MESTRADO PROFISSIONAL

EM ADMINISTRAÇÃO PÚBLICA

INTELIGÊNCIA POLICIAL E OS DESAFIOS DA SEGURANÇA PÚBLICA NAS CIDADES 4.0

CAROLINA VANESSA MEIRELES SILVA

Brasília-DF, 2024

CAROLINA VANESSA MEIRELES SILVA

INTELIGÊNCIA POLICIAL E OS DESAFIOS DA SEGURANÇA PÚBLICA NAS CIDADES 4.0

Dissertação apresentada ao Programa de Pós Graduação em Administração Pública, do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, como requisito parcial para obtenção do grau de Mestre.

Orientador
Professora Doutora Grace Ladeira Garbaccio e Professora Mestre Débora Dossiatti de Lima .

Brasília-DF 2024

CAROLINA VANESSA MEIRELES SILVA

INTELIGÊNCIA POLICIAL E OS DESAFIOS DA SEGURANÇA PÚBLICA NAS CIDADES 4.0

Dissertação apresentada ao Programa de Pós Graduação em Administração Pública, do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, como requisito parcial para obtenção do grau de Mestre.

Aprovado em 18 / 12 / 2024

Banca Examinadora

Profa. Dra. Grace Ladeira Garbaccio - Orientadora

Profa. Me. Débora Dossiatti de Lima - Orientadora

Prof. Dr. Alessandro de Oliveira Gouveia Freire

Prof. Dr. Paulo Henrique Ferreira Alves

S586i Silva, Carolina Vanessa Meireles
Inteligência policial e os desafios da segurança pública nas cidades 4.0 / Carolina Vanessa Meireles Silva. – Brasília: IDP, 2024.

116 f.
Inclui bibliografia.

Dissertação – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP, Mestrado Profissional em Administração Pública, Brasília, 2024.
Orientador: Profa. Dra. Grace Ladeira Garbaccio.

1. Serviço de inteligência. 2. Segurança pública. 3. Problemas sociais . I. Título.

CDD: 363.1

Ficha catalográfica elaborada pela Biblioteca Ministro Moreira Alves
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa

AGRADECIMENTOS

A conclusão desta dissertação de mestrado representa o resultado de uma jornada repleta de desafios, superações e aprendizados. Nenhuma conquista é alcançada sem o apoio de pessoas especiais, e hoje, com muita gratidão, reconheço o valor de cada um que esteve ao meu lado nesta caminhada.

Agradeço primeiramente a Deus, pela força e coragem para enfrentar cada etapa deste trabalho, e por guiar meus passos em todos os momentos.

À minha mãe, que sempre esteve presente, com seu amor incondicional e apoio constante. Sua dedi-cação e sacrifícios me ensinaram o verdadeiro valor da perseverança e do esforço. Você é meu maior exemplo de força e determinação.

Ao meu irmão, Pedro, com sua presença única e especial, me inspira a cada dia a ser uma pessoa me-lhor. Sua alegria e pureza são fontes inesgotáveis de motivação e amor.

Ao meu irmão Beto, sua esposa Mireille e seus filhos João e Marina, pela presença calorosa e pelos momentos de união familiar que me deram forças para continuar, mesmo nos dias mais difíceis. Seu carinho e incentivo foram fundamentais ao longo desta jornada.

Ao meu avô, Agnaldo Meireles, por suas lições de vida e amor. Cada um, à sua maneira, foi essencial em minha formação, e sou profundamente grata pelo legado de sabedoria e carinho que me deixaram.

Às minhas orientadoras e professores do Programa de Pós-Graduação em Administração Pública, agradeço pela paciência, sabedoria e apoio ao longo do desenvolvimento deste trabalho. Suas orienta-ções foram essenciais para o êxito desta pesquisa.

À Polícia Militar do Distrito Federal (PMDF), pela confiança e suporte institucional durante minha jornada acadêmica.

Finalmente, a todos os amigos, colegas e demais pessoas que de alguma forma contribuíram para que eu pudesse concluir esta etapa,

meu sincero muito obrigada. Sem o apoio de cada um, esta conquista não seria possível.

“Conforme as circunstâncias, deve-se modificar os próprios planos.”

Sun Tzu

RESUMO

A pesquisa examina o impacto da inteligência policial na melhoria das atividades de segurança pública em Cidades 4.0, um ambiente urbano marcado pela integração tecnológica intensa. Caracterizadas pelo uso de big data, Internet das Coisas (IoT) e Inteligência Artificial (IA), essas cidades desafiam os métodos convencionais de policiamento e exigem abordagens inovadoras na gestão da segurança. Este estudo investiga como a inteligência corrente – sustentada pela coleta e análise de dados em tem-po real – pode otimizar a eficiência das operações policiais, respondendo de forma ágil às demandas de segurança pública na era digital. O objetivo central é analisar o papel dessa ferramenta analítica baseada em dados em tempo real na eficácia das forças policiais, observando sua contribuição para a segurança pública em Cidades 4.0. A metodologia aplicada inclui uma abordagem dedutiva e qualita-tiva, com análise temática baseada em uma extensa revisão bibliográfica e na exploração de casos práticos de operações policiais. O estudo também aborda os desafios éticos e operacionais da integra-ção de tecnologias emergentes, como sensores inteligentes e drones, além das lacunas em regulamen-tação. Os resultados indicam que o uso estratégico desse tipo de inteligência amplia a capacidade de resposta das forças de segurança, permitindo uma adaptação mais eficiente às complexidades das Ci-dades 4.0. Contudo, a integração tecnológica ainda enfrenta barreiras significativas, como a necessi-dade de formação especializada e de políticas públicas atualizadas. Como contribuição, a pesquisa oferece uma análise crítica para formulação de políticas públicas e práticas de segurança mais moder-nas. Sugere-se, para futuras agendas de pesquisa, um aprofundamento sobre as implicações da IA na segurança pública e estudos longitudinais sobre a adaptação das forças policiais às novas realidades tecnológicas.

Palavras chave: inteligência corrente; Cidades 4.0; segurança pública; tecnologias emergentes; eficiência operacional.

ABSTRACT

The research examines the impact of police intelligence on improving public security activities in Cit-ies 4.0, an urban environment marked by intense technological integration. Characterized by the use of big data, the Internet of Things (IoT) and Artificial Intelligence (AI), these cities challenge conven-tional policing methods and require innovative approaches to security management. This study inves-tigates how current intelligence - underpinned by real-time data collection and analysis - can optimize the efficiency of police operations, responding in an agile way to the demands of public safety in the digital age. The central objective is to analyze the role of this analytical tool based on real-time data in the effectiveness of police forces, looking at its contribution to public safety in Cities 4.0. The meth-odology applied includes a deductive and qualitative approach, with thematic analysis based on an extensive literature review and the exploration of practical cases of police operations. The study also addresses the ethical and operational challenges of integrating emerging technologies such as smart sensors and drones, as well as regulatory gaps. The results indicate that the strategic use of this type of intelligence increases the response capacity of security forces, allowing them to adapt more efficiently to the complexities of Cities 4.0. However, technological integration still faces significant barriers, such as the need for specialized training and updated public policies. As a contribution, the research offers a critical analysis for the formulation of more modern public policies and security practices. It is suggested that future research agendas include a more in-depth look at the implications of AI for pub-lic security and longitudinal studies on the adaptation of police forces to new technological realities.

Keywords: current intelligence; Cities 4.0; public safety; emerging technologies; operational efficiency.

LISTA DE ABREVIATURAS E SIGLAS

ABIN	Agência Brasileira de Inteligência
AID	Atividade de Inteligência de Defesa
ANAC	Agência Nacional de Aviação Civil
ANDIFES	Associação Nacional de Dirigentes de Instituições Federais de Ensino Superior
BID	Banco Interamericano de Desenvolvimento
CPP	Código de Processo Penal
DNISP	Doutrina Nacional de Inteligência de Segurança Pública
ENINT	Estratégia Nacional de Inteligência
GDF	Governo do Distrito Federal
GM-MD	Gabinete do Ministro do Ministério da Defesa
IA	Inteligência Artificial
ILP	Intelligence-Led Policing (Policiamento Orientado por Inteligência)
IoT	Internet das Coisas
IP	Internet Protocol (Protocolo de Internet)
OID	Objetivos de Inteligência de Defesa
PID	Política de Inteligência de Defesa
PM	Polícia Militar
PMDF	Polícia Militar do Distrito Federal
PMMG	Polícia Militar de Minas Gerais
PNI	Política Nacional de Inteligência
RPAs	Remotely Piloted Aircraft Systems (Sistemas de Aeronaves Pilotadas Remotamente)
SINDE	Sistema de Inteligência de Defesa
SISBIN	Sistema Brasileiro de Inteligência
SISP	Subsistema de Inteligência de Segurança Pública
SMSU	Secretaria Municipal de Segurança Urbana
TIC	Tecnologia da Informação e Comunicação
UNODC	Escritório das Nações Unidas sobre Drogas e Crimes

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE TABELAS

SUMÁRIO


1

1 INTRODUÇÃO

As cidades inteligentes, frequentemente denominadas Cidades 4.0, surgem como um fenômeno global, caracterizado pela integração de tecnologias emergentes, como a Internet das Coisas (IoT), *big data*, Inteligência Artificial (IA) e outros dispositivos conectados que transformam a forma como as pessoas vivem e interagem nas áreas urbanas (Giffinger *et al.,* 2007). Nesse cenário, a segurança pública ganha uma dimensão mais complexa, onde a eficiência do policiamento passa a depender não só da presença física dos agentes de segurança, mas também do uso efetivo de inteligência corrente, envolvendo a coleta, análise e utilização de dados em tempo real para a tomada de decisões (Calafate *et al*., 2020).

No Brasil, a segurança pública sempre foi um dos maiores desafios enfrentados pelas administrações locais e federais. Com o surgimento das Cidades 4.0, essa questão torna-se ainda mais relevante, uma vez que as novas tecnologias oferecem a oportunidade de melhorar as operações policiais, a gestão urbana e a resposta a incidentes em tempo real (Brasil, 2023). Assim, a inteligência corrente surge como uma peça-chave para integrar dados de diferentes fontes e transformar informações em conhecimento estratégico para ações de segurança pública, prevenindo e combatendo o crime de forma mais eficiente.

Diante disso, a presente dissertação tem como objetivo principal investigar o papel desse tipo de ferramenta analítica nas operações da polícia militar, avaliando como enfrentar os desafios impostos pela urbanização digital nas Cidades 4.0, especialmente no contexto de segurança pública. Com isso, busca-se entender como essas inovações podem ser aplicadas para otimizar o policiamento e garantir a segurança da população em meio a cenários urbanos cada vez mais complexos.

Hodiernamente, aumento da criminalidade em ambientes urbanos é uma preocupação crescente para as administrações públicas, especialmente em áreas metropolitanas. A expansão das Cidades 4.0, que utiliza um vasto ecossistema de dados para gerir infraestrutura urbana, também abre caminho para novas

vulnerabilidades em termos de segurança cibernética e crimes organizados no ciberespaço (Kunrath, 2017). Embora as tecnologias avançadas proporcionem inúmeras vantagens para a gestão urbana, também criam desafios significativos para as forças de segurança pública, que devem se adaptar rapidamente a essas transformações para proteger as comunidades.

No entanto, a implementação eficaz dessa gestão informacional nas operações policiais ainda enfrenta obstáculos consideráveis, como a falta de integração tecnológica entre diferentes órgãos de segurança, além da escassez de formação específica para policiais no uso de novas tecnologias (Santos, 2020). Essas dificuldades, aliadas à carência de políticas públicas adequadas para gerenciar as Cidades 4.0, criam uma lacuna que esta dissertação busca ajudar a preencher. A utilização de soluções baseadas em tecnologias, IA e análise de dados é fundamental para uma abordagem mais precisa e eficaz na identificação de ameaças e na otimização dos recursos policiais.

Ao analisar as implicações da coleta e uso de dados em cidades inteligentes, o presente estudo justifica-se pela necessidade de explorar como a inteligência corrente pode potencializar o trabalho policial em um cenário urbano cada vez mais tecnológico, permitindo uma resposta mais rápida e eficaz aos desafios impostos pelo crime organizado e outras formas de violência (Ahvenniemi *et al*., 2017).

Conforme dito acima, o objetivo geral desta dissertação é investigar a utilização da inteligência corrente nas operações de segurança pública, com foco na polícia militar, e avaliar os desafios impostos pela integração dessas tecnologias no contexto das Cidades 4.0. Para isso, pretende-se examinar como as ferramentas de monitoramento em tempo real, como câmeras de vigilância conectadas, sistemas de análise de *big data* e sensores urbanos, podem ser aplicadas para melhorar a eficácia das ações policiais (Brasil, 2023).

Os objetivos específicos incluem:

1. **Avaliar a aplicação da inteligência nas operações policiais e sua contribuição para a eficiência da segurança pública;**
2. **Explorar o uso de tecnologias como ferramentas estratégicas no monitoramento e controle de áreas urbanas complexas;**
3. **Analisar a adaptação das políticas públicas às Cidades 4.0;**

4. **Identificar as aplicações práticas da inteligência nas operações da polícia no contexto das Cidades 4.0, assim como,**
5. **Explorar os principais desafios enfrentados pela Segurança Pública no uso da inteligência para lidar com a complexidade das Cidades 4.0 propondo soluções para superá-los identificando as implicações do uso de dados em tempo real.**

A principal contribuição desta dissertação reside em oferecer uma análise crítica sobre a inserção da inteligência corrente nas operações de segurança pública, abordando a adaptação das forças policiais às novas tecnologias e ao aumento do uso de dados em tempo real. Além disso, busca-se fornecer subsídios teóricos e práticos que possam auxiliar na formulação de políticas públicas voltadas à modernização das práticas policiais nas Cidades 4.0.

