagem de Dinheiro (LAB-LD). Nesse sentido, a operacionalização está pautada no compartilhamento de informações técnicas, padronização, compatibilização de tecnologias, interoperabilidade tecnológica/padronização entre as unidades. Os objetivos consistem na busca de desenvolver e aplicar métodos e técnicas para produzir informações a partir de grandes volumes de dados, elaborar e difundir estudos sobre melhores práticas na produção de informações, estabelecendo metodologias, tecnologias e perfis profissionais ideais, apoiar as medidas tecnológicas necessárias para a análise de grandes volumes de dados junto a órgãos federais e estaduais, promover pesquisas e adquirir tecnologias de ponta em análise de dados, buscando o aprimoramento constante dos recursos tecnológicos utilizados, produzir informações, dados, estatísticas e conhecimento sobre o combate à lavagem de dinheiro no país (Brasil, 2014; 2022).

Embora todo empecilho causado pela lacuna legislativa no estabelecimento da interoperabilidade informacional entre o Ministério Público e o Sistema Brasileiro de Inteligência (SISBIN), já demonstrado anteriormente, a atuação cooperativa dessas duas entidades continua a acontecer gerando boas práticas de governança institucional como as seguintes: estruturação de unidades especializadas como Grupo Nacional de Combate às Organizações Criminosas (GNCO), instituído em 2002, para troca de informações e operações interestaduais e nacionais contra o crime organizado; criou o Sistema Nacional de Segurança Institucional do Ministério Público (SNS/MP) em 2016 com foco na Contra-inteligência, adotando uma atuação preventiva e proativa para antecipar ameaças e proteger os ativos informacionais; Conseguiu a regulamentação do Compartilhamento de Dados entre Agências de Inteligência (Sisbin) que passou a ocorrer mediante solicitação devidamente motivada,

comprovação do interesse público e afastamento de qualquer uso privado, exigindo instauração formal de procedimento e a existência de sistemas eletrônicos de segurança e registro de acesso; atuação subsidiária da inteligência na persecução penal onde a atuação da Inteligência passa a ser subsidiária ao órgão ministerial quando as investigações forem lideradas pelo membro do *Parquet*; compartilhamento de relatório de inteligência financeira do COAF diretamente para o Ministério Público sem precisar de autorização judicial, porém estabelecidos por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e instrumentos de apuração de desvios. A interoperabilidade informacional entre agências de Inteligência em Segurança Pública e o MP Estadual se materializa por meio de Relatório Técnico (Rodrigues, 2022).

Araújo Filho e Ishikawa (2025) relatam inovação ligada a governança e interoperabilidade trazendo iniciativa do Poder Judiciário brasileiro de utilizar a Governança Digital e técnicas avançadas para superar os desafios da investigação patrimonial e da recuperação de ativos. Sendo uma política institucional estabelecida através de um plano estratégico chamado de Estratégia Nacional do Poder Judiciário (2021-2026) instituída pelo Conselho Nacional de Justiça (CNJ), que reconhece a necessidade de aprimorar a gestão administrativa e a governança judiciária. Diante disso, cria-se uma heurística investigativa otimizando a mineração de dados em registros públicos do Cadastro Nacional de Pessoas Jurídicas (CNPJ) submetendo-os à análise de vínculos por meio da modelagem de grafos facilitando a descoberta de grupos econômicos que cometem infrações financeiras.

Nunes (2022) propõe o desenvolvimento de uma plataforma de *middleware* no contexto da segurança pública do Rio Grande do Norte, visando conectar sistemas heterogêneos para melhorar o atendimento a crimes contra a vida. O trabalho foi desenvolvido em parceria com o ITEP-RN e teve como objetivo geral promover a interoperabilidade entre os sistemas das forças de segurança do Estado do Rio Grande do Norte. Para criação do artefato, princípios de governança digital e interoperabilidade tecnológica fundamentaram as atividades. O projeto focou em criar interoperabilidade entre os sistemas de três órgãos distintos: o ITEP (Instituto Técnico-Científico de Perícia), a DHPP (Divisão de Homicídios e Proteção à Pessoa, da Polícia Civil) e o CIOSP (Centro Integrado de Operações de Segurança Pública). Os sistemas específicos integrados na solução foram o SIGEP (Sistema Integrado de Gestão de Perícias do ITEP), o CAD-RN (Central de Atendimento e Despacho do Rio Grande do Norte) e o ACC (Assistente de Cena de Crime da DHPP).

Amaral, Vargas e Prates (2023) relacionam algumas ações que integram dados, plataformas e exigem interação entre instituições distintas. Nessa perspectiva, relata a criação

dos Centros de Comando e Controle Integrado (CICC) como o CICC no Rio de Janeiro com a intenção de ser um sistema integrado. O CICC-BF (na Baixada Fluminense) é integrado à rede nacional de dados do Ministério da Justiça, permitindo a agilidade e racionalização de medidas operacionais conjuntas entre diversos órgãos. No estado de São Paulo observa-se o uso de Cercamento eletrônico por meio de Optical character Recognition (OCR) usado em câmeras de videomonitoramento integrado nas cidades para leitura de placas de veículos. A tecnologia permite o cruzamento de informações com o banco de dados da polícia para identificar irregularidades ou ocorrências (como furtos ou roubos), emitindo alertas em tempo real.

No Ceará é utilizada uma plataforma de inteligência artificial que integra diversos bancos de dados com mapas e imagens: o sistema Agilis, aplicado ao Núcleo de Videomonitoramento (Nuvid), cruza dados de 3.300 câmeras com vários bancos para identificar veículos roubados ou utilizados em ações criminosas. Ainda no Ceará, outra ferramenta, o Status, aplica ciência de dados, estatística e geoprocessamento para determinar a "mancha criminal", através da análise de dias e horários de maior incidência de crimes (Amaral; Vargas; Prates, 2023)

O Compartilhamento Informacional via SINESP (Sistema Nacional de Informações de Segurança Pública) é citado como um sistema que possibilita a integração de bases de dados de todo o Brasil, permitindo que a força policial utilize esses dados na análise da atividade criminal, acessando fichas criminais, boletins de ocorrências e informações sobre focos de criminalidade, superando as fronteiras estaduais. Não se deve deixar de apontar as tecnologias de captura para cruzamento como drones, utilizados para filmagem, monitoramento de áreas de risco e georreferenciamento, e câmeras corporais (*bodycams*), também geram dados que, se bem integrados, podem otimizar o tempo de trabalho e aumentar a confiança pública (Amaral; Vargas; Prates, 2023)

A providência, até então, mais recentemente implementada pelo executivo federal na esfera da interoperabilidade informacional e tecnológica foi a criação do Sistema Nacional de Inteligência para Enfrentamento ao Crime Organizado (Orcrim). Criado com fundamento nas seguintes normativas: Lei nº 14.600/2023, no Decreto nº 11.348/2023 e na Lei nº 13.675/2018, o Orcrim é definido como um sistema de informação composto por dados de inteligência relevantes para o enfrentamento das organizações criminosas. A governança do sistema está atribuída ao Ministério da Justiça e Segurança Pública, por intermédio da Secretaria Nacional de Segurança Pública (SENASP), competindo a essa definir normas e procedimentos para a metodologia de tratamento dos dados, gestão, adesão, governança, manutenção e utilização do Sistema Nacional de Inteligência para Enfrentamento ao Crime Organizado (Orcrim). Os

principais objetivos do sistema são: aprimorar a qualidade e a fidedignidade dos dados utilizados no combate ao crime organizado; promover integração em ações estratégicas, operacionais e de inteligência; viabilizar interoperabilidade entre sistemas e bancos de dados; integrar informações de diferentes agências de segurança pública; incentivar ações permanentes de enfrentamento às organizações criminosas; definir metodologia de compartilhamento entre forças de segurança (Brasil, 2025).

