

Governança Institucional de Dados na Segurança Pública: riscos operacionais e desafios do desenho regulatório da persecução penal no Brasil

Institutional Design and Data Governance in Brazilian Public Security: operational risks and implications for public management and law enforcement policy

Gobernanza de Datos en la Seguridad Pública en Brasil: riesgos operativos y desafíos del diseño institucional para la gestión pública y la política de seguridad

GT06 - Gestão Pública e Ciências Policiais: Desafios e Inovações para a Segurança Pública no Brasil

**Wanessa Rezende
Erika Lisboa
Patrícia Mello**

RESUMO

A crescente utilização de dados pessoais e tecnologias de vigilância no âmbito da segurança pública tem reconfigurado os modelos de formulação e implementação de políticas de persecução penal no Brasil. A incorporação de instrumentos de coleta, tratamento e compartilhamento de dados amplia a capacidade estatal de prevenção e repressão ao crime, mas também impõe desafios relevantes de governança institucional, coordenação interorganizacional e *accountability* em um ambiente federativo fragmentado. Neste contexto, o presente artigo analisa o desenho institucional do Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Persecução Penal, examinando-o como instrumento de governança da política de segurança pública baseada em dados. A partir de abordagem qualitativa de natureza analítico-institucional, o estudo identifica riscos operacionais associados à concentração decisória, à indefinição de competências regulatórias e à fragilidade dos mecanismos de coordenação e controle. Ao evidenciar os efeitos do arranjo institucional sobre a implementação da política, o trabalho contribui para o debate em Administração Pública sobre governança, capacidade estatal e gestão de políticas públicas orientadas por dados no contexto brasileiro.

Palavras-chave: Segurança pública. Governança institucional. Políticas públicas baseadas em dados. Persecução penal.

ABSTRACT

The growing use of personal data and surveillance technologies in public security has reshaped the institutional arrangements through which criminal law enforcement policies are formulated and implemented in Brazil. While data collection, processing, and sharing instruments have expanded the state's capacity for crime prevention and repression, they have also generated significant challenges related to institutional governance, interorganizational coordination, and *accountability* in a fragmented federal context. This article analyzes the institutional design of the Draft Bill on Data Protection for Public Security and Criminal Law Enforcement, examining it as a governance framework for data-driven public security policies. Drawing on a qualitative analytical-institutional approach, the study identifies operational risks arising from decision-making concentration, ambiguities in regulatory competencies, and weaknesses in coordination and control mechanisms. By highlighting how institutional arrangements affect policy implementation, the paper contributes to the field of Public Administration, particularly to debates on governance, state capacity, and the management of data-driven public policies in Brazil.



EBAP

Encontro Brasileiro de Administração Pública
XIII EBAP, Junho de 2026, Brasília-DF, Brasil

ARTIGO

Keywords

Public security. Institutional data governance. Data-driven public policies. Criminal law enforcement.

RESUMEN

El creciente uso de datos personales y tecnologías de vigilancia en el ámbito de la seguridad pública ha reconfigurado los arreglos institucionales mediante los cuales se formulan e implementan las políticas de persecución penal en Brasil. La incorporación de instrumentos de recolección, tratamiento y compartición de datos ha ampliado la capacidad estatal de prevención y represión del delito, pero también ha generado desafíos significativos en materia de gobernanza institucional, coordinación interorganizacional y *accountability* en un contexto federativo fragmentado. Este artículo analiza el diseño institucional del Anteproyecto de Ley de Protección de Datos para la Seguridad Pública y la Persecución Penal, examinándolo como un marco de gobernanza de las políticas de seguridad pública orientadas por datos. A partir de un enfoque cualitativo y analítico-institucional, el estudio identifica riesgos operativos derivados de la concentración decisoria, de las ambigüedades en las competencias regulatorias y de la fragilidad de los mecanismos de coordinación y control. Al evidenciar los efectos del arreglo institucional sobre la implementación de la política, el trabajo contribuye al debate en Administración Pública sobre gobernanza, capacidad estatal y gestión de políticas públicas basadas en datos en el contexto brasileño.