A combinação desses aspectos contribui para uma abordagem mais eficaz da segurança pública nas Cidades 4.0, permitindo que a gestão pública se beneficie das tecnologias emergentes, enquanto enfrenta de forma adequada os desafios apresentados pelo crime nas novas realidades urbanas.

A segurança pública é um tema de extrema relevância e preocupação constante, especialmente em áreas metropolitanas e regiões adjacentes. Os casos de violência e criminalidade, como sequestros, têm um impacto profundo na sociedade, evidenciando a necessidade de políticas eficazes e ações coordenadas entre diferentes forças de segurança. (Cordeiro, 2014)

Nesse sentido, a inteligência corrente não só facilita a ação imediata, mas também contribui para a resolução e para o assessoramento na contenção de crimes mais amplos e detalhados, auxiliando no combate ao crime organizado e em outras atividades ilícitas que ameaçam a paz social nas cidades modernas. (Doutrina da Atividade de Inteligência de 2023)

Segundo a Doutrina supramencionada, a inteligência corrente visa manter a autoridade informada diuturnamente sobre eventos e situações em curso, bem como sobre suas evoluções. Esse tipo de processamento de informações estratégicas envolve a coleta, análise e disseminação contínua de informações para decisões rápidas e

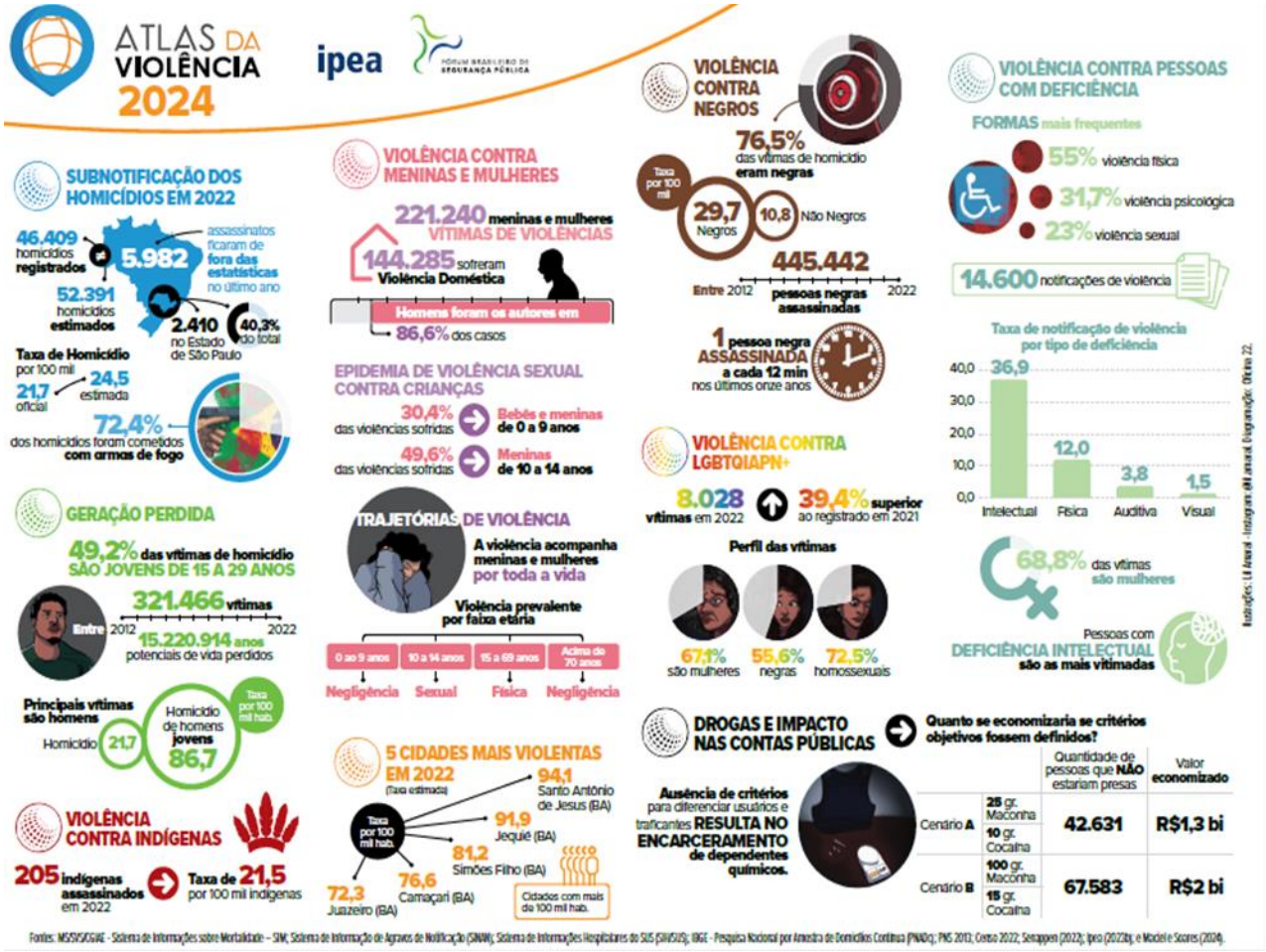
precisas, sendo essencial para a integração e coordenação entre unidades de segurança.

O problema da segurança pública exige um esforço maior para entender suas complexidades e desenvolver soluções concretas. Desse modo, a questão central deste estudo é como a inteligência corrente policial pode melhorar a qualidade das atividades policiais e, consequentemente, a segurança pública. Conforme o explicitado, o objetivo desse estudo é analisar a atuação dessa ferramenta analítica na resolução de crimes e na eficiência das operações policiais, indicando melhorias nos processos de formalização, execução e prestação de serviços policiais, alinhadas às políticas públicas vigentes, otimizando os serviços da Polícia.

Figura 1

Fonte: Anuário Brasileiro de Segurança Pública de 2023.

Figura 2



Fonte: Atlas da Violência de 2024.

As estatísticas apresentadas nas figuras 1 e 2 evidenciam a complexidade e a gravidade dos desafios enfrentados pela segurança pública no Brasil, especialmente no contexto de uma sociedade cada vez mais urbanizada e tecnológica. Os dados destacam a prevalência de crimes violentos e a vulnerabilidade de grupos específicos, como mulheres e crianças, além de sublinharem a importância de estratégias de inteligência corrente para a análise e resposta a essas questões. Essa realidade reforça a relevância de soluções inovadoras, como o uso de tecnologias avançadas e ferramentas analíticas, para promover a eficiência e a eficácia das operações de segurança pública em Cidades 4.0.

Nesse diapasão, a discussão sobre as diferenças conceituais entre cidades inteligentes, cidades digitais e Cidades 4.0 é relevante para a compreensão das transformações urbanas contemporâneas, especialmente no contexto da administração pública. Embora esses termos sejam frequentemente utilizados de forma intercambiável, eles

possuem significados distintos que refletem diferentes níveis de sofisticação tecnológica e de integração social (Brasil, 2024).

As cidades digitais referem-se a ambientes urbanos que utilizam Tecnologia da Informação e Comunicação (TIC) para oferecer serviços públicos e facilitar o acesso à informação. Essas cidades implementam sistemas que permitem a modernização da gestão pública, como agendamentos online e aplicativos para serviços diversos. No entanto, a digitalização por si só não garante uma integração eficiente entre os serviços, o que limita a capacidade de resolver problemas urbanos de forma holística (Exati, 2024). As suas principais características são a disponibilização de serviços online, a melhoria no acesso à informação e a modernização da gestão pública.

As cidades inteligentes (*smart cities*) vão além da digitalização, integrando tecnologias para otimizar a qualidade de vida dos cidadãos e a eficiência dos serviços públicos. Elas utilizam dados em tempo real, sensores e dispositivos conectados para melhorar a mobilidade, segurança e sustentabilidade. O foco está na interconexão dos serviços, permitindo uma gestão mais integrada e responsiva às necessidades da população, de acordo com a Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS, 2024. Os seus atributos mais destacados são a integração de serviços públicos por meio de tecnologia, o uso de dados em tempo real para tomada de decisões e o foco em sustentabilidade e qualidade de vida.

Atualmente, o conceito de Cidades 4.0 é uma evolução dos anteriores, alinhando-se à Quarta Revolução Industrial, que enfatiza a interconexão entre o mundo físico e digital. Esse termo abrange a aplicação de tecnologias avançadas, como a IoT, IA e *big data*, para transformar a infraestrutura urbana e os serviços oferecidos. As Cidades 4.0 buscam não apenas eficiência, mas também inovação e adaptabilidade às mudanças sociais e ambientais (Oliveira, 2024). Suas particularidades são a aplicação de tecnologias avançadas (IoT, AI, *big data*), a transformação da infraestrutura urbana e o foco em inovação e adaptabilidade.

A metodologia deste estudo baseia-se na revisão bibliográfica para explorar dados sobre inteligência, segurança pública, polícia e cidades digitais, contribuindo para o desenvolvimento de políticas públicas mais eficazes (Gil, 2010). A revisão de literatura acadêmica e documentos relacionados as políticas públicas identifica lacunas no

conhecimento e estabelece fundamentos para o estudo, oferecendo *insights* sobre abordagens e teorias ligadas aos temas supramencionados. A análise crítica contextualiza o problema de pesquisa, examinando abordagens anteriores sobre segurança pública e cidades antes da revolução digital, e define diretrizes para o trabalho (Martins, 2011). Organizado em capítulos, o estudo busca proporcionar uma compreensão abrangente da atuação da inteligência policial e suas implicações práticas, avaliando a eficácia da inteligência corrente na resolução de crimes e na eficiência da Polícia.

Pretende-se, ao final do estudo, responder a seguinte pergunta: Como a inteligência corrente na Segurança Pública pode lidar com os desafios apresentados pelas Cidades 4.0?

Nessa pesquisa, pretende-se aprofundar a compreensão sobre os fatores que impactam a eficácia da atividade de inteligência e a gestão pública na segurança nesse novo formato de cidades. Esse estudo visa compreender os fatores facilitadores e as soluções inovadoras adotadas pela segurança pública no âmbito dessa atividade. Além disso, busca-se identificar acertos não previstos e a possibilidade de institucionalizar as práticas bem-sucedidas, contribuindo para o aprimoramento da gestão pública na área de segurança pública.

Este estudo está dividido em capítulos. O primeiro capítulo introduz o tema, a problemática, os objetivos e a justificativa do estudo. No segundo capítulo, será feita uma revisão bibliográfica abrangente sobre o conceito de Cidades 4.0, inteligência corrente e sua aplicação na segurança pública. No terceiro capítulo, discute-se o arcabouço metodológico adotado, destacando o método qualitativo utilizado para a análise dos dados. O quarto capítulo apresenta os resultados da pesquisa e as discussões baseadas nos estudos de caso e nas práticas atuais da Polícia e na sequência, serão expostas as conclusões e as recomendações para futuras pesquisas e políticas públicas.


2

2 REVISÃO DE LITERATURA

2.1 INTELIGÊNCIA

O conceito de inteligência é multifacetado e envolve uma série de processos complexos, que vão muito além da simples coleta de informações. No contexto da segurança pública, esse processo de gestão estratégica é essencial para antecipar ameaças e apoiar a formulação de políticas e operações eficazes. A evolução das Cidades 4.0 trouxe desafios significativos para as forças de segurança, que precisam se adaptar rapidamente a um ambiente marcado pela interconectividade e pela alta densidade de dados digitais. As Cidades 4.0, caracterizadas por uma ampla integração de tecnologias como *big data*, IA e Internet das Coisas (IoT), exigem uma gestão da segurança pública baseada em dados em tempo real.

A inteligência corrente desempenha um papel fundamental nesse novo cenário, fornecendo informações precisas e oportunas para apoiar decisões operacionais. Segundo Santos (2020), a inteligência é um componente essencial da administração pública moderna, facilitando a tomada de decisões e reduzindo incertezas em ambientes de alto risco. As Cidades 4.0 demandam uma vigilância constante e um processamento de dados que permita uma resposta ágil a situações de emergência, como desastres naturais, ataques cibernéticos ou incidentes de segurança.

No entanto, a aplicação prática dessa ferramenta analítica nas Cidades 4.0 enfrenta diversos desafios. A interconectividade que caracteriza esses ambientes urbanos cria vulnerabilidades que podem ser exploradas por atores mal-intencionados, como *hackers* ou grupos terroristas. A segurança cibernética, portanto, torna-se uma preocupação central. Além disso, a gestão eficiente de dados requer infraestruturas robustas, tecnologias avançadas e profissionais altamente capacitados, capazes de interpretar e aplicar as informações de forma eficaz.

2.1.1 INTELIGÊNCIA E CONTRAINTELIGÊNCIA

A inteligência é um elemento indispensável na gestão pública e da segurança nacional, desempenhando um papel crucial no assessoramento estratégico e na proteção de interesses estatais. Nesse estudo explora-se os principais conceitos dessa gestão informacional, sua evolução histórica, os métodos de coleta e análise de informações, além de suas aplicações práticas no contexto da administração pública. A análise é fundamentada em autores renomados, como Gregory Treverton, Sherman Kent, Hank Prunckun, Marco Cepik e Layla Santos.

Inteligência, no contexto da administração pública e da segurança, é o processo de coleta, análise e disseminação de informações com o objetivo de apoiar a tomada de decisões. Kent (1967), um dos pioneiros da teoria sobre esse tema, a conceituou como um conhecimento que reduz a incerteza e orienta as ações estratégicas. Essa definição enfatiza o papel da inteligência na mitigação de riscos e na antecipação de ameaças, elementos cruciais para a segurança pública e a estabilidade governamental.