O Orcrim poderá ser compartilhado entre as Agências de Inteligência de diversos órgãos, incluindo: Secretaria Nacional de Segurança Pública (Senasp), Polícia Federal, Polícia Rodoviária Federal, Secretaria Nacional de Políticas Penais, Secretarias Estaduais de Segurança Pública, Polícias Civis. A portaria também permite que outras agências com atuação no combate ao crime organizado ingressem no sistema, desde que apresentem fundamentação técnica. Os dados terão acesso restrito, seguindo normas da Portaria nº 880/2019, e fica proibida a inserção direta das informações do sistema em inquéritos ou procedimentos judiciais. Com isso revoga-se a Portaria MJSP nº 115, de 13 de março de 2020, que tratava de diretrizes anteriores sobre inteligência de segurança pública e estabelece-se um regimento atual com princípios de governança e cooperação interinstitucional e interoperabilidade focada na Inteligência Policial (Brasil, 2025).

Diante do exposto, observa-se a existência de algumas ações que contribuem para a dinamização da governança de dados criminais no Brasil. Práticas realizadas nas diferentes instâncias federativas: municipal, estadual e federal poderiam ser explicitadas como o Sistema Autua (Federal), Captura (Federal) e o MOP (Mobilidade em Operações Policiais), dentre outros que possuem como princípio a interoperabilidade como fomento para otimização da governança de dados e melhoria da qualidade da segurança pública. No entanto, devido a limitações, foram destacados esses que foram expostos, os quais serão resumidos no quadro 8.

Quadro 8 - Boas práticas de governança e interoperabilidade

Natureza	Ação	Entidade Responsável/Participante	Importância ou Função
Governança Institucional/Política Pública	Criação do Sistema Único de Segurança Pública (SUSP)	Ministério da Justiça e Segurança Pública (MJSP)	Tenta resolver a fragmentação e promove maior integração entre os diferentes entes federativos.
Governança Federal/Política Pública	Fundação da Secretaria Nacional de Segurança Pública (SENASP)	Ministério da Justiça e Segurança Pública (MJSP)	Órgão fundamental para a formulação de políticas públicas mais abrangentes e articuladas em nível federal.
Governança/Inteligência	Criação do Subsistema de	Ministério da Justiça e Segurança Pública (MJSP)	Visa a consolidação do policiamento orientado pela

	Inteligência de Segurança Pública (SISP)		inteligência e baseado em evidência.
Governança em Rede/Combate a Crimes Complexos	Criação da ENCCLA (Rede Colaborativa Interinstitucional com mais de 90 instituições)	Ministério da Justiça e Segurança Pública (MJSP)	Modelo criado para superar a fragmentação institucional e otimizar o uso da informação no enfrentamento a crimes complexos, como combate à corrupção e lavagem de dinheiro.
Governança Informacional/Articulação Institucional	Criação da Rede Nacional de Laboratórios de Tecnologia contra Lavagem de Dinheiro (REDE-LAB)	Ministério da Justiça e Segurança Pública (MJSP)	Programa estratégico para a articulação e o combate a crimes financeiros complexos, buscando o compartilhamento de metodologias e a compatibilização de tecnologias entre as 64 unidades (LAB-LD).
Governança/Interoperabilidade Informacional	Criação do Sistema Nacional de Inteligência para Enfrentamento ao Crime Organizado (Orcrim)	Ministério da Justiça e Segurança Pública (MJSP), por intermédio da SENASP	Aprimorar a qualidade e a fidedignidade dos dados, promover integração em ações estratégicas, viabilizar interoperabilidade entre sistemas e bancos de dados, e definir metodologia de compartilhamento entre forças de segurança.
Governança Institucional/Contraineligência	Criação do Sistema Nacional de Segurança Institucional do Ministério Público (SNS/MP)	Ministério Público (MP)	Foca na Contraineligência, adotando uma atuação preventiva e proativa para antecipar ameaças e proteger os ativos informacionais.
Governança Informacional/Compartilhamento	Regulamentação do Compartilhamento de Dados entre Agências de Inteligência (Sisbin)	Ministério Público e Sistema Brasileiro de Inteligência (SISBIN)	Exige que o compartilhamento ocorra mediante solicitação devidamente motivada, comprovação do interesse público e afastamento de uso privado.
Governança Digital/Investigação Patrimonial	Uso da Governança Digital e técnicas avançadas (mineração de dados, modelagem de grafos)	Poder Judiciário brasileiro (Conselho Nacional de Justiça - CNJ)	Visa superar os desafios da investigação patrimonial e da recuperação de ativos, otimizando a mineração de dados em registros públicos para facilitar a descoberta de grupos econômicos que cometem infrações financeiras.
Interoperabilidade Institucional/Operacional	Implementação do Termo Circunstanciado de Ocorrência (TCO)	Polícias Militares (PM) e Polícia Rodoviária Federal (PRF)	Simplifica processos burocráticos ao acelerar o atendimento de ocorrências, reduzindo a carga de trabalho das delegacias, e permitindo que as Polícias Judiciárias foquem em investigações mais complexas.
Interoperabilidade Tecnológica (Investigação Financeira)	Utilização do Sistema de Investigação de Movimentações	Mais de 80 instituições (Polícia Federal, Ministério Público,	Demonstra alta interoperabilidade tecnológica para investigações financeiras complexas.

	Bancárias (SIMBA)	Polícias Cíveis, Justiça do Trabalho, TSE)	
Interoperabilidade Tecnológica (Regional)	Desenvolvimento de plataforma de middleware para conectar sistemas heterogêneos	Forças de segurança do Rio Grande do Norte (ITEP-RN, DHPP, CIOSP)	Promover a interoperabilidade entre os sistemas das forças de segurança do Estado do Rio Grande do Norte (SIGEP, CAD-RN e ACC), visando melhorar o atendimento a crimes contra a vida.
Interoperabilidade Operacional/Integração	Criação dos Centros de Comando e Controle Integrado (CICC)	Diversos órgãos (integrados à rede nacional de dados do MJSP, ex: Rio de Janeiro)	Ser um sistema integrado que permite a agilidade e racionalização de medidas operacionais conjuntas entre diversos órgãos.
Interoperabilidade Informacional (Nacional)	Compartilhamento Informacional via SINESP (Sistema Nacional de Informações de Segurança Pública)	Sistema Nacional (coordenado pelo MJSP)	Possibilita a integração de bases de dados de todo o Brasil, permitindo que a força policial utilize esses dados na análise da atividade criminal e na superação das fronteiras estaduais.
Interoperabilidade Tecnológica/Monitoramento	Uso de Cercamento eletrônico por meio de Optical Character Recognition (OCR)	Estado de São Paulo	Permite a leitura de placas de veículos e o cruzamento de informações com o banco de dados da polícia para identificar irregularidades (furtos ou roubos), emitindo alertas em tempo real.
Interoperabilidade/Inteligência Artificial	Utilização do sistema Agilis	Ceará (aplicado ao Núcleo de Videomonitoramento - Nuvid)	Integra diversos bancos de dados com mapas e imagens, cruzando dados de 3.300 câmeras para identificar veículos roubados ou utilizados em ações criminosas.

. Fonte: Dados da pesquisa; Elaboração: Autores, 2025

A nível internacional o mais recente acordo de segurança marítima promovido pela Organização das Nações Unidas (ONU) exemplifica as recentes diretrizes e ações adotadas mundialmente para cooperação interestatal. Lothian (2024) descreve inúmeras medidas adotadas oriundas do Acordo de Alto-mar ou Acordo BBNJ (Acordo sobre a Conservação e o Uso Sustentável da Biodiversidade Marinha em Áreas Além da Jurisdição Nacional) que buscam superar a fragmentação do direito marítimo internacional e a falta de coordenação na proteção da biodiversidade e no combate ao crime ambiental transnacional marítimo. O acordo BBNJ enfatiza a integração e a articulação global, regional e setorial, buscando reforçar e promover a cooperação e a coordenação onde o novo regime proposto atem em parceria com regimes legais existentes, contribuindo para o fortalecimento e a coerência entre as medidas existentes.