Palabras clave

Seguridad pública. Gobernanza institucional de datos. Políticas públicas basadas en datos. Criminal law enforcement.

1. Introdução

O uso intensivo de dados e de tecnologias digitais tem se consolidado como um dos principais vetores de transformação das políticas de segurança pública no Brasil. Sistemas de informação integrados, bancos de dados compartilhados, ferramentas de análise preditiva e tecnologias de vigilância passaram a ocupar posição central nas estratégias de prevenção e repressão à criminalidade, alterando de forma significativa os modos de atuação das organizações policiais e dos órgãos responsáveis pela persecução penal (Zagato, 2022).

Esse processo de digitalização da segurança pública ampliou a capacidade estatal de coleta, tratamento e circulação de informações sensíveis, ao mesmo tempo em que expôs limites importantes do arranjo institucional brasileiro para lidar com políticas públicas orientadas por dados (Gleizer, 2021). A multiplicidade de atores envolvidos, a fragmentação das competências decisórias e a ausência de mecanismos claros de coordenação e controle passaram a gerar riscos operacionais relevantes, com impactos diretos sobre a efetividade das ações de segurança e sobre a legitimidade institucional dessas políticas (Ferreira, 2024).

Em políticas públicas de elevada complexidade tecnológica e organizacional, como aquelas baseadas em dados, o desenho institucional exerce papel determinante sobre os resultados da implementação. A distribuição de competências, a estrutura das instâncias regulatórias e a organização dos mecanismos de supervisão e coordenação intergovernamental condicionam diretamente a capacidade estatal. É nesse arranjo que se definem a coerência das decisões, a eficiência administrativa e a legitimidade da atuação pública.

É nesse contexto que se insere o Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Persecução Penal, elaborado por uma Comissão de Juristas indicada pela Câmara dos Deputados em 2020, com o objetivo de estabelecer parâmetros normativos para o uso de dados no âmbito da atividade repressiva estatal. Mais do que um diploma jurídico, o anteprojeto pode ser compreendido como um instrumento de governança da política de segurança pública baseado em dados, na medida em que define arranjos decisórios, distribui competências institucionais e estabelece (ou omite) mecanismos de coordenação, fiscalização e *accountability* (Bioni, 2019; Comissão de Juristas, 2020).

A análise do anteprojeto sob a ótica da gestão pública revela que a efetividade da política de segurança orientada por dados não depende apenas da ampliação das capacidades tecnológicas do Estado, mas sobretudo da qualidade do seu desenho institucional. Modelos regulatórios que concentram decisões, fragilizam instâncias de controle ou deixam indefinidos os papéis dos diferentes atores tendem a produzir assimetrias informacionais (Bioni, 2019), riscos de captura institucional e dificuldades operacionais na implementação das políticas públicas (Mendes & Fonseca, 2020; Nissenbaum, 2010).

Diante disso, o presente artigo busca responder à seguinte questão: de que maneira o desenho institucional previsto no Anteprojeto de Lei de Proteção de Dados para a Segurança Pública influencia a governança, a coordenação interinstitucional e os mecanismos de *accountability* da política de segurança pública baseada em dados no contexto federativo brasileiro?

Parte-se do entendimento de que aspectos centrais do arranjo institucional proposto, especialmente a concentração regulatória e a definição insuficiente de mecanismos formais de coordenação, tendem a gerar obstáculos relevantes à implementação eficiente e legítima da política pública. O trabalho, então, analisa o desenho institucional do Anteprojeto como instrumento de governança da política de segurança pública baseada em dados, com foco nos seus impactos operacionais, nos riscos institucionais associados à sua implementação e nos desafios de coordenação e *accountability* entre os órgãos envolvidos, buscando contribuir para o debate sobre capacidade estatal e gestão pública da segurança no Brasil.