Treverton (2001) amplia essa perspectiva ao afirmar que a inteligência é um processo dinâmico, que envolve não apenas a obtenção de informações, mas também a análise rigorosa e a disseminação eficaz. No ambiente complexo das Cidades 4.0, onde o volume de dados gerados é imenso, essa ferramenta analítica se torna ainda mais relevante. Nesse contexto, a análise preditiva e o uso de tecnologias avançadas, como *big data* e IA, são fundamentais para otimizar o processo de coleta e análise.

Prunckun (2015) argumenta que a inteligência é uma ciência aplicada, que utiliza métodos tanto quantitativos quanto qualitativos para transformar dados brutos em conhecimento útil. Ele destaca a importância da precisão e da objetividade no processo de análise, observando que decisões baseadas em análises imprecisas podem ter consequências desastrosas. Esse aspecto é particularmente relevante na administração pública, onde as decisões precisam ser fundamentadas para garantir segurança e bem-estar à sociedade.

A história da inteligência remonta a tempos antigos, com exemplos de espionagem documentados em textos religiosos e registros históricos. Santos (2020) menciona que a atividade de inteligência tem raízes profundas na história da humanidade, sendo utilizada por líderes desde o período bíblico até as grandes guerras do século XX. A autora destaca que, com a modernização das sociedades,

a mesma evoluiu para se tornar uma disciplina mais estruturada e científica, especialmente a partir do século XX.

Durante a Guerra Fria, essa ciência ganhou um novo significado, com a criação de agências nacionais focadas na coleta e análise de informações sobre potências estrangeiras. Foi nesse período que o conceito de ciclo de inteligência se consolidou, conforme descrito por Kent (1967). Esse ciclo envolve etapas bem definidas, como o planejamento, a coleta, o processamento, a análise e a disseminação de informações. O modelo de ciclo acima mencionado ainda é amplamente utilizado hoje, embora tenha sido adaptado para lidar com as complexidades das ameaças modernas.

Cepik (2003) discute a transformação da inteligência no Brasil, especialmente após o regime militar. Com a redemocratização, houve um esforço para democratizar a atividade e torná-la mais transparente e alinhada aos valores democráticos. Essa mudança é refletida na criação do Sistema Brasileiro de Inteligência (SISBIN) e na promulgação de leis que regulam a mesma, como a Lei 9.883/1999.

Nesse diapasão, o ciclo supramencionado é um processo estruturado que orienta as atividades de coleta, análise e disseminação de informações. Kent (1967) o descreveu como um conjunto de etapas interdependentes que garantem a produção de inteligência de qualidade. As etapas incluem:

1. **Planejamento e Direção: Esta fase envolve a definição das necessidades de informação e o estabelecimento de prioridades. A administração pública utiliza essa etapa para identificar áreas críticas que requerem análise detalhada, como segurança nacional, saúde pública ou política econômica.**
2. **Coleta: A coleta de informações pode ser feita por meio de diversas fontes, como inteligência humana (HUMINT), inteligência de sinais (SIGINT), e inteligência de imagens (IMINT). Prunckun (2015) observa que a eficácia dessa etapa depende da capacidade de obter dados relevantes sem comprometer a segurança das fontes.**
3. **Processamento: Após a coleta, as informações são processadas e organizadas. Isso pode envolver a tradução de documentos, o processamento de imagens ou a**

decodificação de mensagens. Essa etapa é crítica para transformar dados brutos em informações utilizáveis.

4. **Análise e Produção: Esta é a fase mais complexa do ciclo, onde analistas examinam as informações coletadas para identificar padrões, prever ameaças e gerar relatórios. Treverton (2001) destaca que essa etapa requer um alto grau de precisão e objetividade, pois os produtos de inteligência devem ser confiáveis e imparciais.**
5. **Disseminação: Finalmente, as informações analisadas são disseminadas para os tomadores de decisão. Na administração pública, isso pode incluir o presidente, ministros, ou gestores de segurança. A disseminação deve ser rápida e eficiente para garantir que as decisões sejam tomadas com base em informações atualizadas.**

Desse modo, a inteligência é uma disciplina diversa, podendo ser dividida em várias categorias, dependendo da fonte e do objetivo da coleta de informações. Prunckun (2015) a classifica em três tipos principais: estratégica, tática e operacional. Cada tipo desempenha um papel distinto na administração pública e na segurança nacional.

A Inteligência Estratégica é focada no longo prazo, ajudando os tomadores de decisão a desenvolver políticas de segurança nacional e a planejar operações de grande escala. Treverton (2001) argumenta que a mesma é essencial para a formulação de políticas públicas e para a proteção dos interesses nacionais.

A Inteligência Tática é utilizada em operações de curto prazo, como ações policiais ou missões militares específicas. Santos (2020) explica que esse tipo é fundamental para operações que exigem uma resposta rápida, como intervenções em crises ou combate ao crime organizado.

Na sequência, a Inteligência Operacional é uma combinação das duas anteriores, usada para planejar e executar operações complexas. Cepik (2003) observa que a esse último tipo é frequentemente utilizado em situações que exigem um alto grau de coordenação entre diferentes agências governamentais.

Nesse contexto, a coleta de informações é uma etapa crítica no processo de inteligência, e a eficácia dessa etapa depende das fontes e métodos utilizados. Santos (2020) descreve várias técnicas de coleta, incluindo:

a) **Inteligência Humana (HUMINT): Envolve a coleta de informações por meio de interações humanas, como entrevistas, interrogatórios ou infiltração. Essa técnica é particularmente útil em situações onde outras formas de coleta não são viáveis.**
b) **Inteligência de Sinais (SIGINT): Refere-se à coleta de informações por meio de interceptação de comunicações eletrônicas. Prunckun (2015) destaca que a SIGINT é uma das formas mais eficazes de coleta, especialmente em operações militares.**
c) **Inteligência de Imagens (IMINT): Envolve o uso de imagens de satélite ou drones para coletar informações sobre atividades ou locais específicos. Esse método é amplamente utilizado em operações de vigilância e reconhecimento.**

A análise de inteligência, por outro lado, requer o uso de métodos quantitativos e qualitativos para interpretar as informações coletadas. Treverton (2001) sugere que técnicas como análise de redes sociais, modelagem preditiva e análise de cenários são ferramentas valiosas para prever comportamentos e eventos futuros. Prunckun (2015) acrescenta que o uso de algoritmos de aprendizado de máquina e IA está se tornando cada vez mais comum na análise de grandes volumes de dados.

Portanto, esse processamento de informações estratégicas tem inúmeras aplicações na administração pública, desde a segurança nacional até a gestão de crises e a formulação de políticas públicas. Santos (2020) explica que ela é fundamental para antecipar ameaças e mitigar riscos, permitindo que os governos tomem decisões mais informadas e eficazes.

Exemplificando o entendimento acima, na Segurança Pública, a inteligência é amplamente utilizada pelas forças de segurança para prevenir crimes e garantir a segurança dos cidadãos. A coleta de informações sobre atividades criminosas, o monitoramento de redes de tráfico de drogas e a análise de dados de vigilância são exemplos de como a mesma pode ser aplicada na segurança pública.

Em Gestão de Crises, ou seja, em situações de emergência, como desastres naturais ou ataques terroristas, a inteligência fornece informações críticas que ajudam a coordenar a resposta. Cepik (2003) ressalta que a gestão eficaz de crises depende de uma coleta rápida e

precisa de informações, bem como de uma análise eficaz para prever os impactos e planejar a recuperação.

Além disso, ela também é usada para informar a Formulação de Políticas Públicas. Treverton (2001) destaca que a mesma pode fornecer insights sobre tendências econômicas, riscos ambientais e ameaças à segurança nacional, ajudando os governos a desenvolver políticas mais eficazes.

É importante ressaltar que apesar de sua importância, a inteligência enfrenta vários desafios e limitações. Um dos principais problemas é a precisão das informações coletadas. Prunckun (2015) argumenta que, mesmo com os avanços tecnológicos, a coleta de informações pode ser imprecisa ou enviesada. Além disso, o uso de tecnologias emergentes, como *big data* e IA, levanta preocupações éticas e legais, especialmente no que diz respeito à privacidade e à segurança dos dados.

Outro desafio é a transparência e o controle. Santos (2020) enfatiza que a inteligência deve ser conduzida de maneira ética e transparente, respeitando os direitos humanos e a legislação vigente. No Brasil, a Lei de Acesso à Informação (Lei nº 12.527/2011) regula o acesso a informações públicas, mas ainda há um debate sobre como equilibrar a necessidade de sigilo com o direito à transparência.

O amanhã é promissor, mas também apresenta desafios significativos. Treverton (2001) sugere que o avanço das tecnologias de informação e comunicação transformará a maneira como a inteligência é coletada e analisada. O uso de algoritmos de aprendizado de máquina, a integração de redes sociais na coleta de dados e o desenvolvimento de tecnologias de vigilância mais sofisticadas são tendências que moldarão o futuro dessa ferramenta.

Santos (2020) destaca que o futuro da inteligência também dependerá da capacidade de os governos adaptarem suas políticas e estratégias às novas ameaças. Isso inclui não apenas a modernização de infraestruturas de Tecnologias da Informação - TI, mas também o desenvolvimento de uma força de trabalho altamente qualificada, capaz de lidar com as complexidades das Cidades 4.0.

Como dito alhures, a inteligência é amplamente definida como o processo de coleta, análise e disseminação de informações para apoiar decisões estratégicas. Ela não é apenas uma questão de coleta

de dados, mas uma atividade estruturada que transforma informações em conhecimento acionável para o Estado (Treverton, 2001). No entanto, sua aplicação prática é muito mais complexa e envolve uma série de etapas interligadas. Antunes (2001) afirma que, embora a informação seja a matéria-prima da mesma, ela só se torna útil quando é processada e analisada de forma a gerar conhecimento aplicável. A diferença entre dados brutos e inteligência está na capacidade de transformar informação em uma ferramenta que possa orientar ações concretas.

Ao longo das últimas décadas, a atividade de inteligência evoluiu significativamente, especialmente no Brasil. Durante o regime militar, ela era vista principalmente como uma ferramenta de controle e repressão. Contudo, com a redemocratização, houve uma reestruturação do sistema de inteligência, e a atividade passou a ser considerada um assessoramento estratégico ao processo decisório, com o objetivo de proteger a segurança pública, a economia e outros setores cruciais (Santos, 2020).

A inteligência no contexto contemporâneo é diversificada e inclui várias ramificações, como a inteligência militar e a de segurança pública. A militar, conforme discutido por Stepan (1971), é crucial para o planejamento estratégico das Forças Armadas, envolvendo atividades como o monitoramento de ameaças externas, a coleta de informações de campo e a análise de dados sobre potenciais adversários. A de segurança pública, por outro lado, é focada em ameaças internas, como o crime organizado, a violência urbana e o terrorismo doméstico (Santos, 2020). Esse último tipo atualmente utiliza tecnologias avançadas, como a análise de *big data* e aeronaves remotamente pilotadas (drones), para otimizar as operações de policiamento. Essa última ramificação é essencial para operações de policiamento preventivo e repressivo (Ratcliffe, 2016).

Nesse contexto, é necessário ressaltar conceitos agregadores presentes na recente Portaria do Gabinete do Ministro do Ministério da Defesa (GM-MD) nº 4.846, de 29 de setembro de 2023, que aprova a Política de Inteligência de Defesa – MD 60-P-01 (1ª Edição/2023).

A recente Portaria do Gabinete do Ministro do Ministério da Defesa (GM-MD) nº 4.846, de 29 de setembro de 2023, aprova a Política de Inteligência de Defesa (PID), a qual estabelece diretrizes e conceitos-chave para orientar a Atividade de Inteligência de Defesa (AID) no

Brasil. A PID se destaca por formalizar uma estrutura robusta de atuação da AID, essencial para a produção de conhecimentos que subsidiam decisões estratégicas no âmbito da defesa nacional (Brasil, 2023).

Entre os conceitos agregadores definidos na PID, destaca-se a Inteligência de Defesa, que se configura como a atividade destinada a reunir, processar e analisar informações estratégicas para orientar decisões cruciais relacionadas à segurança e à soberania do país. Além disso, a portaria institui o Sistema de Inteligência de Defesa (SINDE), uma estrutura que integra a execução da AID no Ministério da Defesa e nas Forças Singulares, fornecendo subsídios fundamentais aos processos decisórios de altos líderes militares, permitindo uma resposta coordenada às necessidades de defesa nacional (Brasil, 2023).

Outro conceito central é o dos Objetivos de Inteligência de Defesa (OID), que consistem em metas estratégicas delineadas pela PID para guiar a atuação da AID, incluindo a antecipação e identificação de ameaças e oportunidades que possam impactar a segurança nacional. A PID também destaca a importância da identificação de ameaças observadas, como terrorismo, espionagem e crimes cibernéticos, enfatizando a necessidade de monitoramento constante de atividades que possam comprometer a integridade do país (Brasil, 2023).

Por fim, a portaria estabelece diretrizes estabelecidas que orientam a AID, abrangendo o aprimoramento contínuo das técnicas e doutrinas de inteligência, o desenvolvimento de capacidades tecnológicas e a capacitação de recursos humanos especializados. Essas diretrizes visam não apenas responder aos desafios contemporâneos da defesa, mas também preparar o Brasil para ameaças futuras, consolidando um instrumento de defesa adaptável e proativo (Brasil, 2023).

A integração desses conceitos no sistema de inteligência nacional reforça a importância da PID para a administração pública, especialmente no que tange à segurança nacional e à defesa estratégica, fortalecendo o arcabouço de proteção da soberania brasileira.

Essa portaria destaca a necessidade da organização e da estrutura da atividade no Brasil, estabelecendo diretrizes fundamentais para promover a eficiência e a segurança nas operações da mesma. Um

dos pontos centrais é a ênfase na integração e coordenação entre diferentes agências e entidades de segurança, buscando a uniformização de métodos e a padronização de procedimentos.