A interoperabilidade é viabilizada pelo compartilhamento de dados seguida pela melhoria da infraestrutura de transferência de tecnologia no intuito de reduzir a disparidade tecnológica entre o norte global e o sul global. Para isso criou uma ferramenta de compartilhamento de dados na modalidade de *Clearing-House Mechanism* (Mecanismo de compensação) para aprimorar a infraestrutura e transmissão e garantir acesso equitativo aos dados. Funciona como um *hub* central que fornecerá *links* para outros mecanismos *clearing-house*, repositórios e bases de dados. O CHM centraliza a plataforma para que as partes possam acessar, fornecer e disseminar informações sobre dados, conhecimento científico marinho e pesquisa. Além disso, facilitará a cooperação científica e técnica conectando usuários em um ambiente colaborativo (Lothian, 2024).

Mais especificamente voltados para interoperabilidade na atividade policial, alguns sistemas e redes têm o objetivo de padronizar procedimentos, integrar informações e coordenar operações policiais em nível nacional. Os sistemas e redes de integração da segurança pública com a atividade policial contidos nas fontes podem ser resumidos no quadro 9, detalhando suas siglas e focos principais:

Quadro 9: Segurança Pública e Integração Policial

Rede/Sistema	Sigla	Foco Principal
Sistema Único de Segurança Pública	SUSP	Estrutura nacional que visa integrar as ações de segurança pública dos entes federados (União, Estados e Municípios) e as forças policiais, alinhando políticas e recursos.
Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Voz	SINESP	Plataforma tecnológica central que coleta, processa e integra dados de segurança pública, judiciário e sistema prisional, sendo crucial para o SUSP.
Rede Integrada de Perfis Genéticos	RIBPG	Coleta, armazenamento e cruzamento de perfis genéticos de vestígios de crimes e de condenados, essenciais para investigações criminais.
Rede Nacional de Altos Estudos em Segurança Pública	RENAESP	Promove a formação continuada e o desenvolvimento de estudos e pesquisas para aprimorar a atuação dos profissionais de segurança pública.
Rede Nacional de Enfrentamento às Organizações Criminosas	RENOCRIM	Foca no desenvolvimento e compartilhamento de estratégias para identificar, dismantelar e combater as organizações criminosas interestaduais.
Programa Captura	-	Articulação nacional para identificar, localizar e prender criminosos considerados de alta periculosidade, com foco em foragidos estratégicos ligados a organizações criminosas.

Fonte: Dados da pesquisa; Elaboração: Autores, 2025

Em síntese, os resultados desta revisão evidenciam que as respostas à fragmentação de dados, quando formuladas como diretrizes e mecanismos de cooperação, tendem a combinar

dois movimentos complementares: a criação de arranjos institucionais voltados à coordenação entre atores e níveis, e o desenvolvimento de infraestruturas e dispositivos de compartilhamento capazes de reduzir assimetrias tecnológicas e ampliar a circulação de informações. O exemplo internacional do Acordo BBNJ, ao enfatizar integração, coerência entre regimes e a operacionalização do compartilhamento por meio de um mecanismo do tipo Clearing-House, ilustra um princípio relevante para o debate deste estudo: interoperabilidade não é apenas conectividade entre sistemas, mas resultado de desenho institucional e de instrumentos que viabilizam acesso, disseminação e cooperação técnico-científica em bases compartilhadas (Lothian, 2024).

No recorte nacional, a sistematização de sistemas e redes direcionadas à integração policial e à coordenação da segurança pública (Quadro 8) reforça que existem arquiteturas e iniciativas voltadas à padronização e à integração de dados e operações, ainda que sua efetividade dependa de condições de governança e de implementação no interior do arranjo interorganizacional.

Na seção seguinte, esses achados serão discutidos de forma interpretativa e crítica, conectando-os à pergunta de pesquisa e ao referencial teórico do artigo, de modo a explicitar convergências, tensões e implicações para a governança de dados criminais e para a efetividade da análise criminal.

4. DISCUSSÃO

Esta pesquisa investigou em que medida a fragmentação de dados criminais entre órgãos do sistema de defesa social compromete a governança de dados e, por consequência, a efetividade da análise criminal, assumindo como objetivo geral analisar os impactos dessa fragmentação sobre os fluxos informacionais e decisórios do campo.

Nesta seção, os achados da revisão integrativa são interpretados criticamente à luz do referencial que o próprio artigo constrói: de um lado, a centralidade estratégica dos dados e sua dimensão de soberania e segurança (Cassiolato, 2025; Siqueira, 2025; Cristóvam & Souza, 2024) e, de outro, a lente da Governança Multinível aplicada à ação pública e aos fluxos informacionais (Freire, 2021; Kempner-Moreira, Freire & Souza, 2022; Nunes, 2025).

A discussão se organiza por eixos analíticos coerentes com os resultados e com os objetivos específicos: fragmentação e Governança Multinível; entraves institucionais, tecnológicos e legais; impactos na efetividade da análise criminal; e, por fim, boas práticas e modelos de interoperabilidade, culminando na integração teórica e na contribuição do estudo.

Eixo 1: Fragmentação de dados e Governança Multinível

Os resultados convergem ao indicar que a fragmentação de dados criminais é um fenômeno estruturante, persistente e historicamente condicionado, caracterizado por baixa interoperabilidade entre instituições e ausência de padronização de registros e classificações, o que produz redundâncias, lacunas e inconsistências que degradam a confiabilidade informacional (Lima, 2008; Durante, 2009; Lira, Caballero & Nascimento, 2022). Essa configuração não pode ser lida apenas como lacuna operacional, uma vez que a efetividade da ação pública depende da articulação de fluxos decisórios e informacionais entre diferentes níveis e atores. No campo da segurança pública, tal premissa se torna ainda mais sensível, dado o caráter interorganizacional e federativo do setor (Kempner-Moreira, Freire & Souza, 2022; FBSP, 2024).

Assim, decisões e rotinas de produção, circulação e uso de dados não se alinham entre instâncias e organizações, gerando um descompasso entre o volume de informações disponíveis e sua conversão em inteligência institucional utilizável (Lima, 2008; Durante, 2009).

Sob a lente da Governança Multinível, a evidência mais robusta dos resultados é a tensão entre modelos normativos de integração, que pressupõem coordenação, padrões e mecanismos estáveis de cooperação, e um arranjo empírico no qual “ilhas de dados”, competição institucional e baixa institucionalização do compartilhamento permanecem como traços recorrentes (Amaral, Vargas & Prates, 2023; Lima, 2008).

Essa tensão é particularmente visível quando se observa que, mesmo em cenários de modernização tecnológica e difusão de soluções de *big data*, a governança continua “travada” pela fragmentação institucional, com bancos separados, pouca comunicação e retrabalho, o que limita a transição de respostas reativas para respostas preventivas e orientadas por evidências (Amaral, Vargas & Prates, 2023). Isso reforça a premissa de que interoperabilidade e integração não são propriedades automáticas do sistema técnico, são realizações de governança, dependentes de pactos multiníveis e de mecanismos institucionais de coordenação.

Além disso, há uma ampliação epistemológica ao propor a lente da Governança Multinível de Dados (MultiGov-Data), visto que a literatura sobre governança de dados na administração pública tende a privilegiar dimensões técnicas e tecnológicas, negligenciando fatores sociopolíticos e culturais que condicionam a efetividade da governança (Neves, 2024; Zilli, 2022). A leitura dos resultados sustenta esse deslocamento: a fragmentação aparece como sistema de interdependências entre atores, níveis e políticas, e não como falha localizada de

ferramenta, o que torna a explicação mais aderente à complexidade institucional do SUSP e do sistema de defesa social (Freire, 2021; Kempner-Moreira, Freire & Souza, 2022; Nunes, 2025).