Para examinar essa questão, torna-se necessário explicitar o percurso analítico adotado, bem como as categorias teóricas mobilizadas para a leitura institucional do anteprojeto.

2. Método

O presente estudo adota abordagem qualitativa, de natureza analítico-institucional, fundamentada na análise documental do texto do Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Persecução Penal, elaborado pela Comissão de Juristas instituída pela Câmara dos Deputados, em 2020.

A opção por uma análise institucional fundamenta-se na premissa de que políticas públicas orientadas por dados não dependem exclusivamente de parâmetros normativos materiais, mas do arranjo organizacional que sustenta sua formulação, regulação e implementação. O desenho institucional — entendido como a distribuição de competências, a definição de instâncias decisórias, os mecanismos de supervisão e os instrumentos de coordenação intergovernamental — exerce influência direta sobre a capacidade estatal, a coerência decisória e os resultados operacionais da política pública.

A unidade de análise do estudo consiste no desenho institucional previsto no anteprojeto, especialmente no que se refere: (i) à distribuição de competências regulatórias; (ii) à definição de papéis entre os diferentes órgãos envolvidos na persecução penal; (iii) à existência ou ausência de mecanismos formais de coordenação interinstitucional; e (iv) às estruturas de fiscalização e *accountability* previstas.

Para fins analíticos, utilizam-se categorias derivadas da literatura de governança pública e implementação de políticas públicas complexas, tais como: separação funcional entre formulação, regulação e controle; coordenação interorganizacional e federativa; *accountability* institucional; e capacidade estatal para execução de políticas públicas em contextos de elevada complexidade tecnológica.

A partir dessas categorias, procede-se à identificação de potenciais riscos institucionais associados ao modelo proposto, considerando suas implicações para a eficiência administrativa, a segurança jurídica e a legitimidade democrática da política pública de segurança baseada em dados.

Não se trata de avaliação empírica de resultados nem de análise quantitativa de desempenho institucional. O objetivo é realizar uma análise prospectiva do desenho normativo e de suas possíveis implicações operacionais, antecipando desafios de implementação e de governança a partir do arranjo institucional proposto.

3. Delimitação da Situação-Problema

A política de segurança pública brasileira caracteriza-se historicamente por um elevado grau de fragmentação institucional (Gleizer, 2021). Polícias civis e militares, Ministérios Públicos, órgãos do Poder Judiciário, unidades de inteligência e, em determinados contextos, entidades privadas e concessionárias de serviços públicos atuam de forma simultânea e interdependente no ciclo de produção, compartilhamento e utilização de dados para fins de persecução penal.

Com a intensificação do uso de tecnologias digitais, essa fragmentação passou a produzir efeitos ainda mais sensíveis. Diferentes órgãos passaram a acessar e tratar grandes volumes de dados pessoais e sensíveis, frequentemente por meio de sistemas próprios, com padrões distintos de governança, segurança da informação e controle. A ausência de protocolos operacionais unificados e de instâncias claras de coordenação interinstitucional contribui para a opacidade dos fluxos de dados e para a dificuldade de fiscalização efetiva das práticas adotadas na ponta da política pública (Gleizer, 2021).

Nesse cenário, o problema central não reside na utilização de dados como instrumento da política de segurança pública, mas na forma como o Estado organiza institucionalmente esse uso. A indefinição quanto às responsabilidades decisórias, a sobreposição de competências regulatórias e a fragilidade dos mecanismos de controle criam um ambiente propício a riscos operacionais, como o uso inadequado de tecnologias, a assimetria de poder informacional entre os atores envolvidos e a dificuldade de correção de desvios na implementação das políticas (Ferreira, 2024).

O Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Persecução Penal surge como tentativa de responder a esse problema, ao estabelecer parâmetros para o tratamento de dados no âmbito da atividade repressiva. No entanto, ao concentrar funções regulatórias e de supervisão em determinados órgãos (Moura, 2021) e ao deixar em aberto aspectos relevantes da coordenação interinstitucional, o modelo proposto levanta questionamentos quanto à sua capacidade de promover uma governança equilibrada, transparente e operacionalmente eficiente da política de segurança pública baseada em dados (Bioni et al., 2020).

A situação-problema que orienta este trabalho, portanto, pode ser sintetizada na seguinte questão: em que medida o desenho institucional proposto pelo anteprojeto oferece condições adequadas de governança, coordenação e *accountability* para a implementação de políticas de segurança pública orientadas por dados em um ambiente institucional marcado pela fragmentação e pela multiplicidade de atores? A resposta a essa pergunta é fundamental para compreender os riscos e os limites do modelo regulatório proposto, bem como para subsidiar ajustes institucionais capazes de aprimorar a gestão pública da segurança no contexto brasileiro.

A partir dessa delimitação, passa-se à análise do desenho institucional propriamente dito.

4. O Desenho Institucional da Política de Segurança Pública Baseada em Dados

A análise do Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Persecução Penal, quando observada sob a ótica da gestão pública, revela um desenho institucional que busca responder ao desafio do uso intensivo de dados na persecução penal, mas o faz por meio de uma arquitetura decisória marcada por centralização e indefinições operacionais relevantes. Mais do que estabelecer parâmetros técnicos para o tratamento de dados, o anteprojeto estrutura relações de poder, distribui competências e define, ainda que implicitamente, os mecanismos de governança da política de segurança pública orientada por dados.

Um dos elementos centrais desse desenho é a atribuição de funções regulatórias e de supervisão a instâncias que não atuam diretamente na implementação cotidiana das políticas de segurança. Ao concentrar competências normativas, interpretativas e fiscalizatórias em um mesmo polo institucional, o modelo proposto reduz a separação funcional entre formulação, regulação e controle, o que tende a produzir assimetrias decisórias e dificuldades de correção de rumos ao longo do processo de implementação. Em termos de gestão pública, trata-se de um arranjo que fragiliza a lógica de freios internos e limita a aprendizagem institucional decorrente da prática operacional (Barbosa, 2019; Moura, 2021)

Além disso, o anteprojeto apresenta lacunas importantes no que se refere à coordenação interinstitucional. A política de segurança pública baseada em dados envolve, necessariamente, a atuação integrada de órgãos policiais, Ministérios Públicos, Poder Judiciário, unidades de inteligência e estruturas administrativas responsáveis por tecnologia da informação. No entanto, o modelo proposto não define de forma clara os mecanismos de articulação entre esses atores, tampouco estabelece instâncias permanentes de coordenação capazes de harmonizar procedimentos, padronizar fluxos de dados e resolver conflitos operacionais.

A ausência de protocolos institucionais explícitos para a interoperabilidade dos sistemas e para a governança do compartilhamento de dados reforça a tendência à fragmentação já observada na prática da segurança pública brasileira. Cada órgão tende a operar com seus próprios sistemas, critérios e prioridades, o que dificulta tanto a eficiência da política quanto a fiscalização externa e interna das práticas adotadas. Do ponto de vista da implementação, essa indefinição institucional amplia o risco de soluções *ad hoc* e de decisões casuísticas, pouco transparentes e de difícil controle (Bioni et al., 2020).

Outro aspecto relevante do desenho institucional analisado é a limitação dos mecanismos de *accountability* operacional. A literatura clássica de Administração Pública enfatiza que arranjos institucionais eficazes dependem da existência de mecanismos claros de responsabilização e controle, capazes de equilibrar autonomia decisória e supervisão institucional (Hood, 1998). O anteprojeto estabelece diretrizes gerais para o uso de dados, mas não detalha instrumentos claros de monitoramento contínuo, avaliação de desempenho ou revisão periódica das práticas institucionais. Em políticas públicas orientadas por dados, a ausência desses mecanismos compromete a capacidade do Estado de identificar falhas, corrigir desvios e ajustar o uso das tecnologias às finalidades públicas pretendidas.