A portaria também reforça a importância de um sistema ágil, eficaz e capacitado para responder rapidamente às ameaças contemporâneas, especialmente no contexto das Cidades 4.0 e da crescente interconectividade digital. Conforme a Doutrina da Atividade de Inteligência Nacional, é necessário que as instituições de inteligência mantenham um comportamento ético rigoroso, garantindo que suas ações sejam transparentes e responsáveis. A ética é apontada como um componente essencial da atividade, sendo crucial para o controle e a supervisão eficazes.

A estrutura do SISBIN foi reorganizada de forma significativa por meio do Decreto nº 11.693/2023, que também é mencionado como referência para a portaria. Este decreto estabeleceu novas categorias de órgãos integrantes, incluindo entidades federadas, que agora podem ser formalmente integradas ao sistema, promovendo maior segurança jurídica e operacional. A ABIN, como órgão central, é designada para facilitar a cooperação interinstitucional e oferecer suporte às operações de inteligência em todo o território nacional.

Esse arcabouço normativo reforça a importância da criação de subsistemas especializados, como os voltados para inteligência fiscal e financeira, e da adoção de tecnologias de comunicação segura. O fortalecimento dessas medidas é fundamental para garantir que a atividade de inteligência se mantenha atualizada e eficaz na proteção dos interesses nacionais. A Portaria GM-MD nº 4.846, assim, torna-se um marco na atualização e modernização das políticas de inteligência de defesa, alinhando-as com as melhores práticas internacionais e com as exigências de segurança do século XXI.

A Política Nacional de Inteligência (PNI), estabelecida pelo Decreto nº 8.793/2016, e a Estratégia Nacional de Inteligência (ENINT) são pilares fundamentais para a aplicação da inteligência no Brasil. Esses documentos definem os principais objetivos estratégicos e estabelecem um arcabouço institucional que facilita a integração de diversas agências de segurança. Segundo Santos (2020), a integração promovida pela PNI é essencial para combater o crime organizado e proteger a sociedade contra ameaças modernas, como o terrorismo e os ataques cibernéticos.

Ao lado da inteligência e igualmente importante, a contrainteligência é definida como um conjunto de medidas voltadas à proteção de informações sensíveis contra espionagem e sabotagem, desempenhando um papel crucial na preservação da segurança dos sistemas de informação e das redes utilizadas pelas forças de segurança pública (Marrin, 2012). Contudo, a falta de profissionais capacitados para operar essas novas tecnologias é um desafio a ser enfrentado para maximizar o potencial da inteligência corrente.

A Doutrina da Atividade de Inteligência de 2023 enfatiza a necessidade de medidas preventivas e ativas de contrainteligência, incluindo a criação de redes seguras e a proteção de sistemas de dados sensíveis (Hank Prunckun, 2015). Portanto, a contrainteligência é uma área fundamental dentro da atividade de inteligência, voltada para a proteção de informações sensíveis e a neutralização de ameaças que podem comprometer a segurança de um Estado. No contexto da administração pública, ela desempenha um papel relevante, pois garante que informações críticas sejam protegidas contra a espionagem, a sabotagem e outras formas de subversão. Será examinado os conceitos principais de contrainteligência, suas aplicações práticas e a relevância para a segurança pública.

A contrainteligência também é definida como o conjunto de medidas destinadas a proteger um sistema contra ações de inteligência adversas. De acordo com Treverton (2001), ela é essencial para garantir a segurança das informações e a integridade das operações de um Estado. Prunckun (2015) destaca que a contrainteligência envolve tanto ações defensivas, como a proteção de redes e sistemas, quanto ações ofensivas, que incluem a identificação e a neutralização de espiões e agentes adversos.

Santos (2020) define a contrainteligência como uma atividade proativa que visa não apenas a defesa, mas também a antecipação de ameaças. Essa perspectiva é vital no cenário das Cidades 4.0, onde o uso de tecnologias digitais e a interconectividade criam novas vulnerabilidades. A autora enfatiza que o ambiente contemporâneo requer uma abordagem integrada que combine medidas tradicionais de segurança com soluções tecnológicas avançadas.

Cepik (2003) discute o dilema entre agilidade e transparência na implementação de políticas de contrainteligência. O autor argumenta que, embora seja necessário agir rapidamente para proteger

informações sensíveis, isso não deve ser feito à custa da transparência e da responsabilidade. Esse equilíbrio é fundamental para assegurar que as práticas de contrainteligência sejam compatíveis com os princípios de um Estado Democrático de Direito.

A contrainteligência pode ser dividida em duas categorias principais: defensiva e ofensiva. A contrainteligência defensiva se concentra na proteção de informações, pessoas e instalações. Prunckun (2015) descreve medidas como criptografia de dados, vigilância física, controle de acesso e o uso de tecnologias de detecção de intrusões como exemplos de contrainteligência defensiva.

Por outro lado, a contrainteligência ofensiva envolve ações para identificar, monitorar e neutralizar ameaças ativas. Treverton (2001) argumenta que essas ações são essenciais para desestabilizar operações adversas e prevenir danos antes que eles ocorram. No entanto, essas medidas devem ser realizadas com rigor ético, respeitando os direitos dos indivíduos e evitando abusos de poder.

O ciclo de contrainteligência segue uma lógica semelhante ao ciclo de inteligência, com etapas de planejamento, coleta, análise e execução. No entanto, possui suas peculiaridades. Santos (2020) explica que, na fase de planejamento, as ameaças são identificadas e avaliadas. Na coleta, informações relevantes são obtidas por meio de vigilância e monitoramento. A análise dessas informações visa detectar padrões de comportamento que possam indicar atividades adversas.

Uma parte crítica desse ciclo é a execução de medidas preventivas e reativas. Cepik (2003) destaca que a execução eficaz da contrainteligência depende de uma coordenação precisa entre diferentes agências e setores da administração pública. Além disso, é crucial que essas ações sejam revisadas continuamente para garantir que sejam eficazes e ajustadas às mudanças no ambiente de segurança.

A transição para as Cidades 4.0 trouxe desafios únicos para a contrainteligência. Prunckun (2015) observa que a interconectividade digital aumenta o risco de ataques cibernéticos, espionagem industrial e manipulação de dados críticos. Para lidar com essas ameaças, é necessário adotar uma abordagem integrada que combine tecnologias avançadas com treinamento constante dos profissionais envolvidos.

Treverton (2001) argumenta que as agências de inteligência devem desenvolver parcerias com o setor privado para monitorar e proteger as infraestruturas críticas. Essa colaboração é especialmente importante no caso de ameaças cibernéticas, que podem ser difíceis de detectar e neutralizar sem o apoio de especialistas em tecnologia da informação.

Santos (2020) destaca a importância da contrainteligência argumentando que o uso eficaz da informação pode ajudar a identificar e neutralizar ameaças antes que elas causem danos significativos. No entanto, isso requer um compromisso com a educação e o treinamento contínuos dos profissionais de inteligência.

A ética desempenha um papel central na contrainteligência. Prunckun (2015) enfatiza que as atividades desse ramo devem ser conduzidas de maneira que respeitem os direitos humanos e as liberdades civis. No Brasil, a legislação que regula as atividades dessas ferramentas é detalhada na Lei 9.883/1999, que criou o SISBIN, e no Decreto 11.693/2023, que reorganizou esse sistema.

Cepik (2003) ressalta que a transparência e o controle externo são fundamentais para evitar abusos. Ele sugere que a criação de mecanismos de supervisão eficazes, como comissões parlamentares e auditorias independentes, é crucial para garantir que as operações de contrainteligência não sejam usadas indevidamente. Além disso, a participação da sociedade civil no monitoramento dessas atividades pode fortalecer a legitimidade e a eficácia do sistema.

Destarte, para fortalecer a contrainteligência na administração pública, é necessário investir em tecnologia, treinamento e cooperação interinstitucional. Treverton (2001) sugere que a modernização das infraestruturas de TI e a implementação de políticas de segurança cibernética robustas são passos essenciais. Além disso, a promoção de uma cultura de segurança dentro das organizações pode ajudar a prevenir vazamentos de informações e outros incidentes de segurança.

Prunckun (2015) acrescenta que a cooperação internacional é cada vez mais importante no campo da contrainteligência. Ele observa que as ameaças muitas vezes transcendem as fronteiras nacionais e requerem uma abordagem coordenada entre diferentes países e agências. No entanto, essa cooperação deve ser baseada na confiança mútua e no respeito às leis e normas internacionais.

Por conseguinte, essa ferramenta analítica é uma componente essencial da segurança pública e da administração estatal moderna. Sua eficácia depende de uma combinação de tecnologia avançada, práticas éticas e uma legislação robusta. À medida que as cidades se tornam mais conectadas e digitalizadas, a necessidade de estratégias de contrainteligência eficazes só aumentará. Autores como Treverton, Prunckun, Cepik e Santos oferecem perspectivas valiosas que podem ajudar a moldar essas estratégias, garantindo que a administração pública esteja preparada para enfrentar as ameaças hodiernas.

Após apresentar os fundamentos acima, é essencial destacar a importância da inteligência de segurança pública como um campo indispensável da atividade no Brasil. Voltada para a proteção da sociedade e a resposta a ameaças internas, como o crime organizado, o terrorismo doméstico e outras formas de violência urbana, essa área assume um papel crucial na defesa do interesse público. Este estudo examina como a legislação brasileira estrutura e regulamenta essas atividades, evidenciando o papel da Política Nacional de Inteligência (PNI) e da Estratégia Nacional de Inteligência (ENINT) na promoção de uma integração eficaz entre diversos órgãos de segurança.

A PNI, estabelecida pelo Decreto n.º 8.793/2016, orienta as atividades de inteligência no país, abrangendo tanto a defesa nacional quanto a segurança interna. Ela estabelece os principais objetivos estratégicos do SISBIN e promove a integração entre diversos órgãos, como a Polícia Militar, a Polícia Civil e outras entidades. Essa integração é fundamental para a eficácia das operações de segurança, especialmente no combate ao crime organizado e à proteção contra ameaças cibernéticas.

A ENINT complementa a PNI, detalhando diretrizes específicas para a segurança pública. Ela enfatiza a importância de priorizar ações em setores críticos e integra práticas de coleta e análise de dados para proteger a sociedade de ameaças contemporâneas (Brasil, 2016). Essa abordagem integrada permite uma resposta coordenada a desafios complexos, como os que surgem nas Cidades 4.0, caracterizadas por uma vasta interconectividade tecnológica.

No Brasil, a inteligência de segurança pública tem evoluído significativamente, adotando tecnologias emergentes para enfrentar os desafios modernos. O uso de sistemas de vigilância avançados, análise de *big data* e aeronaves remotamente pilotadas (RPAs),

popularmente conhecido como drones, tem sido cada vez mais comum. Essas tecnologias não apenas aprimoram a capacidade de resposta das forças de segurança, mas também permitem uma gestão mais eficiente dos recursos disponíveis.

Ratcliffe (2016) observa que a aplicação de inteligência baseada em dados é vital para antecipar ameaças e desenvolver estratégias preventivas eficazes. No entanto, a interconectividade das Cidades 4.0 também cria novas vulnerabilidades, exigindo que a administração pública esteja continuamente atualizada em termos de infraestrutura tecnológica e segurança cibernética.

Para ser eficaz, a inteligência de segurança pública deve operar também dentro de um ciclo bem definido, com etapas que vão desde a coleta até a disseminação de informações. Sherman Kent (1967) descreve esse processo como uma série de atividades interligadas que garantem a produção de inteligência de qualidade. A flexibilidade do ciclo é essencial para lidar com ameaças em constante evolução, como o terrorismo e o crime organizado, que podem se manifestar de maneiras inesperadas.

Santos (2020) destaca a importância de métodos rigorosos de análise de dados, especialmente em um ambiente urbano onde a velocidade da informação é crítica. O uso de tecnologias como IA e *big data* permite que as forças de segurança atuem de forma proativa, mas também exige que as operações sejam conduzidas com responsabilidade e sob supervisão adequada.

Dessa forma, a inteligência de segurança pública deve equilibrar a necessidade de proteger informações sensíveis com o respeito aos direitos fundamentais dos cidadãos. No Brasil, as atividades de inteligência são reguladas por uma série de legislações para garantir esse equilíbrio. Além da PNI e da ENINT, mecanismos de controle externo, supervisionados pelos Poderes Executivo e Legislativo, asseguram que esse processamento de informações estratégicas seja usada de forma ética.

A legislação brasileira para promover esse equilíbrio, busca estabelecer diretrizes claras para o uso e a proteção de dados, ao mesmo tempo em que almeja preservar a segurança nacional. Esses princípios são especialmente importantes em um ambiente cada vez mais interconectado, onde a privacidade e a segurança estão em constante tensão.

A colaboração entre diferentes órgãos de segurança é um dos pilares da inteligência de segurança pública. A ENINT estabelece diretrizes que promovem a troca de informações e a coordenação de esforços para enfrentar ameaças de forma mais eficaz. Essa colaboração é essencial para evitar redundâncias e garantir uma resposta rápida a crises.

A integração entre os subsistemas de inteligência, conforme destaca Santos (2020), não apenas melhora a eficiência das operações, mas também fortalece a capacidade do Estado de proteger a sociedade. No contexto das Cidades 4.0, onde ameaças cibernéticas podem ter um impacto devastador, essa integração se torna ainda mais relevante.

Nesse cenário, essa ferramenta analítica de segurança pública no Brasil está em constante evolução, adaptando-se às novas tecnologias e às exigências de um ambiente urbano digitalmente conectado. A legislação, como a PNI e a ENINT, fornece um arcabouço para garantir que as operações sejam eficazes e alinhadas aos princípios democráticos. No entanto, o sucesso dessas atividades depende de um equilíbrio delicado entre segurança, transparência e respeito aos direitos fundamentais.