Eixo 2: Entraves institucionais, tecnológicos e legais

No eixo dos entraves, os resultados apontam que a fragmentação se sustenta por um conjunto articulado de barreiras, que não operam em paralelo, mas se reforçam mutuamente. No plano institucional, sobressaem a competição e a falta de articulação entre agências, conflitos de atribuição e ausência de coordenação estratégica única, favorecendo ações segmentadas e isoladas (Rocha, 2020).

Em contexto brasileiro mais amplo, os estudos revisados também associam o problema da cultura organizacional, gestão de recursos humanos, despreparo e resistência dos agentes às novas tecnologias, além da persistência de “ilhas de dados”, indicando que a fragmentação é, simultaneamente, produto e reforço de arranjos organizacionais que não internalizam o dado como ativo institucional (Amaral, Vargas & Prates, 2023).

Essa dimensão institucional tem implicações diretas para a governança, entendida como conjunto de princípios, estruturas e mecanismos voltados a garantir qualidade, integridade e uso responsável do conhecimento nas organizações (Silva, Couto & Freire, 2017). Quando a cooperação se mantém como informalidade baseada em contatos pessoais e não como estrutura institucionalizada, a fragmentação limita a conversão de dados em inteligência acionável, produzindo redundâncias, sobreposição de tarefas e retrabalho (Silva, 2024).

Nesse sentido, os resultados corroboram o argumento de que a governança de dados criminais, para além de arquitetura tecnológica, é mecanismo estruturante de eficiência pública: sua ausência impede o salto de uma gestão informacional dispersa para um regime de coordenação que sustente práticas analíticas orientadas por evidências (Freire, 2021; Kempner-Moreira, Freire & Souza, 2022; Nunes, 2025; Boba, 2005; Azevedo, Riccio & Ruediger, 2011).

No plano tecnológico, as barreiras incluem infraestrutura desarticulada, multiplicidade de sistemas, centralização assimétrica e “feudalização” informacional, que se traduzem em ilhas de dados e falhas na gestão e no compartilhamento de informações (Gomes, 2022). Os resultados também apontam dificuldades de acesso a bases, carência de padronização tecnológica e lacunas de inovação e capacitação, o que compromete a circulação eficiente da informação e a interoperabilidade (Rocha, 2020; Silva, 2024).

Ou seja, a tecnologia aparece como condição necessária, mas não suficiente. A heterogeneidade de sistemas e a baixa padronização reproduzem, no plano técnico, as

descoordenações do plano institucional, de modo que soluções digitais podem consolidar a fragmentação quando implementadas sem engenharia de governança.

No plano legal, os resultados indicam um duplo movimento. Por um lado, há avanço do marco normativo geral de proteção de dados e consolidação do direito fundamental à proteção de dados pessoais, com repercussões relevantes para a segurança pública (Amaral, Vargas & Prates, 2023). Por outro, persistem insuficiência de leis para lidar com a complexidade de determinados crimes e, sobretudo, lacunas e insegurança jurídica quanto ao manejo e ao compartilhamento de informações, o que tende a elevar custos percebidos de cooperação e estimular práticas defensivas de retenção de dados (Rocha, 2020; Amaral, Vargas & Prates, 2023).

A implicação é que o problema é técnico, institucional, jurídico e cultural ao mesmo tempo. Embora a LGPD (Lei nº 13.709/2018) excetue o tratamento de dados para fins de segurança pública, a ausência de uma legislação específica gera inseguranças interpretativas no intercâmbio prático de informações. Sem clareza operacional e salvaguardas padronizadas, essa tensão eleva os custos percebidos da cooperação e estimula práticas defensivas de retenção de dados por parte das instituições, que temem a ineficácia prática das ações em razão de nulidades, aprofundando assim a fragmentação.

Eixo 3: Impactos na efetividade da análise criminal

Os resultados sustentam que a fragmentação compromete a efetividade da análise criminal sobretudo por degradar a qualidade e a confiabilidade dos dados que alimentam diagnósticos e decisões. No período de institucionalização de políticas baseadas em análise criminal e uso sistemático de dados, consolidou-se a ideia de que respostas mais eficientes dependem de coleta, organização, análise e interpretação de dados voltadas ao planejamento de ações e políticas (Silveira, 2024; Senasp, 2021). Contudo, quando a produção e o tratamento de dados permanecem fragmentados, a análise se desloca do uso estratégico para a administração de inconsistências, lacunas e dificuldades de acesso, reduzindo sua capacidade de orientar inteligência e prevenção (Lima, 2008; Durante, 2009; Silveira, 2025).

Esse impacto aparece também como problema de “cadeia de confiança” informacional. Ainda que a alta gestão passe a reconhecer o dado como ativo organizacional capaz de gerar valor e subsidiar ações estratégicas, a ausência de cultura de dados e de processos de governança e qualidade faz com que a coleta massiva se converta em informação de baixa utilidade analítica (Amaral, Vargas & Prates, 2023).

Nessa direção, os resultados enfatizam que interoperabilidade implica linguagem comum e condições para leitura e uso interinstitucional, especialmente diante da disparidade tecnológica entre organizações e unidades federativas (Amaral, Vargas & Prates, 2023). Assim, a fragmentação não é apenas “falta de integração”; ela implica perda de integridade, dificuldade de interpretação e baixa aplicabilidade estratégica, mantendo a segurança pública em dinâmica reativa, em vez de orientada por evidências e proatividade (Silveira, 2025).

Em síntese, a fragmentação interfere diretamente na qualidade, confiabilidade e integridade das informações para tomada de decisão estratégica: ela reduz comparabilidade, dificulta construção de séries e estatísticas integradas e fragiliza a capacidade de produzir conhecimento acionável para coordenação e accountability, pilares associados à governança orientada por evidências (Boba, 2005; Azevedo, Riccio & Ruediger, 2011). Ou seja, melhorar a análise criminal exige tratar a governança de dados como infraestrutura institucional e não como etapa posterior à implantação de sistemas.

Eixo 4: Boas práticas e modelos de interoperabilidade

Os resultados também identificam repertórios de integração e interoperabilidade, em escalas e domínios distintos, que ajudam a pensar caminhos de mitigação da fragmentação. Um exemplo conceitual de arquitetura voltada a reduzir assimetrias de acesso e apoiar cooperação técnica é a proposta de mecanismos de compensação e hubs colaborativos para compartilhamento e disseminação de informação, como discutido em arranjos de governança internacional (Lothian, 2024).

Embora não seja um caso de segurança pública doméstica, esse tipo de desenho ilumina um princípio relevante: interoperabilidade depende de infraestrutura comum, regras de acesso e incentivos à cooperação, elementos que se aproximam das exigências multiníveis que o artigo discute para o campo da segurança.

No recorte da segurança pública, os resultados sistematizam sistemas e redes voltados a padronizar procedimentos, integrar informações e coordenar ações em nível nacional, destacando o SUSP como estrutura de integração federativa e o SINESP como plataforma tecnológica central de coleta, processamento e integração de dados de segurança pública, justiça e sistema prisional.

No entanto, a existência de estruturas como o SUSP e plataformas como o SINESP não resolve automaticamente a fragmentação. As potencialidades dessas redes (como a padronização técnica e o compartilhamento de metodologias da REDE-LAB) muitas vezes

esbarram em limites institucionais severos. Na prática, a eficácia dessas iniciativas encontra limites na dependência de relações interpessoais informais, na competição interagências e na falta de uma cultura de compartilhamento consolidada. Ou seja, sem institucionalização de rotinas, governança de qualidade e clareza jurídico-organizacional sobre o compartilhamento, tais iniciativas podem operar aquém do potencial, mantendo a integração como projeto e não como prática consolidada (Freire, 2021; Kempner-Moreira, Freire & Souza, 2022; Nunes, 2025).