A comparação com modelos regulatórios internacionais voltados à segurança pública baseada em dados evidencia essas fragilidades. Em experiências estrangeiras, observa-se a preocupação em separar funções regulatórias e executivas, criar instâncias colegiadas de governança e estabelecer mecanismos de auditoria independente e revisão *ex post* das práticas institucionais (European Union, 2016; Lodder, 2020). Esses elementos contribuem para reduzir riscos de captura institucional, aumentar a transparência e fortalecer a legitimidade das políticas públicas, sem inviabilizar sua efetividade operacional.

No caso brasileiro, o desenho institucional proposto pelo anteprojeto parece priorizar a centralização normativa como estratégia de controle, em detrimento da construção de uma governança distribuída e cooperativa. Embora a intenção de conferir maior segurança jurídica ao uso de dados na persecução penal seja legítima, a ausência de arranjos claros de coordenação e de *accountability* pode comprometer tanto a implementação eficiente da política quanto a confiança institucional nos mecanismos adotados.

A análise do desenho institucional demonstra que os desafios da política de segurança pública baseada em dados não se esgotam na definição de limites normativos para o tratamento de informações. O ponto decisivo está na forma como o Estado organiza suas estruturas decisórias, articula seus atores e constrói mecanismos operacionais de controle.

Essas características estruturais permitem identificar, com maior precisão, os riscos operacionais e os desafios de governança que emergem do modelo proposto.

5. Riscos Operacionais e Desafios de Governança

O desenho institucional previsto no Anteprojeto estrutura a política de segurança pública baseada em dados a partir de um modelo centralizado, com mecanismos limitados de coordenação. Esse arranjo projeta riscos operacionais que repercutem diretamente na implementação da política e na capacidade estatal de controlar o uso das tecnologias de informação.

Mais do que discutir a centralização normativa em si, importa examinar como esse desenho decisório influencia a dinâmica concreta de coordenação, controle e execução das atividades de persecução penal. Os riscos identificados decorrem não da adoção de tecnologias digitais, mas da forma como competências, fluxos informacionais e mecanismos de supervisão são organizados no interior das instituições responsáveis pela política.

ARTIGO

Um primeiro risco relevante diz respeito à concentração decisória. A centralização de competências regulatórias e interpretativas tende a reduzir a pluralidade de perspectivas na definição dos parâmetros de uso dos dados, dificultando a incorporação de aprendizados oriundos da prática operacional. Em políticas públicas orientadas por dados, a ausência de instâncias deliberativas mais amplas e técnicas pode gerar decisões desconectadas das realidades enfrentadas pelos órgãos que atuam na ponta, comprometendo tanto a efetividade das ações de segurança quanto a aderência dos procedimentos adotados aos objetivos públicos estabelecidos.

Associado a esse aspecto, emerge o risco de assimetria informacional entre os diferentes atores da política de segurança pública. Órgãos com maior capacidade tecnológica e acesso privilegiado a sistemas de informação passam a deter poder decisório desproporcional, influenciando a formulação e a interpretação das regras aplicáveis. Essa assimetria dificulta a supervisão cruzada entre instituições, enfraquece os mecanismos de controle interno e amplia a dependência de soluções técnicas cuja lógica nem sempre é plenamente compreendida ou auditável pelos demais atores envolvidos (Mendes & Fonseca, 2020).

Outro desafio central refere-se à fragilidade dos mecanismos de *accountability* operacional. O modelo proposto carece de instrumentos claros de monitoramento contínuo do uso de dados, de avaliação periódica dos impactos das tecnologias empregadas e de responsabilização institucional por eventuais desvios ou falhas. Na ausência desses mecanismos, a política de segurança pública baseada em dados corre o risco de se tornar opaca, com dificuldades para identificar responsabilidades, corrigir práticas inadequadas e promover ajustes ao longo do tempo.