2.1.2 POLICIAMENTO ORIENTADO PELA INTELIGÊNCIA

O Policiamento Orientado pela Inteligência (POI) ou (*Intelligence-Led Policing* - ILP), é uma metodologia de aplicação da lei que surgiu como resposta às complexidades crescentes da criminalidade contemporânea, especialmente em um mundo globalizado e altamente conectado. Essa abordagem inovadora prioriza a coleta e a análise de dados para antecipar ameaças e otimizar o uso dos recursos das forças de segurança. Ao invés de reagir aos crimes, o POI busca prevenir delitos com base em evidências, direcionando os esforços policiais de forma estratégica e eficiente. Busca-se, nesse momento, os fundamentos, as bases teóricas, os desafios e as aplicações práticas do POI no contexto da segurança pública, especialmente no Brasil.

O conceito de Policiamento Orientado pela Inteligência – POI, não é uma novidade, mas sua aplicação moderna tem sido transformadora para as forças de segurança em todo o mundo. Segundo Ratcliffe (2016), o POI representa uma mudança de

paradigma, movendo-se de um modelo de policiamento reativo para um modelo proativo, no qual a coleta e a análise de informações são cruciais. Essa abordagem ajuda a identificar padrões criminais, prever delitos e aplicar medidas de prevenção, tornando as operações mais eficazes.

Peterson (2005) descreve o POI como uma "nova arquitetura de inteligência", que envolve a integração de informações de diversas fontes e a colaboração entre diferentes agências de segurança. Para ela, o objetivo é garantir que as decisões sejam informadas e baseadas em uma compreensão precisa das ameaças e dos riscos. Essa abordagem tem sido particularmente eficaz no combate ao crime organizado, ao terrorismo e a outras formas de criminalidade complexa.

No Brasil, a relevância do POI é amplificada pelas altas taxas de violência urbana e pelo impacto do crime organizado. O país tem experimentado um aumento no uso dessa metodologia, com a introdução de tecnologias avançadas, como drones, IA e análise de *big data*, para reforçar as operações de segurança pública. Silva *et al.* (2020) apontam que o POI é fundamental para enfrentar os desafios das Cidades hodiernas, onde o volume de dados gerado é significativo e as ameaças estão em constante evolução.

Segundo Silva *et al.* (2020), o ILP nasceu no Reino Unido e se tornou um modelo padrão entre as forças policiais britânicas a partir da década de 1990, sendo adotado por várias organizações policiais ao redor do mundo após os atentados de 2001 nos Estados Unidos (Ratcliffe, 2016). O modelo enfatiza a coleta e análise de dados para orientar ações policiais, transformando uma abordagem tradicional reativa em uma estratégia proativa e preventiva.

Portanto, O POI surgiu inicialmente como uma resposta às limitações do policiamento tradicional na luta contra o crime organizado. Durante os anos 1990, as forças de segurança começaram a perceber que estratégias baseadas apenas em patrulhas e resposta a incidentes não eram suficientes para conter o aumento da criminalidade. A necessidade de uma abordagem mais estratégica levou ao desenvolvimento do POI, que foi formalizado por meio de políticas de segurança baseadas na inteligência.

Ratcliffe (2016) explica que a base teórica do POI é o ciclo de inteligência, que envolve as etapas de coleta, processamento, análise e disseminação de informações. Ele argumenta que esse ciclo é

fundamental para a produção de gestão informacional de qualidade, que pode orientar a alocação de recursos e a execução de operações de forma mais eficaz. Essa abordagem é inspirada no trabalho de Kent (1967) e Prunckun (2015), que defendem o uso de métodos rigorosos e analíticos para transformar dados brutos em conhecimento acionável.

O Policiamento Orientado pela Inteligência é estruturado em torno de três pilares principais: coleta sistemática de dados, análise baseada em evidências e implementação estratégica de ações. Silva *et al*. (2020) discutem que o sucesso do POI depende de uma infraestrutura robusta de coleta de informações. Hoje em dia, esse sistema inclui o uso de tecnologias avançadas e a colaboração entre diferentes agências de segurança.

Conforme esses três pilares, a Coleta de Dados ou Coleta de Informações é o primeiro passo no processo de POI e pode ser realizada por meio de diversas fontes, incluindo câmeras de vigilância, sensores de IoT, relatórios de campo e dados de redes sociais. O segundo pilar é a Análise de Inteligência. A análise é o coração do desse tipo de Policiamento, transformando dados em insights acionáveis. Técnicas como análise de rede social, modelagem preditiva e geoprocessamento são amplamente usadas para identificar hotspots criminais e prever incidentes. Peterson (2005) argumenta que a precisão da análise é essencial para o sucesso do POI, pois informações incorretas podem levar a falhas operacionais.

A Disseminação e Execução fecham a triangulação dos pilares do POI. As informações analisadas são disseminadas para os tomadores de decisão, que utilizam esses dados para planejar operações de segurança. A execução deve ser ágil e adaptável, com a capacidade de ajustar as operações conforme novas informações se tornem disponíveis. Silva *et al*. (2020) destacam que a flexibilidade é um componente crítico para o sucesso do POI.

É importante considerar uma avaliação contínua desse processo. O ciclo de inteligência não termina com a execução e a avaliação é uma etapa ininterrupta que garante a melhoria das estratégias implementadas. Essa avaliação envolve a análise dos resultados obtidos e a identificação de oportunidades de melhoria. Ratcliffe (2016) observa que a revisão contínua permite que o POI se adapte rapidamente às mudanças no ambiente de segurança.

O Policiamento Orientado pela Inteligência oferece uma série de benefícios que o tornam uma abordagem atraente para a segurança pública. Em primeiro lugar, ele promove uma alocação mais eficiente dos recursos, garantindo que os esforços policiais sejam direcionados para as áreas com maior necessidade. Ratcliffe (2016) argumenta que essa eficiência operacional pode reduzir significativamente os custos e aumentar a eficácia das operações.

Outro benefício importante é a capacidade de prevenir crimes antes que eles ocorram. A análise de padrões criminais e a modelagem preditiva permitem que as forças de segurança antecipem ameaças e adotem medidas preventivas. Silva *et al*. (2020) destacam que essa abordagem também promove uma maior transparência e responsabilidade, já que as decisões são baseadas em dados objetivos.

O POI também facilita a cooperação entre diferentes agências de segurança. No Brasil, a integração entre a Polícia Militar, a Polícia Civil e outros órgãos é fundamental para enfrentar o crime organizado. Silva *et al*. (2020) ressaltam que a troca de informações e a coordenação interinstitucional são essenciais para o sucesso das operações de segurança, especialmente em um ambiente urbano complexo.

Apesar de suas vantagens, o Policiamento Orientado pela Inteligência enfrenta vários desafios na prática. Um dos principais obstáculos é a resistência à mudança dentro das organizações policiais. Silva *et al*. (2020) observam que muitos ainda preferem métodos tradicionais de policiamento, e a transição para uma abordagem baseada em processamento de informações estratégicas requer uma mudança cultural significativa. O treinamento e a capacitação contínua são fundamentais para superar essa resistência.

Outro desafio é a integração de sistemas de informação. No Brasil, as agências de segurança frequentemente operam com bancos de dados desconectados, o que dificulta a troca de informações e a coordenação das operações. Silva *et al*. (2020) argumentam que a falta de interoperabilidade tecnológica é um problema sério que precisa ser resolvido para o sucesso do POI.

A legislação brasileira desempenha um papel crucial na regulamentação do Policiamento Orientado pela Inteligência. A Política Nacional de Inteligência (PNI) e a Estratégia Nacional de Inteligência (ENINT) buscam fornecer a estrutura legal necessária para a coleta e o uso de dados na segurança pública. Silva *et al*. (2020)

enfatizam que essas leis buscam promover a colaboração entre diferentes órgãos de segurança e tentam garantir que as operações de POI sejam realizadas de forma ética.

Além da PNI e da ENINT, a Lei Geral de Proteção de Dados (LGPD) estabelece regras claras para o tratamento de informações pessoais. Silva *et al*. (2020) argumentam que o respeito a essas leis é essencial para manter a confiança do público, especialmente em um ambiente onde a privacidade é uma preocupação crescente. A legislação também prevê mecanismos de controle e supervisão para garantir que as operações de POI sejam realizadas de forma transparente e responsável.

Estudos de caso em diferentes partes do mundo demonstram a eficácia do Policiamento Orientado pela Inteligência. Em Nova York, por exemplo, o uso do POI ajudou a reduzir significativamente a taxa de crimes violentos. Ratcliffe (2016) relata que a análise de dados permitiu identificar áreas críticas e direcionar o patrulhamento de forma mais eficiente. Essa abordagem também facilitou a identificação de redes criminosas e o desmantelamento de gangues.

No Brasil, cidades como São Paulo, através do CompStat Paulistano, e Rio de Janeiro têm adotado o policiamento supramencionado para combater o crime organizado. Silva *et al*. (2020) descrevem o POI no Distrito Federal através da Operação Atena como uma medida eficaz na coordenação de operações e na prevenção de crimes. Embora ainda existam desafios, como a falta de integração tecnológica e a resistência cultural, esses exemplos mostram o potencial do mesmo para transformar a segurança pública.

Consequentemente, o Policiamento Orientado pela Inteligência está intrinsecamente ligado à atividade de inteligência discutida nos tópicos anteriores. O ciclo de inteligência, que envolve a coleta, análise, disseminação e execução, é um elemento central do POI. Essa integração permite que as forças de segurança atuem de forma mais estratégica, utilizando dados para antecipar ameaças e planejar operações eficazes.

Dessa forma, entende-se que a inteligência de segurança pública é um componente do POI, especialmente em um ambiente urbano onde as ameaças são dinâmicas e imprevisíveis. A análise em tempo real de dados e a capacidade de adaptar as operações rapidamente são fatores que diferenciam o mesmo de outras

abordagens de policiamento. A legislação brasileira, por sua vez, busca garantir que essa integração seja feita de forma ética e conforme as normas de proteção de dados.

O Policiamento Orientado pela Inteligência representa uma abordagem transformadora para a segurança pública, oferecendo uma maneira mais eficaz e eficiente de enfrentar o crime. No entanto, sua implementação requer investimento em tecnologia, treinamento de pessoal e uma legislação robusta que equilibre segurança e direitos individuais. O sucesso do POI no Brasil dependerá da capacidade das agências de segurança de se adaptarem às novas tecnologias e de colaborarem de forma eficaz.

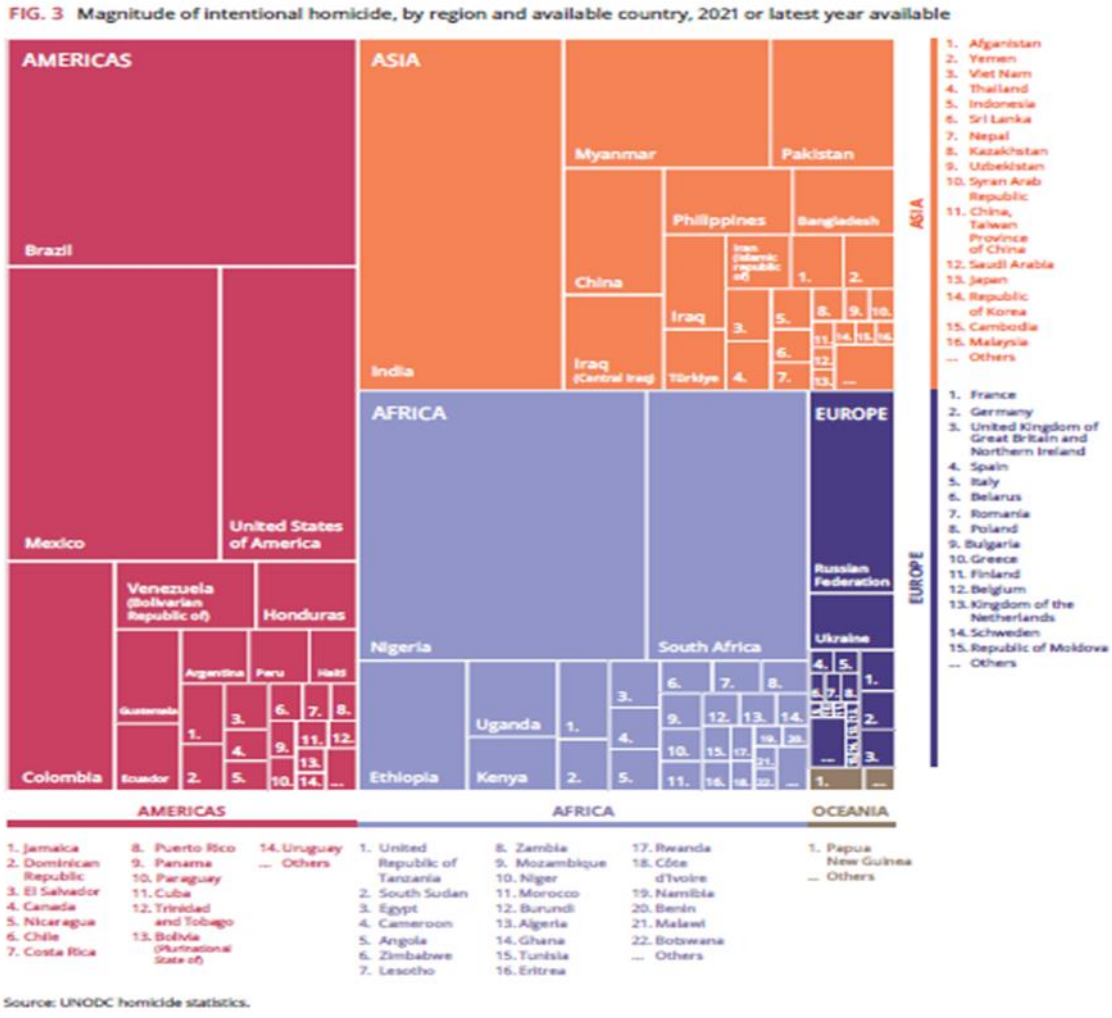
A integração do POI com as estratégias de inteligência e contrainteligência discutidas anteriormente é fundamental para enfrentar as ameaças modernas de forma holística. O futuro desse tipo de policiamento está vinculado à evolução das Cidades 4.0 e às inovações tecnológicas que continuarão a moldar a segurança pública nas próximas décadas. Por conseguinte, uma análise Policiamento Orientado pela Inteligência na Segurança Pública, apresentando definições e demonstrando o papel desse policiamento orientado pela inteligência como instrumento para assessoramento na tomada de decisões é relevante. Tal abordagem se fez necessária, pois as estruturas de inteligência das forças de segurança pública têm essa nova forma de atuação, qual seja, o espaço virtual propiciado com o advento da internet. Nesse lugar fatos e eventos ocorrem, às vezes livremente e fora do escopo de atuação primária das instituições policiais, abalando a ordem e a paz social no mundo real.