Os resultados também sugerem que a adaptação e o fortalecimento de boas práticas devem considerar capacidades institucionais e cultura de cooperação. A literatura revisada aponta que, onde a cooperação é informal e dependente de relações pessoais, a inteligência se torna frágil e sujeita a volatilidades; onde há estrutura institucionalizada, padrões e interoperabilidade, há maior chance de transformar dados em conhecimento acionável (Silva, 2024). Em termos práticos, isso implica reconhecer que interoperabilidade é simultaneamente tecnológica e política: requer engenharia institucional (coordenação e accountability), engenharia técnica (padrões e integrações) e engenharia jurídica (salvaguardas operacionais), sob pena de reproduzir a fragmentação em novas camadas de sistemas. O Quadro 10 sistematiza as discussões por eixo.

Quadro 10 - Síntese das discussões por eixo e principais autores

Eixo	Síntese	Implicação	Autores (ano)
Eixo 1 – Fragmentação de dados e Governança Multinível	A fragmentação se apresenta como fenômeno estruturante e historicamente condicionado, expresso em baixa interoperabilidade, ausência de padronização e produção de inconsistências que degradam a confiabilidade informacional. A leitura multinível evidencia tensão entre modelos normativos de integração e um arranjo empírico persistente de “ilhas de dados” e baixa institucionalização do compartilhamento. A proposta MultiGov-Data reforça que o fenômeno não se explica por “falha de ferramenta”, mas por interdependências sociopolíticas, culturais e federativas que travam a governança mesmo diante de modernização tecnológica.	Responde diretamente como a fragmentação compromete a governança e por que a integração depende de coordenação multinível e pactos institucionais (e não apenas de soluções técnicas), conectando o diagnóstico às premissas do referencial e ao objetivo geral.	Lima (2008); Durante (2009); Lira, Caballero & Nascimento (2022); Kempner-Moreira, Freire & Souza (2022); FBSP (2024); Amaral, Vargas & Prates (2023); Neves (2024); Zilli (2022); Freire (2021); Nunes (2025).

Eixo 2 – Entraves institucionais, tecnológicos e legais	Os entraves são articulados e mutuamente reforçadores. No plano institucional, sobressaem competição interagências, conflitos de atribuição, falta de coordenação e cultura organizacional resistente, mantendo cooperação informal e instável. No plano tecnológico, a heterogeneidade de sistemas e a “feudalização” informacional reproduzem descoordenações institucionais na camada técnica. No plano legal, há simultaneamente avanço do marco protetivo de dados e persistência de inseguranças/lacunas operacionais que elevam custos percebidos de cooperação e estimulam retenção defensiva.	Explica por que a fragmentação persiste e se estabiliza: não é um problema “setorial” (tecnologia) nem “pontual” (norma), mas um arranjo institucional-jurídico-técnico-cultural que impede governança integrada e, por consequência, reduz efetividade analítica.	Rocha (2020); Amaral, Vargas & Prates (2023); Silva, Couto & Freire (2017); Silva (2024); Freire (2021); Kempner-Moreira, Freire & Souza (2022); Nunes (2025); Boba (2005); Azevedo, Riccio & Ruediger (2011); Gomes (2022).
Eixo 3 – Impactos na efetividade da análise criminal	A fragmentação compromete a efetividade analítica ao degradar qualidade, integridade e confiabilidade dos dados que sustentam diagnósticos e decisões. Mesmo com a institucionalização de políticas e práticas orientadas por análise criminal, a persistência de produção e tratamento fragmentados desloca o esforço para conciliar bases, lidar com lacunas e superar dificuldades de acesso. Isso rompe a “cadeia de confiança” informacional, reduz comparabilidade, dificulta séries/estatísticas integradas e enfraquece coordenação e accountability baseadas em evidências.	Conecta a fragmentação aos efeitos (governança → qualidade/confiabilidade e → uso estratégico), atendendo especialmente aos objetivos ligados à análise criminal e à qualidade informacional para decisão estratégica.	Silveira (2024); Senasp (2021); Lima (2008); Durante (2009); Silveira (2025); Amaral, Vargas & Prates (2023); Boba (2005); Azevedo, Riccio & Ruediger (2011).
Eixo 4 – Boas práticas e modelos de interoperabilidade	Há repertórios de integração e modelos que iluminam caminhos de mitigação da fragmentação, inclusive por analogia com desenhos institucionais de hubs colaborativos e mecanismos de compensação. No arranjo brasileiro, sistemas e redes nacionais (como SUSP e SINESP) apontam direções de integração, mas sua existência não garante interoperabilidade efetiva sem institucionalização de rotinas, governança de qualidade e clareza jurídico-organizacional do compartilhamento. A adaptação de boas práticas depende de capacidades institucionais e cultura de cooperação, sob risco de apenas “reempacotar” a fragmentação em novas camadas de sistemas.	Mostra o que pode funcionar (e sob quais condições) e evita a conclusão tecnicista: modelos e plataformas só geram interoperabilidade se acompanhados de engenharia institucional, técnica e jurídica coerente com governança multinível.	Lothian (2024); Freire (2021); Kempner-Moreira, Freire & Souza (2022); Nunes (2025); Silva (2024).

Fonte: Dados da pesquisa; Elaboração: Autores, 2025

Ao articular os eixos, a contribuição teórica central do estudo é explicitar que a fragmentação de dados criminais deve ser compreendida como problema de Governança Multinível de Dados (MultiGov-Data) e não como falha meramente tecnológica.

A literatura sustenta que, embora a Governança Multinível esteja consolidada no debate de políticas públicas, sua aplicação aos fluxos informacionais e decisórios da segurança pública ainda é pouco explorada (Freire, 2021; Kempner-Moreira, Freire & Souza, 2022), e os resultados corroboram essa lacuna ao mostrar que as barreiras institucionais, legais e tecnológicas se combinam e se retroalimentam, produzindo um “regime de fragmentação” que degrada qualidade e utilidade estratégica dos dados (Rocha, 2020; Amaral, Vargas & Prates, 2023; Gomes, 2022; Silva, 2024).

Nessa perspectiva, a governança de dados criminais aparece como mecanismo estruturante de eficiência e de inteligência institucional: sua efetividade depende de articulação multinível de regras, capacidades e incentivos que garantam padronização, interoperabilidade e confiança informacional, condições para práticas analíticas orientadas por evidências (Silva, Couto & Freire, 2017; Freire, 2021; Kempner-Moreira, Freire & Souza, 2022; Nunes, 2025; Boba, 2005).

Isso também responde à lacuna de que abordagens excessivamente tecnicistas negligenciam dimensões sociopolíticas e culturais: os achados indicam que cultura de dados, coordenação interagências e segurança jurídica operacional são tão decisivas quanto infraestrutura e sistemas (Neves, 2024; Zilli, 2022; Amaral, Vargas & Prates, 2023).

Em termos de síntese teórica, este estudo sustenta que a fragmentação de dados criminais é um fenômeno multinível produzido por descoordenações institucionais, ambivalências jurídico-normativas e heterogeneidades tecnológicas, que, em conjunto, enfraquecem a governança e degradam a capacidade de transformar dados em inteligência pública. Sustenta-se, adicionalmente, que interoperabilidade, nesse domínio, deve ser tratada como realização de governança — institucional, técnica e legal, e não como mera integração de bases (Lima, 2008; Durante, 2009; Lira, Caballero & Nascimento, 2022; Boba, 2005; Azevedo, Riccio & Ruediger, 2011).

Ao mesmo tempo, os resultados indicam que iniciativas e modelos de integração só se tornam efetivos quando sustentados por arranjos multiníveis de coordenação, capacidades institucionais e clareza jurídico-operacional (Freire, 2021; Kempner-Moreira, Freire & Souza, 2022; Nunes, 2025; Amaral, Vargas & Prates, 2023).