A implementação na ponta da política pública também se apresenta como fonte relevante de risco. A literatura clássica sobre implementação destaca que as políticas públicas são concretamente moldadas pelas decisões cotidianas tomadas pelos agentes responsáveis por sua execução, cuja discricionariedade operacional influencia diretamente os resultados institucionais (Lipsky, 2019). No contexto da segurança pública orientada por dados, a falta de protocolos operacionais padronizados e de diretrizes claras para a interoperabilidade dos sistemas favorece a adoção de práticas heterogêneas entre órgãos e unidades, ampliando o risco de inconsistências, falhas de segurança e decisões casuísticas. Em ambientes institucionais marcados por elevada complexidade tecnológica, a ausência de orientação clara na implementação amplia a margem de discricionariedade operacional. Com isso, decisões estruturais passam a ser assumidas pelos agentes da ponta, quando deveriam estar previamente organizadas no plano institucional.

Além disso, a combinação entre concentração decisória e fragilidade de controle cria um ambiente propício ao risco de captura institucional. A definição e a interpretação das regras de uso de dados passam a ser influenciadas por interesses organizacionais específicos ou por lógicas internas de funcionamento das instituições, em detrimento de uma visão sistêmica da política de segurança pública. Esse risco é particularmente sensível em políticas que envolvem tecnologias complexas e decisões técnicas de difícil escrutínio externo (Nissenbaum, 2010).

Por fim, a ausência de mecanismos robustos de revisão e de avaliação *ex post* limita a capacidade de aprendizagem institucional. Políticas públicas orientadas por dados exigem ciclos contínuos de avaliação, ajustes e aperfeiçoamento, de modo a responder tanto às mudanças tecnológicas quanto às dinâmicas sociais e criminais. Sem instrumentos formais de revisão periódica, o modelo regulatório tende a se cristalizar, tornando-se progressivamente menos responsivo e menos eficiente.

Dessa forma, os riscos operacionais e os desafios de governança identificados não decorrem da utilização de dados como ferramenta da segurança pública, mas da insuficiência do desenho institucional proposto para lidar com a complexidade dessa política. A superação desses desafios exige a construção de arranjos institucionais que

combinem coordenação interinstitucional, *accountability* operacional e capacidade adaptativa, elementos fundamentais para a efetividade e a legitimidade da segurança pública baseada em dados no contexto brasileiro.

6. Recomendações Institucionais e de Gestão

As recomendações institucionais apresentadas na seção anterior não se limitam a ajustes pontuais do anteprojeto, mas indicam a necessidade de repensar a arquitetura decisória que sustenta a política de segurança pública baseada em dados. O debate sobre governança institucional, coordenação e *accountability* revela que a consolidação desse modelo regulatório exige mais do que parâmetros normativos abstratos: demanda arranjos organizacionais capazes de responder à complexidade tecnológica e federativa que caracteriza a persecução penal no Brasil.

Nesse contexto, a consolidação de políticas de segurança pública orientadas por dados representa um movimento irreversível no cenário contemporâneo, impulsionado tanto pela expansão das capacidades tecnológicas do Estado quanto pela crescente sofisticação dos fenômenos criminais. Entretanto, a análise conduzida demonstra que os desafios centrais não se concentram na utilização de dados em si, mas na forma como o Estado organiza institucionalmente esse uso.

Em complemento, recomenda-se o fortalecimento de mecanismos permanentes de coordenação interinstitucional. A política de segurança pública orientada por dados exige a atuação integrada de órgãos com culturas organizacionais, capacidades técnicas e responsabilidades distintas. A instituição de comitês ou fóruns técnicos de governança, com representação dos principais atores da segurança pública, pode contribuir para a harmonização de procedimentos, a definição de protocolos comuns e a resolução de conflitos operacionais relacionados ao uso e ao compartilhamento de dados.