De acordo com o Anuário Brasileiro de Segurança Pública de 2023, houve 47.452 mortes violentas intencionais (MVI) no Brasil em 2022, correspondendo a uma taxa de 23,4 mortes por 100 mil habitantes. Essa taxa não supera apenas os números de 2011 quando foi registrado os índices de forma inaugural pelo Fórum Brasileiro de Segurança Pública – FBSP. O Brasil nos dias de hoje, se destaca entre os países mais violentos do mundo de acordo com o Escritório das Nações Unidas sobre Drogas e Crimes - UNODC. Esse estudo da UNODC é feito a cada quatro ou cinco anos sendo que o instituto escolheu 2021 como referência, pois é o último ano com dados mundiais completos sobre homicídio.

Esses dados alarmantes evidenciam a necessidade de políticas públicas mais eficazes, assim como de uma atuação estratégica das forças de segurança. Além de buscar enfrentar essas intempéries supramencionadas, o recrudescimento das áreas controladas por organizações criminosas e a sofisticação de suas operações demandam uma inteligência policial vigorosa, já que interferem diretamente nesses índices.

A taxa global de homicídios foi de 5,8 a cada 100 mil habitantes em 2021, para um total de 458 mil. Em 81,1% dos casos, as vítimas eram homens. Mais pessoas morreram de homicídios do que em guerras ou por atos terroristas entre 2019 e 2021. (UNODC, 2023).

Figura 3



Fonte: Escritório das Nações Unidas sobre Drogas e Crimes - UNODC.

A figura mostra a magnitude de homicídios intencionais por região e país em 2021 ou no último ano com dados disponíveis, dividida pelos continentes (Américas, Ásia, África, Europa e Oceania). O gráfico

destaca visualmente os países com as maiores taxas de homicídio, com um foco notável em países da América Latina, como Jamaica, Venezuela, Honduras e El Salvador, que apresentam algumas das taxas mais elevadas.

O Brasil e o México também aparecem com números significativos na região das Américas. Na Ásia, países como Myanmar, Paquistão e Filipinas se destacam, enquanto na África, Nigéria e África do Sul registram altas taxas de homicídio. A Europa, por sua vez, apresenta taxas mais baixas de homicídios intencionais, com Rússia e Ucrânia liderando na região, enquanto a Oceania, representada principalmente por Papua Nova Guiné, registra taxas relativamente baixas em comparação com as Américas e a África. Esta visualização ressalta a variação das taxas de homicídio intencional globalmente, destacando regiões e países onde esse problema é mais intenso.

Em virtude disso, o Governo do Distrito Federal e a Polícia Militar do Distrito Federal, possuem diversas estratégias na tentativa de controlar a violência através de políticas públicas de segurança. Algumas regiões administrativas conseguiram resultados positivos, mas redes de criminalidade organizada continuaram a se expandir (Atlas da Violência, 2023).

Apesar da redução dos índices criminais no Distrito Federal, esses ainda permanecem elevados (Fórum Brasileiro de Segurança Pública, 2023).

Tabela 1 – Número absoluto e taxa de MVI

Número absoluto e taxa de MVI
Brasil e regiões, 2021-2022

Brasil e Regiões	Número Absoluto		Taxa		Variação (%)
	2021	2022	2021	2022	
Brasil	48.228	47.452	23,9	23,4	-2,2
Centro-Oeste	3.614	3.685	22,4	22,6	0,8
Norte	6.462	6.333	37,5	36,5	-2,7
Nordeste	20.964	20.176	38,5	36,9	-4,2
Sul	5.127	5.328	17,3	17,8	3,2
Sudeste	12.121	11.930	14,3	14,1	-2,0

Fonte: Secretarias Estaduais de Segurança Pública e/ou Defesa Social; Polícia Civil de Minas Gerais; Núcleo de Apoio Técnico do Ministério Público do Acre (NAT/MPAC); Instituto de Segurança Pública do Rio de Janeiro; Instituto Brasileiro de Geografia e Estatística (IBGE); Fórum Brasileiro de Segurança Pública.

Observação: Esta versão foi modificada em 04/08/2023 a partir da retificação dos dados de Mortes Violentas Intencionais no Estado do Rio Grande do Sul e em 16/01/2024 a partir da retificação dos dados de Mortes Violentas Intencionais no Estado da Paraíba.

Fonte: Anuário Brasileiro de Segurança Pública de 2023.

Conforme o Anuário Brasileiro de Segurança Pública (2023, p. 25):

> "na escala subnacional, o estado mais violento do país em 2022 foi o Amapá, com taxa de MVI de 50,6 por 100 mil habitantes, mais do que o dobro da média nacional." A Bahia aparece em segundo lugar, com uma taxa de 47,1 por 100 mil, seguida pelo Amazonas, com 38,8 por 100 mil. No outro extremo, "as unidades da federação com as menores taxas de violência letal foram São Paulo, com 8,4 mortes por 100 mil habitantes, Santa Catarina, com 9,1 por 100 mil e o Distrito Federal, com taxa de 11,3." Em termos gerais, vinte estados registraram taxas de MVI acima da média nacional (grifos acrescidos).

Internacionalmente, diversas políticas de segurança pública bem-sucedidas foram implementadas em vários países. Desde os anos 2000, algumas iniciativas brasileiras também começaram a adotar experiências estrangeiras, introduzindo ações inovadoras como o Infocrim em São Paulo e o Pacto pela Vida em Pernambuco segundo o Atlas da Violência (2023, p. 10):

> Conforme já referido no Atlas da Violência 2020, nos anos 2000 alguns Estados e Municípios brasileiros passaram a introduzir políticas e ações inovadoras: como o Informações Criminais-Infocrim (2000), em São Paulo; o Programa Ficar Vivo (2003) e o Integração de Gestão em Segurança Pública - Igesp (2005),

> em Minas Gerais, o Pacto pela Vida (2007), em Pernambuco; as Unidades de Polícia Pacificadoras - UPPs (2008), no Rio de Janeiro; o Paraíba Unida pela Paz (2011); o Estado Presente (2011), no Espírito Santo; e, mais recentemente, a partir de 2019, o RS Seguro e o Territórios pela Paz (TerPaz), no Pará, além de ações e planos de segurança pública municipais em cidades do Sul, de São Paulo e de alguns outros estados. A respeito da gestão orientada por resultados, o Instituto Sou da Paz lançou um interessante documento detalhando essas inovações em vários estados da federação.

Nesse seguimento:

> Além do impacto desses dois fatores para diminuir a taxa de homicídios em várias Unidades da Federação ao longo da década, houve um armistício entre as duas maiores facções nacionais do narcotráfico em 2018 e 2019, após a guerra que eclodiu em meados de 2016 e seguiu até o final de 2017, conforme analisado nas edições de 2019 e 2020 do Atlas da Violência. Esse armistício, cujas consequências foram mais substantivas nas regiões Norte e Nordeste, junto com os dois fatores sublinhados anteriormente, contribuíram para a reversão da trajetória de crescimento dos homicídios agregados a partir de 2018.

Os "dois fatores" mencionados no trecho do Atlas da Violência que contribuíram para a diminuição da taxa de homicídios em várias Unidades da Federação ao longo da década são: o envelhecimento populacional e o controle de armas de fogo. Diante do envelhecimento da população, desde o começo dos anos 2000, o Brasil passou por uma transição demográfica significativa, com a diminuição da proporção de jovens na população, fator que foi identificado como contribuinte para a redução de homicídios.

Em relação ao controle de armas de fogo, a partir de 2003, com a sanção do Estatuto do Desarmamento, o país observou um controle mais rígido sobre a circulação de armas de fogo, o que foi estimado como responsável pela preservação de milhares de vidas ao longo dos anos. Esses fatores, aliados ao armistício entre facções criminosas em 2018 e 2019, ajudaram a reverter a tendência de crescimento dos homicídios em algumas regiões do país. (Atlas da Violência, 2023)

Muitas dessas iniciativas supramencionadas se basearam na estratégia CompStat, inicialmente aplicada pelo Departamento de Polícia de Nova Iorque em 1994. O CompStat é uma ferramenta computacional de georreferenciamento de ocorrências e gestão de

recursos implementada nesse Estado norte americano de Nova Iorque. O Estado de São Paulo investiu nessa estratégia a qual esse trabalho mencionará adiante.

Nesse ínterim, o Estado do Espírito Santo deu maior relevância ao Policiamento Orientado pela Inteligência em seu o programa "Estado Presente" através de métodos baseados em dados para realizar diagnósticos, planejar e monitorar ações, atuando preventivamente para evitar que jovens vulneráveis se tornem futuros criminosos, de acordo com Silva *et al* (2020),

Portanto, o Policiamento Orientado pela Inteligência (POI) é uma abordagem moderna que utiliza a inteligência para orientar o planejamento e a tomada de decisões nas atividades policiais. Segundo a Organização para a Segurança e Cooperação na Europa (OSCE), o mesmo visa identificar e planejar medidas corretivas para combater ameaças transnacionais, como o terrorismo e o crime organizado, além de ser aplicado no planejamento diário das operações policiais (OSCE, 2017).

No Brasil, a adoção do desse tipo de policiamento ainda está em estágio inicial. Poucos gestores conhecem a estratégia, que não é amplamente ensinada nos cursos de formação policial. A maioria das polícias brasileiras ainda não integra efetivamente a inteligência no planejamento e execução de suas operações (Andrade, 2018). No entanto, algumas iniciativas locais mostram avanços, como a Operação Atena no Distrito Federal e o uso do sistema Mobile pela Polícia Militar do Piauí. (Silva *et al.* 2020)

Para Silva *et al.* (2020) para o POI ser implementado com sucesso no Brasil, é necessário um maior investimento em tecnologia e capacitação, além de uma mudança cultural nas instituições policiais para promover a integração e o compartilhamento de informações. A Estratégia Federal de Desenvolvimento para o Brasil 2020-2031 destaca a importância da inteligência para enfrentar a criminalidade violenta, mas são necessárias ações concretas para transformar essa visão em realidade (Brasil, 2020).

A implementação eficaz do ILP pode transformar a abordagem policial no Brasil, tornando-a mais eficiente e proativa, e contribuindo significativamente para a redução da criminalidade e a melhoria da segurança pública. (Silva, *et al.,* 2020)

2.1.2.1 O COMPSTAT PAULISTANO

A análise do impacto do programa CompStat, implantado pela Prefeitura de São Paulo, destaca a evolução do uso de tecnologias de informação geográfica e estatística no combate à criminalidade urbana.

A Portaria nº 1, de 4 de janeiro de 2019, da Secretaria Municipal de Segurança Urbana (SMSU) do Estado de São Paulo, institui o Sistema Inteligente de Suporte à Tomada de Decisão em Segurança Urbana, conhecido como CompStat Paulistano. Esta norma estabelece um programa voltado para a melhoria contínua na prevenção da criminalidade e da violência por meio da coleta e análise sistemática de dados sobre a segurança urbana.

O CompStat Paulistano integra a gestão de segurança municipal com procedimentos detalhados para diagnóstico, planejamento, execução, monitoramento e avaliação das ações, bem como para a utilização de indicadores de segurança urbana. A portaria detalha a estrutura de governança e os ciclos de reuniões para o acompanhamento e controle das ações, além de prever a utilização de dados provenientes de diversas fontes para a tomada de decisões estratégicas na área de segurança (Portaria SMSU nº 1, 2019).

Em consonância com a legislação acima este estudo examina três matérias jornalísticas que abordam diferentes momentos e aspectos da implementação e operacionalização do CompStat Paulistano, revelando como o programa tem influenciado a segurança pública na cidade.