5. CONSIDERAÇÕES FINAIS

Este artigo partiu do problema de que, no sistema de defesa social, a persistência de bases criminais “em silos” e com baixa articulação entre organizações tende a impedir que dados disponíveis se convertam em inteligência pública útil para coordenação e decisão estratégica (Lima, 2008; Durante, 2009). A investigação buscou responder em que medida essa fragmentação compromete a governança de dados e a efetividade da análise criminal, assumindo como objetivo geral analisar os impactos desse arranjo fragmentado para a governança e para o uso estratégico da informação na segurança pública (Silva, 2024).

Ao fazê-lo, o estudo se inseriu numa lacuna empírico-teórica de conhecimento: apesar da consolidação da Governança Multinível no debate de políticas públicas, ainda são raros trabalhos que a mobilizem para explicar fluxos informacionais e decisórios da segurança pública, e a literatura de governança de dados frequentemente privilegia dimensões técnicas em detrimento de fatores sociopolíticos e culturais que condicionam a efetividade da governança (Kempner-Moreira, Freire & Souza, 2022; Freire, 2021; Neves, 2024; Zilli, 2022).

A síntese integrada dos achados da revisão mostra, em primeiro lugar, que a fragmentação é tratada como fenômeno recorrente e historicamente condicionado, associado à baixa padronização, à existência de “ilhas de dados” e à dificuldade de coordenação interinstitucional (Lima, 2008; Durante, 2009; Lira, Caballero & Nascimento, 2022). Em segundo lugar, os estudos revisados convergem ao indicar que os entraves que sustentam a fragmentação são interdependentes e atravessam dimensões institucionais, tecnológicas e legais, o que impede leituras reducionistas centradas apenas em infraestrutura ou sistemas (Rocha, 2020; Gomes, 2022; Amaral, Vargas & Prates, 2023).

Em terceiro lugar, esse conjunto de barreiras degrada qualidade, confiabilidade e integridade informacional, deslocando a análise criminal do uso estratégico para esforços de conciliação, depuração e superação de lacunas de acesso, com efeitos sobre coordenação e efetividade institucional (Silveira, 2025; Silva, 2024). Em quarto lugar, embora existam iniciativas e repertórios de interoperabilidade e arranjos colaborativos, seu desempenho é condicionado por governança operacional — padrões, responsabilidades e rotinas — e por capacidades institucionais e culturais que sustentem cooperação além de vínculos informais (Brasil, 2024; Silva, 2024; Gomes, 2022).

O que há de novo, frente ao que a literatura já vinha apontando sobre integração e qualidade de dados, é a forma como o estudo hierarquiza e reconstrói explicativamente o problema como um “regime multinível” de governança, em que descoordenações entre atores

e níveis federativos se reproduzem na camada tecnológica e se estabilizam sob ambiguidades jurídico-operacionais e baixa institucionalização da cooperação (Kempner-Moreira, Freire & Souza, 2022; Freire, 2021; Rocha, 2020; Amaral, Vargas & Prates, 2023).

Esse enquadramento dialoga com a proposta de ampliação epistemológica assumida no artigo ao adotar a lente da Governança Multinível de Dados (MultiGov-Data), precisamente para evitar a redução do fenômeno à dimensão “ferramental” e incorporar condicionantes sociopolíticos e culturais da governança (Neves, 2024; Zilli, 2022; Nunes, 2025). Ao articular governança pública, governança de dados e análise criminal, a revisão também reforça que a efetividade analítica depende de condições de governança e de cultura organizacional, e não apenas de disponibilidade de dados e tecnologia (Azevedo, Riccio & Ruediger, 2011; Boba, 2005; Silva, Couto & Freire, 2017).

As contribuições deste estudo direcionam-se a duas frentes. Como implicação teórica, a pesquisa propõe a articulação inédita do conceito de Governança Multinível de Dados (MultiGov-Data) à análise criminal. Os achados refinam essa compreensão ao sustentar que a interoperabilidade e a qualidade não emergem automaticamente da digitalização, mas resultam de coordenação multinível, de mecanismos de *accountability* e de rotinas institucionais que sustentam padrões e confiança interinstitucional (Freire, 2021; Kempner-Moreira, Freire & Souza, 2022; Silva, Couto & Freire, 2017). Sob essa ótica, evidencia-se que a fragmentação de dados criminais é um fenômeno estrutural, produzido pela combinação de entraves institucionais, heterogeneidades tecnológicas e ambivalências jurídico-operacionais, que degradam a confiança informacional e reduzem a efetividade da análise criminal (Rocha, 2020; Gomes, 2022; Amaral, Vargas & Prates, 2023; Silva, 2024). Como implicação prática, o estudo fornece subsídios baseados em evidências para o fortalecimento do SUSP e de políticas públicas informacionais, recomendando que a integração migre de contatos informais interpessoais para uma engenharia institucional regulamentada.

A interoperabilidade, nesse domínio, deve ser tratada como realização de governança, institucional, técnica e legal, e não como simples integração de bases, pois sem pactos, padrões e rotinas a fragmentação tende a ser apenas “reembalada” em novas camadas tecnológicas (Neves, 2024; Zilli, 2022; Freire, 2021; Kempner-Moreira, Freire & Souza, 2022).

As implicações práticas e de política pública indicadas pelos resultados são diretas e exigem abordagem combinada, já que os entraves identificados são articulados entre si (Rocha, 2020; Gomes, 2022). No plano institucional, gestores devem institucionalizar instâncias interagências de governança, com definição de papéis, responsabilidades e mecanismos de coordenação e responsabilização pela qualidade e pelo compartilhamento, reduzindo a

dependência de contatos pessoais e acordos informais que fragilizam a cooperação (Silva, 2024; Gomes, 2022).

No plano técnico, a prioridade deve ser padronização e interoperabilidade semântica e organizacional, de modo a reduzir redundâncias, retrabalho e inconsistências, o que é condição para que análises criminais sejam comparáveis, auditáveis e úteis ao planejamento (Azevedo, Riccio & Ruediger, 2011; Boba, 2005). No plano jurídico-operacional, os achados sugerem que é decisivo traduzir princípios e marcos de governança em regras operacionais de compartilhamento, trilhas de auditoria e salvaguardas, para reduzir insegurança jurídica percebida e comportamentos defensivos de retenção de dados, alinhando proteção de direitos e capacidade analítica legítima (Amaral, Vargas & Prates, 2023; Brasil, 2024).

Portanto, apresenta-se, em nível conceitual, que uma proposta sintética de Governança Multinível de Dados na segurança pública (MultiGov-Data) precisa estruturar-se sobre três engrenagens interorganizacionais: (i) Engenharia Institucional, focada na criação de incentivos para romper a cultura de 'silos' e fomentar a cooperação; (ii) Marcos Regulatórios, estabelecendo regras operacionais que garantam a segurança jurídica; e (iii) Padronização Técnica, mediante a unificação de registros e protocolos de dados.

5.1 Limitações da Pesquisa e Agenda Futura

As limitações do estudo decorrem do desenho adotado e condicionam o alcance das inferências aqui produzidas, preservando o procedimento metodológico e delimitando adequadamente o campo de validade das conclusões, sem, contudo, invalidá-las (Whittemore & Knafl, 2005; Souza, Silva & Carvalho, 2010). Por tratar-se de uma pesquisa de revisão integrativa exclusivamente bibliográfica e documental — sem a extração de dados empíricos primários ou realização de entrevistas com atores institucionais —, os resultados refletem os padrões normativos e teóricos documentados na literatura. Desse modo, sintetizam explicações sobre rotinas de registro e circulação de informações, mas não mensuram de forma causal o desempenho operacional diário das instituições (Whittemore & Knafl, 2005; Creswell, 2014).