Outra medida relevante consiste na formalização de protocolos operacionais padronizados para o tratamento e a interoperabilidade de dados. A definição de critérios mínimos de segurança da informação, de padrões técnicos para integração de sistemas e de fluxos claros de acesso e compartilhamento reduziria a heterogeneidade das práticas institucionais e ampliaria a previsibilidade das ações na ponta da política pública. Esses protocolos devem ser acompanhados de orientações claras quanto às responsabilidades institucionais e aos mecanismos de controle aplicáveis.

No campo da *accountability*, recomenda-se a adoção de instrumentos contínuos de monitoramento e avaliação do uso de dados na segurança pública. Auditorias periódicas, avaliações de impacto institucional e mecanismos de revisão *ex post* das práticas adotadas podem contribuir para identificar falhas, corrigir desvios e ajustar a política às mudanças tecnológicas e organizacionais. A transparência desses processos, ainda que com as cautelas necessárias à atividade de persecução penal, é elemento fundamental para a construção de confiança institucional.

Também se mostra pertinente a incorporação de cláusulas de revisão periódica do modelo regulatório, de modo a evitar a cristalização de arranjos institucionais inadequados. A rápida evolução das tecnologias de informação e das dinâmicas criminais impõe a necessidade de mecanismos formais de atualização normativa e institucional, capazes de garantir que a política de segurança pública baseada em dados permaneça alinhada às suas finalidades públicas e às capacidades efetivas do Estado.

Por fim, recomenda-se o investimento contínuo na capacitação dos agentes públicos envolvidos na implementação da política. A efetividade do uso de dados na segurança pública depende não apenas de tecnologias adequadas, mas da capacidade dos servidores de compreender, aplicar e supervisionar os instrumentos disponíveis.

Programas de formação voltados à governança de dados, à gestão da informação e à ética institucional podem contribuir para reduzir riscos operacionais e fortalecer a cultura de responsabilidade no uso das tecnologias.

Em conjunto, essas recomendações apontam para a necessidade de uma abordagem integrada e institucionalmente equilibrada da política de segurança pública orientada por dados. O fortalecimento da governança, da coordenação e da *accountability* não apenas amplia a efetividade operacional das ações de segurança, como também contribui para a legitimidade e a sustentabilidade das políticas públicas de persecução penal no contexto brasileiro.

Considerações Finais

A análise desenvolvida ao longo deste artigo indica que a consolidação de políticas de segurança pública orientadas por dados exige mais do que inovação tecnológica ou definição abstrata de limites normativos. Nesse cenário, o debate sobre o uso de dados na persecução penal não pode se limitar à definição de limites normativos abstratos, devendo incorporar, de forma central, a análise dos arranjos institucionais que sustentam a implementação dessas políticas.

A análise do Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Persecução Penal, conduzida sob a perspectiva da gestão pública, evidencia que os principais desafios associados à segurança pública baseada em dados estão relacionados ao seu desenho institucional. A concentração decisória, a fragilidade dos mecanismos de coordenação interinstitucional e a ausência de instrumentos robustos de *accountability* operacional configuram riscos relevantes para a efetividade e a legitimidade da política proposta.

Ao tratar o anteprojeto como instrumento de governança, o presente trabalho buscou deslocar o foco do debate jurídico tradicional para a dimensão operacional e institucional da política pública. Esse deslocamento permite compreender que a eficiência do uso de dados na segurança pública depende menos da ampliação das capacidades tecnológicas e mais da capacidade do Estado de organizar suas estruturas decisórias, articular seus atores e construir mecanismos de controle e aprendizagem institucional. Essa perspectiva amplia o debate em Administração Pública sobre a gestão de políticas públicas complexas, evidenciando que o êxito de iniciativas baseadas em dados depende menos da tecnologia empregada e mais da qualidade dos arranjos institucionais que estruturam sua implementação.