A primeira matéria datada, 27/02/2019 da Prefeitura de São Paulo, destaca o histórico do CompStat e introdução do CompStat em São Paulo, inspirado no sistema original de Nova York. O programa utiliza dados estatísticos e informações geográficas para antecipar a ocorrência de crimes, auxiliando a Guarda Civil Metropolitana (GCM) no planejamento estratégico de patrulhamento preventivo. O Secretário Municipal de Segurança Urbana na época, José Roberto Rodrigues de Oliveira, explica que o foco inicial estaria em crimes de oportunidade, como furtos e roubos, que afetam diretamente a sensação de segurança dos cidadãos. (Prefeitura de São Paulo, 2019)

Em uma nova data é feita uma nova matéria com o seguinte título: a Gestão Covas implanta programa contra crime adotado em

Nova York (22/02/2019). Essa segunda matéria detalha a implementação do CompStat Paulistano pela gestão Bruno Covas. A reportagem destaca como o sistema, utilizado desde 1994 em Nova York, tem sido adaptado para São Paulo. A versão paulistana do CompStat compila dados de delegacias e sistemas de monitoramento para desenhar um mapa detalhado da criminalidade, orientando ações de segurança pública de maneira mais eficiente. O sistema foi testado em uma operação específica no Largo da Concórdia, resultando em uma redução de mais de 70% nos furtos na região. (Folha de São Paulo, 2019)

No ano de 2023, quatro anos após a inauguração do Sistema, podemos mencionar a evolução e impactos do CompStat Paulistano com a matéria: CompStat Paulistano - sistema integrado para identificação de áreas sensíveis à desordem urbana (14/09/2023). Essa terceira matéria analisa a evolução do CompStat Paulistano desde sua implementação. O sistema integrado permite o monitoramento contínuo do território municipal através do cruzamento de dados de diferentes fontes. As informações geolocalizadas são utilizadas para produzir diagnósticos constantes e orientar ações operacionais da GCM. A matéria destaca exemplos práticos, como o Programa Guardiã Maria da Penha, que utiliza dados do sistema para planejar visitas e rondas, garantindo a segurança de vítimas de violência doméstica. (Prefeitura de São Paulo, 2023)

Uma análise crítica da implantação do CompStat em São Paulo pode indicar um avanço significativo na utilização de tecnologias de inteligência policial, tanto para o combate à criminalidade quanto para a formulação de políticas públicas. A análise das matérias revela um progresso na eficácia das operações de segurança pública, desde a fase de testes até a implementação plena do sistema.

O Planejamento Estratégico e Prevenção do CompStat permite uma abordagem preventiva ao crime, ao identificar padrões e antecipar a ocorrência de delitos. Isso é fundamental para reduzir crimes de oportunidade e aumentar a sensação de segurança da população.

Essa integração de Dados e colaboração interinstitucional pela utilização de múltiplas fontes de dados, como o SP+Segura e o Sistema INFOCRIM, destaca a importância da integração e colaboração entre diferentes órgãos de segurança. No entanto, críticas apontam para a falta de articulação entre a segurança municipal e estadual, sugerindo

a necessidade de maior cooperação para otimizar recursos e reduzir gastos públicos.

Trazendo o assunto para uma avaliação de resultados, a implementação do CompStat em São Paulo demonstrou resultados positivos, como a significativa redução de furtos durante a operação no Largo da Concórdia. No entanto, a eficácia do programa a longo prazo depende de avaliações contínuas e ajustes baseados em dados empíricos. (Folha de São Paulo, 2019)

Os próximos desafios e críticas a esse como a qualquer outro sistema está na pressão excessiva sobre os funcionários para mostrar resultados e a potencial manipulação de estatísticas. Além disso, estudos sugerem que outros fatores, como o aumento do efetivo policial e mudanças econômicas, podem ter contribuído para a redução da criminalidade em Nova York, relativizando o impacto exclusivo do CompStat.

Sobre o CompStat Paulistano é possível concluir que esse Sistema representa uma evolução importante na gestão da segurança pública em São Paulo, ao combinar tecnologia e inteligência policial para prevenir e combater a criminalidade. A análise das matérias jornalísticas revela um progresso contínuo na implementação do programa, embora desafios e críticas devam ser considerados para garantir sua eficácia a longo prazo. A integração de dados e a colaboração interinstitucional são fundamentais para o sucesso do CompStat, tornando-o uma ferramenta poderosa para melhorar a segurança urbana e a qualidade de vida dos cidadãos.

2.1.3 INTELIGÊNCIA CORRENTE

O desenvolvimento urbano impulsionado por novas tecnologias provocou mudanças profundas na sociedade, transformando a estrutura das cidades e a maneira como questões de segurança pública são gerenciadas. As Cidades 4.0, caracterizadas por redes digitais interconectadas e o uso de IA, demandam estratégias de vigilância e proteção que sejam ágeis e dinâmicas. Nesse contexto, a Inteligência Corrente se destaca como uma ferramenta estratégica crucial, definida pela Doutrina da Atividade de Inteligência 2023 como a prática contínua de coleta, análise e disseminação de informações em tempo real, essencial para apoiar decisões rápidas e precisas em operações policiais.

Essa modalidade de ferramenta de informações estratégicas fornece uma base sólida que permite às forças de segurança antecipar ameaças e ajustar suas ações conforme necessário. Em ambientes urbanos densamente povoados, onde a rapidez na resposta pode determinar o sucesso das operações, a Inteligência Corrente torna-se particularmente valiosa. Essa abordagem aprimora a coordenação entre unidades operacionais, otimizando o uso de recursos e garantindo maior segurança para agentes e cidadãos.

A capacidade de monitorar situações em tempo real é um dos pilares da Inteligência Corrente. O uso de sensores, câmeras conectadas e sistemas de análise preditiva oferece às autoridades uma visão abrangente e imediata das áreas urbanas, possibilitando a identificação de atividades suspeitas antes que se tornem ameaças reais. Treverton (2001) afirma que essa vigilância contínua é essencial para prevenir crimes em ambientes urbanos complexos, onde as circunstâncias podem mudar rapidamente.

O processamento de grandes volumes de dados em tempo real, facilitado por técnicas de *big data* e algoritmos de IA, é outro elemento crítico. Hulnick (2006) destaca que o uso de tecnologias avançadas permite a detecção precoce de ameaças e a identificação de padrões comportamentais que passariam despercebidos sem o suporte da tecnologia. Essa vantagem temporal proporciona uma resposta mais ágil e eficaz, aumentando a capacidade operacional das forças de segurança.

A aplicação da Inteligência Corrente em ambientes urbanos altamente conectados é amplamente reconhecida como um avanço significativo na gestão da segurança pública. A integração contínua de informações facilita a cooperação entre diferentes unidades e agências de segurança, o que é vital em operações de grande escala ou em situações emergenciais. Essa colaboração aumenta a eficiência operacional e fortalece a capacidade de resposta, conforme ressaltado por Marrin (2012), que discute como a análise integrada pode otimizar a alocação de recursos em áreas de risco elevado.

No combate ao crime organizado, como o tráfico de drogas e o terrorismo, a Inteligência Corrente é uma ferramenta imprescindível. A utilização de RPAs (drones) e câmeras inteligentes permite uma vigilância mais abrangente e eficaz. Marrin (2012) observa que a coleta de dados em tempo real, aliada a algoritmos de IA, não apenas melhora

a precisão das operações, mas também otimiza a gestão dos recursos, permitindo respostas mais rápidas e estratégias mais eficazes.

Apesar das vantagens, a implementação da Inteligência Corrente enfrenta desafios significativos. Um dos principais é a segurança cibernética, pois a conectividade das Cidades 4.0 expõe os sistemas de segurança a ataques digitais. A Doutrina da Atividade de Inteligência 2023 enfatiza a necessidade de desenvolver medidas robustas para proteger essas redes, uma vez que a segurança digital é tão vital quanto a segurança física.

Outro desafio relevante envolve as questões éticas e de privacidade. O uso extensivo de tecnologias de vigilância pode gerar tensões quanto à proteção dos direitos dos cidadãos. O equilíbrio entre segurança e privacidade é um tema crítico, exigindo transparência e regulamentações claras para garantir que a coleta de dados seja feita de forma responsável. Em ações policiais, a supervisão independente e o respeito às normas legais são essenciais para manter a confiança pública nas operações de inteligência.

A Inteligência Corrente se integra a um modelo mais amplo de policiamento orientado por inteligência, que busca combinar dados em tempo real com análises históricas para otimizar a gestão das operações. Essa integração não apenas permite respostas mais rápidas, mas também facilita uma abordagem preditiva, onde as forças de segurança podem agir preventivamente com base em padrões identificados. Santos (2020) destaca que essa abordagem integrada é fundamental para a eficácia das operações, sobretudo em cenários urbanos complexos.

A Inteligência Corrente representa um avanço sistemático na gestão da segurança pública em Cidades 4.0. Sua implementação eficaz depende de um equilíbrio entre a eficiência operacional e a proteção dos direitos civis. Com investimento contínuo em tecnologia, treinamento especializado e regulamentações apropriadas, essa ferramenta pode transformar a maneira como as cidades são protegidas, tornando-as mais seguras e resilientes. Assim, as estratégias baseadas em inteligência garantem que as autoridades estejam sempre um passo à frente, preparadas para enfrentar os desafios de um mundo cada vez mais interconectado.

Dessa forma, o uso da inteligência, contrainteligência e inteligência corrente nas Cidades 4.0 através do policiamento

orientado pela inteligência é fundamental para garantir a segurança pública em um ambiente cada vez mais digital e interconectado. A aplicação dessas estratégias permite que as forças de segurança antecipem ameaças, protejam informações estratégicas e respondam rapidamente a incidentes. No entanto, os desafios são consideráveis, especialmente no que diz respeito à proteção contra-ataques cibernéticos e à necessidade de análise rápida de grandes volumes de dados. Para enfrentar esses desafios, é necessário um investimento contínuo em tecnologia e capacitação profissional.

Na sequência, se trará uma abordagem do crime, com conceituação e impactos na segurança pública. Por último, sob o enfoque de uma premissa menor, são abordados os principais desafios enfrentados pela Inteligência de Segurança Pública no contexto das Cidades 4.0, integrando as ideias extraídas das análises anteriores.

2.2 SEGURANÇA PÚBLICA

2.2.1 A ATIVIDADE DE SEGURANÇA PÚBLICA

Para contextualizar a Atividade de Segurança Pública deve-se realizar uma breve descrição do modelo de segurança pública no Brasil, previsto na Constituição de 1988, no Título da Defesa do Estado e das Instituições Democráticas. Para incrementar essa tarefa, a inteligência de segurança pública surge como instrumento de relevância no combate ao crime.

A segurança pública no Brasil se perfaz sob uma estrutura bipartida das funções de prevenção e repressão (Constituição Federal de 1988, art. 144). Nesse cenário, tem-se como referência de atuação aquele em que um evento da natureza (catástrofes, calamidade etc.) ou um comportamento humano (violência, crimes etc.) são causadores de prejuízo ou perigo. Naturalmente, as ações de segurança se destinam a evitar a ocorrência de tais eventos lesivos (naturais e humanos). Por sua vez, quando ocorrem, a resposta deve ser imediata e eficaz, a fim de resgatar a ordem e reparar os danos. (Carneiro; Moreira, 2023)

Nesse ponto, se fixa a distribuição de atribuições aos órgãos de segurança pública quanto à prevenção e repressão. Com efeito, de forma típica, o corpo de bombeiros militar cuida dos eventos da natureza. As polícias se dedicam precipuamente ao comportamento humano. Nesse cenário, os procedimentos desses órgãos visam

preservar a ordem, bem como afastar pessoas e seus bens dos perigos, danos, prejuízos e/ou ameaças, com ações de prevenção ou de resposta imediata e mediata (Lazzarini *et al*., 1987).

Conforme estabelecido na Constituição da República Federativa do Brasil de 1988 (CRFB/88), nos §§ 2º, 3º e 5º do art. 144, os órgãos policiais têm a responsabilidade de realizar a prevenção de crimes de forma fundamental. Esse emprego policial é conduzido principalmente pela Polícia Rodoviária Federal, Polícia Ferroviária Federal e pelas Polícias Militares, mediante o policiamento ostensivo, que tem o propósito de evitar a ocorrência de eventos prejudiciais ou de responder a eles de maneira rápida, incluindo a detenção de indivíduos envolvidos em atividades criminosas.

Entretanto, é importante observar que não é adotado o modelo de ciclo completo de polícia no Brasil, que engloba tanto a prevenção quanto a repressão completa (imediata e mediata), incluindo a investigação de crimes, com exceção da Polícia Federal. A Polícia Federal assume essa função em casos relacionados ao combate ao tráfico de drogas, contrabando e descaminho, além das responsabilidades de polícia marítima, portuária e de fronteiras, conforme estabelecido no parágrafo 1º, incisos II e III do mesmo artigo mencionado anteriormente. (Carneiro; Moreira, 2023)

As polícias Civis e Federal têm como principal foco a realização da repressão imediata e mediata, desempenhando atividades voltadas para a investigação da autoria e evidências de crimes, além de desempenhar funções de polícia judiciária, com o objetivo de apoiar o processo criminal no sistema judiciário. Por outro lado, a recém-criada Polícia Penal é responsável pela segurança nos estabelecimentos penais. Para facilitar as operações dos órgãos policiais, seja na prevenção ou na repressão, são conduzidas atividades de inteligência, entre outras ações. (Carneiro; Moreira, 2023)

2.2.2 INTELIGÊNCIA DE SEGURANÇA PÚBLICA (ISP)

A aplicação da lei e a segurança pública são questões de importância primordial em qualquer sociedade. A capacidade das forças de segurança pública, como a Polícia Militar, de responder eficazmente a incidentes, prevenir crimes e proteger os cidadãos desempenha um papel fundamental na construção de comunidades seguras e no fortalecimento da confiança na aplicação da lei. No

entanto, em um mundo cada vez mais digital e interconectado, surgem desafios significativos que afetam diretamente a eficácia das operações policiais.

Majoritariamente, a atividade de inteligência é utilizada como uma ferramenta para garantir que os objetivos do Estado sejam alcançados. Ela fornece informações que auxiliam na formulação de estratégias de ação no momento da tomada de decisões, incluindo a implementação de políticas públicas, bem como no fortalecimento da influência política, militar, econômica e tecnológica. (Cepik, 2003).