Além disso, a pesquisa apresenta restrições relacionadas ao recorte temporal adotado, aos idiomas selecionados e à dependência considerável de literatura cinzenta (como relatórios técnicos e portarias para compreender a materialização das redes). Somado a isso, as escolhas de bases e descritores podem ter restringido a captura de estudos fora dos indexadores utilizados, o que recomenda cautela na pretensão de exaustividade do *corpus* (Cochrane, 2019; PRISMA, 2020). Por fim, a heterogeneidade do conjunto de estudos incluídos amplia a

capacidade interpretativa em nível conceitual, mas limita inferências estritas sobre a efetividade relativa de modelos específicos de interoperabilidade em contextos organizacionais distintos (Denzin & Lincoln, 2018; Creswell, 2014).

A agenda de pesquisas futuras deriva diretamente tanto dos achados quanto destas limitações, apontando para quatro frentes diretamente acionáveis (Whittemore & Knafl, 2005; Creswell, 2014):

Primeiro, sugere-se a realização de estudos empíricos primários e estudos de caso em unidades federativas distintas. Essas pesquisas devem incluir entrevistas, grupos focais e observação de processos para mapear fluxos concretos de dados, rotinas de validação e pontos de falha, testando empiricamente as hipóteses de descoordenação multinível diretamente na prática das agências (Denzin & Lincoln, 2018; Kempner-Moreira, Freire & Souza, 2022).

Segundo, é recomendável construir e validar indicadores de maturidade de Governança Multinível de Dados em segurança pública, incorporando dimensões institucionais, tecnológicas e jurídico-operacionais, em consonância com diretrizes de governança aplicáveis ao setor público (Brasil, 2024; Freire, 2021).

Terceiro, avaliações orientadas por teoria e desenhos quase-experimentais ou análises comparativas de casos concretos podem investigar as condições de implementação e a eficácia de plataformas de interoperabilidade diretamente no fluxo operacional, examinando impactos sobre a qualidade do dado e o uso estratégico da análise criminal (Azevedo, Riccio & Ruediger, 2011; Boba, 2005).

Quarto, pesquisas jurídico-institucionais devem aprofundar como os marcos e instrumentos normativos são operacionalizados no cotidiano interagências e como produzem, na prática, incentivos à cooperação ou à retenção defensiva de dados (Amaral, Vargas & Prates, 2023; Brasil, 2024).

Em termos de encerramento, o artigo contribui ao demonstrar que o debate sobre dados criminais precisa ser reposicionado do plano estritamente técnico para o plano da governança multinível, porque é nesse nível que se definem padrões, incentivos, responsabilidades e condições de confiança que tornam a análise criminal efetiva e socialmente legítima (Freire, 2021; Kempner-Moreira, Freire & Souza, 2022). Ao evidenciar que a fragmentação compromete governança, degrada a confiabilidade informacional e limita a capacidade estatal de resposta integrada, o estudo conecta segurança pública baseada em evidências a desafios mais amplos de coordenação democrática, accountability e racionalidade decisória no Estado (Silva, 2024; Azevedo, Riccio & Ruediger, 2011; Brasil, 2024).

Em síntese final, fortalecer a governança de dados criminais não é apenas modernizar sistemas, é instituir cooperação, padronização e responsabilidade pública como infraestrutura analítica para políticas de segurança mais eficazes e legitimadas (Brasil, 2024; Amaral, Vargas & Prates, 2023).

REFERÊNCIAS

- AMARAL, Thiago Bottino do; VARGAS, Daniel; PRATES, Fernanda. **Segurança pública na era do Big Data: mapeamento e diagnóstico da implementação das novas tecnologias no combate à criminalidade**. Rio de Janeiro: FGV Direito Rio, 2023.
- AZEVEDO, Ana Luísa Vieira de; RICCIO, Vicente; RUEDIGER, Marco Aurélio. **A utilização das estatísticas criminais no planejamento da ação policial: cultura e contexto organizacional como elementos centrais à sua compreensão**. *Ciência da Informação*, v. 40, p. 9–21, 2011.
- BOBA, Rachel. **Crime Analysis and Crime Mapping**. Thousand Oaks, CA: Sage Publications, 2005.
- BARDIN, Laurence. **Análise de Conteúdo**. Tradução de Luís Antero Reto e Augusto Pinheiro. São Paulo: Edições 70, 2016.
- BORGES, Dorian. Notas sobre a qualidade dos dados de homicídios no Brasil. In: LIMA, Renato Sérgio de; BARROS, Betina Warmling (org.). **Estatísticas de Segurança Pública: produção e uso de dados criminais no Brasil**. São Paulo: Fórum Brasileiro de Segurança Pública, 2022. p. 134-145.
- BRASIL. [Portaria MJSP nº 847, de 8 de dezembro de 2025]. **Institui o Sistema Nacional de Inteligência para Enfrentamento ao Crime Organizado**. Diário Oficial da União: seção 1, Brasília, DF, 8 dez. 2025.
- BRASIL. Ministério da Gestão e Inovação em Serviços Públicos. Secretaria de Governo Digital. **Cartilha de Governança de Dados**. Poder Executivo Federal, 2024. Disponível em: <https://www.gov.br/governodigital/>. Acesso em: 19 out. 2025.
- BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Justiça. **ENCCLA 2023: estratégia nacional de combate à corrupção e à lavagem de dinheiro**. Brasília, DF: Secretaria Nacional de Justiça, 2022.
- SILVEIRA, Claudio Todisco. **Segurança pública baseada no uso de dados**. *Brazilian Journal of Business*, v. 7, n. 1, p. 77-91, jan./mar. 2025.
- LASTRES, Helena Maria Martins; CASSIOLATO, José Eduardo; DANTAS, Marcos; *et al.* **Economia política de dados e soberania digital**. Avaré, SP: Editora Contracorrente, 2025.
- CASSIOLATO, José Eduardo. **Soberania Digital e Desenvolvimento: um olhar crítico sobre as possibilidades e limites do Brasil nas tecnologias digitais**. *Revista Eptic*, v. 26, n. 3, set./dez. 2024.
- CORCINO, Kevin Ferreira; PREARO, Leandro. **A percepção da qualidade dos serviços públicos por parte da população em municípios de baixo Índice de Desenvolvimento Humano**. *REUNIR Revista de Administração, Contabilidade e Sustentabilidade*, v. 15, n. 1, p. 100–114, 17 ago. 2025.

CORDEIRO, A. M. *et al.* Revisão sistemática: uma revisão narrativa. **Revista do Colégio Brasileiro de Cirurgiões**, v. 34, n. 6, p. 428-431, 2007.

COVARRUBIAS, Jersain Zadamig. **Cybersecurity in Mexico: An In-Depth Analysis of a Fragmented Regulatory Landscape**. Mexican Law Review, v. 18, n. 1, 2025

CRISTÓVAM, J. S. S.; SOUZA, R. **Colonialismo digital e soberania informacional**. São Paulo: Atlas, 2024.

CRISTÓVAM, José Sérgio da Silva; SOUSA, Thanderson Pereira de. Soberania tecnológica vs. colonialidade digital: Estado inteligente e políticas públicas para uma IA Bethânia. **Sequência**, Florianópolis, v. 45, p. e103426, 2024.

DURANTE, Marcelo Ottoni. Sistema nacional de estatísticas de segurança pública e justiça criminal. **Coleção Segurança com Cidadania: sistemas de informação, estatísticas criminais e cartografias sociais**, Brasília, DF, v. 1, n. 2, p. 181–206, 2009.

DURANTE, Marcelo; RIBEIRO, *et al.* **Modernização dos modelos de policiamento: uso das estatísticas na segurança pública para além da análise dos registros de ocorrência na polícia (DF – 2015 a 2018)**. In: LIMA, Renato Sérgio de; BARROS, Betina Warmling (org.). Estatísticas de Segurança Pública: produção e uso de dados criminais no Brasil. São Paulo: Fórum Brasileiro de Segurança Pública, 2022. p. 282-297.