As recomendações apresentadas apontam para a necessidade de ajustes que fortaleçam a governança distribuída, a coordenação entre instituições e a capacidade adaptativa do modelo regulatório. A adoção de instâncias permanentes de coordenação, a formalização de protocolos operacionais, a separação clara de funções institucionais e a incorporação de mecanismos de avaliação contínua constituem elementos centrais para a construção de uma política de segurança pública baseada em dados que seja operacionalmente eficiente e institucionalmente sustentável.

Por fim, a experiência brasileira analisada indica que o sucesso das políticas de segurança orientadas por dados não reside apenas na regulação do tratamento de informações, mas na qualidade dos arranjos institucionais que viabilizam sua implementação. O aprimoramento desses arranjos não constitui apenas exigência técnica, mas condição estruturante para que o uso de dados fortaleça, e não fragilize, a legitimidade institucional da política de segurança pública no Brasil.

Referências

- Barbosa, C. M. (2019). A juristocracia no Brasil e o futuro da Constituição. *Revista Eletrônica do Curso de Direito da UFSM*, 14(2).
- Bioni, B. R. (2019). *Proteção de dados pessoais: A função e os limites do consentimento*. Forense.
- Bioni, B. R., Monteiro, D. D., & Zanatta, R. A. F. (2020). *Proteção de dados no campo penal e de segurança pública*. Associação Data Privacy Brasil de Pesquisa.
- Câmara dos Deputados. (2020). *Exposição de motivos: Anteprojeto de lei de proteção de dados para segurança pública e perseguição penal*. Comissão de Juristas.
- Cerqueira, D., & Bueno, S. (Coords.). (2025). *Atlas da violência*. IPEA.
- Doneda, D. (2021). Liberdade, vigilância e autodeterminação informativa. In D. Doneda & L. S. Mendes (Orgs.), *Proteção de dados pessoais: A função e os limites do consentimento*. Revista dos Tribunais.
- European Union. (2016). *Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences*.
- Ferreira, A. R. (2024). Tratamento de dados pessoais em investigações criminais: O direito fundamental à autodeterminação informativa como limite constitucional. *Revista Brasileira de Ciências Criminais*, 185.
- Gesta Leal, R. (2023). Limites do direito fundamental à proteção de dados em face da instrução probatória no processo penal. *Novos Estudos Jurídicos*, 28(1).
- Gleizer, O. (2021). *O direito de proteção de dados no processo penal e na segurança pública*. Marcial Pons.
- Hood, C. (1998). *The art of the state: Culture, rhetoric, and public management*. Oxford University Press.
- Lipsky, M. (2019). *Burocracia de nível de rua: Dilemas do indivíduo nos serviços públicos* (A. E. M. da Cunha, Trad.). ENAP. (Trabalho original publicado em 1980)
- Lodder, G. N. (2020). Autoridade nacional de proteção de dados: Questões penais. In V. B. Aras et al. (Orgs.), *Proteção de dados pessoais e investigação criminal*. ANPR.
- Mendes, L. S. F., & Fonseca, G. C. S. (2020). Proteção de dados para além do consentimento: Tendências contemporâneas de materialização. *REI – Revista Estudos Institucionais*, 6(2).
- Moura, M. T. A. (2021). Oportunidades e desafios do CNJ como órgão regulador de proteção de dados. In F. B. Cruz & B. Simão (Eds.), *Direitos fundamentais e processo penal na era digital*. Internetlab.



EBAP

Encontro Brasileiro de Administração Pública
XIII EBAP, Junho de 2026, Brasília-DF, Brasil

ARTIGO

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Zagato, J. S. (2022). *Privacidade e proteção de dados: Os desafios da modelagem de cultura da privacidade no Brasil*. Lumen Juris.