ENAP. Escola Nacional de Administração Pública. **Introdução à interoperabilidade**. Brasília, DF, 2015. Disponível em: <https://repositorio.enap.gov.br/>. Acesso em: 19 out. 2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário Brasileiro de Segurança Pública**. São Paulo: FBSP, ano 18, 2024.

FREIRE, Patrícia de Sá. **Glossário de Governança Multinível do Conhecimento e da Aprendizagem**. Curitiba: CRV, 2021.

FREIRE, Patrícia de Sá; MARQUES, Demis. **Coprodução transhumana: manual de uso ético de inteligência artificial na escrita acadêmica**. Editora Arquétipos, 2023.

FURTADO, Vasco. **Inteligência artificial na segurança pública: conceitos, perspectivas e desafios**. In: LIMA, Renato Sérgio de; BARROS, Betina Warmling (org.). Estatísticas de Segurança Pública: produção e uso de dados criminais no Brasil. São Paulo: Fórum Brasileiro de Segurança Pública, 2022. p. 178-189.

GOMES, Rodrigo Carneiro. **A Inteligência policial e a cooperação interagências no combate ao crime organizado nas fronteiras**. Revista Brasileira de Ciências Policiais, Brasília, v. 13, n. 8, p. 287–331, 2022.

JANNUZZI, Paulo de Martino. **A importância da informação estatística para as políticas sociais no Brasil: breve reflexão sobre a experiência do passado para considerar no presente**. Revista Brasileira de Estudos de População, v. 35, p. e0055, 2018.

KEMPNER-MOREIRA, Fernanda; FREIRE, Patrícia de Sá; SOUZA, João Artur. **Governança Multinível Pública: um novo modelo para a governança pública brasileira**. Curitiba: CRV, 2022.

LIMA, Renato Sérgio de. **A produção da opacidade: estatísticas criminais e segurança pública no Brasil**. Novos Estudos CEBRAP, São Paulo, n. 80, p. 65–69, mar. 2008.

LIMA, Renato Sérgio de. **Estatísticas criminais e fragmentação institucional no Brasil**. Revista Brasileira de Segurança Pública, v. 2, n. 4, p. 45–62, 2008.

LIMA, Renato Sérgio de. **Sistemas de informações criminais: construindo uma metodologia de integração de dados e de análise do fluxo da justiça criminal do estado de São Paulo**. In: CERQUEIRA, D.; LEMGRUBER, J.; MUSAMECI, L. (org.). Criminalidade, Violência e Segurança Pública no Brasil: uma discussão sobre as bases de dados e questões metodológicas. Rio de Janeiro: IPEA, 2000.

LIMA, Renato Sérgio de; BARROS, Betina Warmling (org.). **Estatísticas de Segurança Pública: produção e uso de dados criminais no Brasil**. São Paulo: Fórum Brasileiro de Segurança Pública, 2022.

LIRA, Pablo; CABALLERO, Bárbara; NASCIMENTO, Daniel Cruz do. **Informação qualificada a partir de estatísticas criminais oficiais: avanços e desafios nacionais e a experiência do Espírito Santo**. In: LIMA, Renato Sérgio de; BARROS, Betina Warmling (org.). Estatísticas de Segurança Pública: produção e uso de dados criminais no Brasil. São Paulo: Fórum Brasileiro de Segurança Pública, 2022. p. 298-309.

LOIK, Ramon. **European internal security interests and Brexit: legal and operational aspects of the post-Brexit cooperation model**. Romanian Journal of European Affairs, v. 20, n. 2, p. 55-74, dez. 2020.

LOTHIAN, Sarah Louise. **Transnational maritime environmental crime and the BBNJ Agreement**. Frontiers in Conservation Science, v. 5, 2024.

MELATI, Claudia; JANISSEK-MUNIZ, Raquel. **A inteligência na gestão pública: uma análise sob a perspectiva institucional**. Revista de Administração Pública, v. 56, p. 721–744, 2022.

MISSE, Michel. **Sobre as estatísticas criminais no Rio de Janeiro (1908–2020): uma breve história e um testemunho**. In: LIMA, Renato Sérgio de; BARROS, Betina Warmling (org.). Estatísticas de Segurança Pública: produção e uso de dados criminais no Brasil. São Paulo: Fórum Brasileiro de Segurança Pública, 2022. p. 190-201.

NEVES, Marta Silva. **Diretrizes e métodos para o desenvolvimento organizacional sustentável (DOS), com base na equidade de stakeholders**. 2024. Tese (Doutorado em Engenharia e Gestão do Conhecimento) – Universidade Federal de Santa Catarina, Florianópolis, 2024.

NUNES, Carlos Francisco Oliveira. **Framework da Governança Multinível do Sistema Único de Segurança Pública (SUSP) - Brasil**. 2025. Tese (Doutorado em Engenharia e Gestão do Conhecimento) – Universidade Federal de Santa Catarina, Florianópolis, 2025.

PAGE, Matthew James. *et al.* **The PRISMA 2020 statement: an updated guideline for reporting systematic reviews.** BMJ, v. 372, n. 71, 2021.

ROCHA, Leonino Gomes. **Redes interorganizacionais no enfrentamento à corrupção: um estudo da Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro - ENCCLA.** 2020. Tese (Doutorado) – Universidade de Salamanca, Espanha, 2020.

RODRIGUES, Luiz Cláudio de Queiroz. **Interoperabilidade informacional entre Sisbin e Ministério Público e aplicação pelo órgão ministerial de conhecimentos oriundos da atividade de inteligência – estágio atual e desafios.** Revista Brasileira de Inteligência, Brasília, n. 17, p. 65–80, 2022.

SEDGWICK, Donna; CALLAHAN, Jason; HAWDON, James. **Institutionalizing partnerships: a mixed methods approach to identifying trends and perceptions of community policing and multi-agency task forces.** Police Practice and Research, v. 22, n. 1, p. 727-744, 2020.

SETZER, Valdemar W. **Dado, Informação, Conhecimento e Competência.** [S. l.], 2015. Disponível em: <https://www.ime.usp.br/~vwsetzer/datagrama.html>. Acesso em: 19 out. 2025.

SILVA, João Apolinário da. **Análise criminal: teoria e prática.** Salvador: Artpoesia, 2015.

SILVA, Marcos Paulo Hiath. **A Segurança pública brasileira no contexto Pós-88: desafios da integração.** 2024. 73 f. Dissertação (Mestrado em Políticas Públicas e Desenvolvimento) – Instituto de Pesquisa Econômica Aplicada (IPEA), Brasília, 2024.

SILVA, Talita Caetano; COUTO, Rogeria Moreira; FREIRE, Patrícia de Sá. **Governança do Conhecimento: uma revisão em direção à conceituação e diferenciação da Gestão do Conhecimento.** CIKI Journal, v. 7, n. 1, p. 33–49, 2017.

SIQUEIRA, Bruno. **Fundamentos da biopolítica nos estudos em geopolítica: o ciberespaço e as novas estratégias de disputas e dominação.** Uberlândia: UFU, 29 abr. 2025.

VIOLÊNCIA é a maior preocupação dos brasileiros, aponta pesquisa Genial/Quaest. UOL, [S. l.], 2 abr. 2025. Disponível em: <https://noticias.uol.com.br/>. Acesso em: 15 out. 2025.

ZILLI, Júlio César Farias. **Framework para a Governança Multinível do Sistema Portuário Brasileiro em direção ao Porto Inteligente.** 2022. Tese (Doutorado em Engenharia e Gestão do Conhecimento) – Universidade Federal de Santa Catarina, Florianópolis, 2022.

ZUBILLAGA, Verónica; HANSON, Rebecca; SÁNCHEZ, Francisco. **Gobernanzas criminales en tiempos de revolución post-Chávez y legitimidad cuestionada: una mirada a los distintos órdenes territoriales y actores armados en Caracas.** Dilemas: Revista de Estudos de Conflito e Controle Social, Rio de Janeiro, Edição Especial n. 4, p. 497-527, 2022.