De acordo com Portaria GM-MD nº 4.846, de 29 de setembro de 2023: "A Inteligência, em qualquer nível de atuação, possui como meta precípua a perfeita captura da realidade e a constante identificação das ameaças, minimizando incertezas e buscando oportunidades para o sucesso das operações. "

Nesse diapasão, a Lei nº 9.883/1999 estabelece o Sistema Brasileiro de Inteligência (SISBIN) no artigo 2º, delineando os órgãos que podem participar do Sistema de Inteligência e definindo suas responsabilidades. De acordo com o texto legal:

> Art. 2º **Os órgãos e entidades da Administração Pública Federal que, direta ou indiretamente,** possam **produzir conhecimentos de interesse das atividades de inteligência**, em especial aqueles responsáveis pela defesa externa, segurança interna e relações exteriores, **constituirão o Sistema Brasileiro de Inteligência**, na forma de ato do Presidente da República.
>
> § 1º **O Sistema Brasileiro de Inteligência é responsável pelo processo de obtenção, análise e disseminação da informação necessária ao processo decisório do Poder Executivo,** bem como **pela salvaguarda da informação contra o acesso de pessoas ou órgãos não autorizados.**
>
> § 2º Mediante ajustes específicos e convênios, ouvido o competente órgão de controle externo da atividade de inteligência, **as Unidades da Federação poderão compor o Sistema Brasileiro de Inteligência**. (Grifos acrescidos)

Dentro deste contexto, devido à importância das atividades realizadas pelos órgãos de segurança pública e sua relação com as operações internas, os órgãos de segurança pública fazem parte do SISBIN, sendo parte integrante do Subsistema de Inteligência de

Segurança Pública (SISP), conforme Decreto Federal nº 3.695/2000, art. 1º.

Nesse sentido, cabe aos órgãos que compõem o SISP utilizar a inteligência para tomar medidas preventivas e repressivas, apoiando ações para garantir a ordem pública e a proteção de pessoas e propriedades (Santos, 2020). A inteligência é um instrumento fundamental para controlar a violência, manter a ordem e combater a criminalidade.

A Inteligência de Segurança Pública (ISP) tem como objetivo desenvolver procedimentos para identificar, acompanhar e avaliar ameaças à segurança pública, fornecendo informações que ajudam a neutralizar e reprimir atos criminosos, especialmente quando estes são praticados de forma dissimulada. Isso se torna essencial, uma vez que a dissimulação criminosa visa dificultar a identificação dos autores e detalhes dos crimes. Essa ferramenta analítica também é usada para identificar padrões criminais e eventos de interesse público, orientando o emprego eficaz das forças de segurança. Além disso, as operações de inteligência podem apoiar ações policiais por meio de métodos técnicos de coleta de informações, desde que estejam em conformidade com a legislação. Essas ações são aplicadas tanto na prevenção quanto na repressão de crimes. (Cepik, 2003).

Portanto, a inteligência desempenha um papel crucial nas Cidades 4.0 e na eficácia das operações de segurança pública. Em um mundo cada vez mais complexo e interconectado, onde as ameaças à segurança podem surgir de formas dissimuladas e inesperadas, a capacidade de obter, analisar e disseminar informações relevantes é fundamental.

A integração dos órgãos de segurança pública no SISBIN e a criação do SISP refletem a importância de utilizar a inteligência como uma ferramenta estratégica para combater a criminalidade, manter a ordem pública e proteger os cidadãos. Através dessa gestão informacional, as forças de segurança podem identificar ameaças, prevenir crimes e responder de maneira eficaz a incidentes, contribuindo assim para a construção de comunidades mais seguras e para o fortalecimento da confiança na aplicação da lei nas cidades inteligentes do futuro.

O policiamento ostensivo (Constituição Federal, 1988) tem como principal objetivo evitar distúrbios à paz social, e para isso, os agentes

de polícia são identificáveis visualmente, usando uniformes e insígnias. Eles realizam patrulhamento preventivo, tomando medidas como averiguação, advertência e, se necessário, repressão imediata, como busca pessoal e prisão em flagrante. (Art. 301 do Decreto-Lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal Brasileiro – CPP)

No entanto, alguns criminosos adotam métodos furtivos para se esquivar do policiamento ostensivo, dificultando sua atuação. Nesse contexto, a inteligência desempenha um papel fundamental, usando a vigilância, observação e entrevistas para obter informações que possibilitam ao policiamento ostensivo uma atuação mais eficaz. Isso se enquadra no serviço velado, descrito na Doutrina Nacional de Inteligência de Segurança Pública (DNISP, 2016).

A legislação, especialmente o CPP, fornece diretrizes para a atuação policial nesse contexto, incluindo os procedimentos de busca e prisão em flagrante, conforme, o arts. 240, 242, 244 a 250, 301 e 302 do diploma legal supramencionado e da DNISP, 2016.

Nessa conjuntura das Cidades 4.0, a importância da inteligência se torna ainda mais evidente, pois as novas tecnologias se tornam instrumentos essenciais para o serviço velado das forças de segurança. A capacidade de coletar e analisar dados em tempo real, usar câmeras de vigilância, reconhecimento facial, análise de padrões criminais e outras ferramentas avançadas oferece aos órgãos de segurança a vantagem de identificar ameaças dissimuladas de forma mais eficaz.

Essas tecnologias podem ser aplicadas para rastrear suspeitos, prevenir crimes e fornecer informações críticas para as operações de policiamento ostensivo. Assim, a combinação da inteligência tradicional com as inovações tecnológicas permite uma atuação mais eficaz das forças de segurança, garantindo a paz social e a segurança pública nas cidades inteligentes do futuro.

Um exemplo de cooperação internacional em inovação tecnológica encontra-se nas relações entre o Brasil e o Reino Unido, onde a IA e o *machine learning* desempenham um papel crucial: no final de 2020, o Reino Unido e o Brasil reforçaram laços econômicos através de acordos abrangendo questões tributárias, serviços financeiros e finanças verdes. Os esforços visam facilitar o acesso ao mercado, impulsionar o crescimento sustentável e fortalecer a cooperação em projetos ambientalmente conscientes. Essa parceria ressalta a importância das alianças internacionais em tecnologia para

aprimorar as economias e promover colaborações em iniciativas de inovação e pesquisa conjunta. (Brasil, 2023)

Nas Cidades 4.0, a importância da inteligência se torna ainda mais evidente, estendendo-se à cooperação internacional e às relações do Brasil e outros países. As novas tecnologias se tornam instrumentos essenciais para o serviço velado das forças de segurança, e a colaboração com parceiros mundiais em áreas como segurança cibernética e compartilhamento de informações desempenha um papel vital na proteção contra ameaças globais.

A capacidade de coletar e analisar dados em tempo real, juntamente com a adoção de melhores práticas em matéria de inteligência e segurança pública, permite aos órgãos brasileiros se beneficiarem de uma troca de conhecimento valiosa. Isso fortalece a capacidade do Brasil de identificar ameaças dissimuladas de forma mais eficaz e contribui para um ambiente mais seguro.

Portanto, a combinação da inteligência com as inovações tecnológicas, aliada à colaboração internacional, permite uma atuação mais eficaz das forças de segurança, garantindo a paz social e a segurança pública nas cidades inteligentes do futuro, fortalecendo, assim, as relações entre o Brasil e a países parceiros em prol da segurança global.

Quanto aos procedimentos de investigação policial, diante da notícia uma infração penal, a persecução criminal é normalmente instaurada com a investigação policial, conduzida essencialmente para colher os elementos e informação sobre a autoria e a materialidade de um delito (Ferreira; Ferreira, 2011), devendo encontrar respostas aos questionamentos sobre ator e vítima, natureza do fato, local, outros autores, meios e modos, tempo, motivos, dentre outros aspectos.

Para responder a tais perguntas, a apuração deve ser conduzida com emprego de procedimentos e ferramentas elencadas na legislação e nos protocolos técnicos de investigação. Os primeiros procedimentos, conhecidos como diligências, estão elencados inicialmente no art. 6º do Código de Processo Penal, Decreto-Lei nº 3.689/1941 (Ferreira; Ferreira, 2011), sendo eles: apreender os objetos que tiverem relação com o fato; ouvir o ofendido, colher todas as provas que servirem para o esclarecimento do fato; ouvir o ofendido, testemunhas e indiciado; proceder a reconhecimento de pessoas e coisas; determinar que proceda a exame de corpo de delito e outras perícias;

ordenar a identificação do indiciado, fazer juntar folha de antecedentes do indiciado, averiguar vida pregressa do indiciado, etc.

Ressalte-se que o produto desse trabalho é levado ao Ministério Público (CPP art. 12), titular da ação penal pública (Constituição Federal, 1988, art. 129, Inciso I; CPP art. 24), sendo esta função exercida mediante apresentação de denúncia perante a justiça criminal, desde que demonstrada a justa causa, caracterizada pela existência de elementos mínimos de autoria e materialidade de uma infração penal (Mougenot, 2019).

A depender da complexidade da conduta, do número de agentes envolvidos, dos meios empregados, da gravidade e quantidade dos delitos, é necessário promover ações de investigação policial de caráter mais invasivo, tais como: prisão temporária, prisão preventiva, busca e apreensão, interceptação ambiental, interceptação telefônica e telemática, infiltração de agente ação controlada, quebra dos sigilos etc. (Ferreira; Ferreira, 2011). Tais medidas recaem sobre direitos de dimensão constitucional, com menção sobre o princípio constitucional da reserva de jurisdição. Nesse sentido, exige-se a provocação prévia do Poder Judiciário. O magistrado, como autoridade de salvaguarda de direitos individuais, examina a legalidade, necessidade, adequação e a proporcionalidade da medida indicada na investigação criminal.

Para tanto, a ordem jurídica fixa pressupostos e requisitos para justificar a quebra episódica de determinados direitos constitucionais em atos de investigação policial. Como pressuposto para isso, tem-se a gravidade do delito, natureza dolosa do crime, punido com reclusão e existência de indício suficiente de autoria e materialidade da infração penal. Como requisitos, impõe-se evidenciar a inexistência de outra forma de se obter a prova do fato, a liberdade do indiciado gera prejuízos à sociedade e traz riscos ao esclarecimento dos fatos, dentre outros elementos. (Carneiro; Moreira, 2023)

Importante nesse contexto de segurança pública destacar a ascensão do crime organizado e, dessa forma, se faz necessária uma análise preliminar sobre a ideia por trás dos conceitos de sociedade e Estado. Sob o viés contratualista, vem a noção de que "os homens se reúnem e estabelecem entre si um pacto que funciona como instrumento de passagem do momento ‘negativo’ de natureza para o estágio político (social), pelo que se tem o fundamento de legitimação do Estado de sociedade" (Streck; Morais, 2014).

O Estado se caracteriza pela reunião de forças de coalisão de diversos grupos organizados, para firmar uma dominação natureza política, social e econômica, criando uma autoridade suprema com imposição de uma vontade coletiva (poder), não se submetendo a outra ordem (soberania), em uma porção de espaço geográfico (território), estabelecendo vínculo e exercendo autoridade sobre um grupo de pessoas população), para atingir o bem comum, mediante ações de governo (Streck; Morais, 2014).

Dentro desse ambiente, surgem ordens paralelas, contrárias às menções sociais e à margem da lei para fazer frente aos interesses e intenções a sociedade, da coletividade e do Estado, subtraindo-lhes sistematicamente, de forma ilícita e criminosa, a riqueza e a paz social. Nessa perspectiva, os órgãos de segurança enfrentam desafios intensos e complexos, buscando controlar e eliminar as ações dessas ordens, merecendo, nesse momento, um breve estudo sobre a origem, evolução e estrutura das organizações criminosas e os atos de prevenção e resposta do Estado. (Carneiro; Moreira, 2023)

Há, portanto, dois fatores a serem considerados sobre a origem das organizações de natureza paralela às ordens convencionais. Elas foram e são criadas como forma de proteger os indivíduos hipossuficientes diante das injustiças, desigualdades sociais e abusos praticados pelos entes dominantes (instituições e órgãos do Estado). Em outras oportunidades, uma horda de pessoas se uniu e se une para fortalecer as relações entre si, explorando atividades ilegais, auferido ganhos financeiros, políticos, sociais e patrimoniais, em um cenário local, regional ou transnacional. Nesse ponto, citam-se grupos mafiosos, cartéis, falanges, gangues e os grupos à margem da lei. (Carneiro; Moreira, 2023)

Como referência mais consistente da gênese do crime organizado no Brasil, na década de 1980, surge o Comando Vermelho (CV), no Presídio de Ilha Grande, Rio de Janeiro, visando o tráfico de drogas nos morros daquela cidade. Em São Paulo, foi criado, no ano de 1993, o Primeiro Comando Capital (PCC), com estatuto próprio. Além destes, existem o Terceiro Comando (TC), Amigos dos Amigos (ADA) e etc. (Pacheco, 2011).

Segundo Costa (2017) para exploração do crime de forma sistematizada, como fonte e recurso financeiro, dominação de espaço,

controle de pessoas e conquista do poder, exige-se a criação de uma estrutura, captação de recursos e definição de regras.

Dessa forma, parte-se da premissa básica de que uma organização possui uma estrutura com um líder, ou um pequeno grupo que gerencia suas ações, fixando a distribuição de funções e atividades no tempo e no espaço, assumindo uma forma hierarquizada, centralizada ou descentralizada, buscando ainda recrutar pessoas e aliciar agentes do Estado (Costa, 2017).

Algumas organizações criminosas assumem natureza de empresa buscando o lucro e o poder econômico. Para tanto, constituem grupo dirigente, definem critérios de recrutamento e seleção, um código de ética e estatuto com normas para disciplinar a estrutura. Também fixam responsabilidades e áreas de ação (local, regional, transnacional e cibernética), empregando violência e intimidação, estabelecem sanções por desvio de conduta, com pena de morte. Exercem, ainda, grande poder de corrupção sobre os agentes do Estado, podendo também desenvolver ações sociais como se órgãos estatais fossem, bem como utilizam soluções de tecnologia da informação e comunicação para otimizar suas ações, dentre outros aspectos (Costa, 2017)

A prevenção e o enfrentamento realizados pelos órgãos de segurança pública sobre o crime organizado nascem com o conjunto de normas jurídicas, editados pelo parlamento, para legitimar as medidas necessárias à tutela dos interesses da coletividade. Alberto Silva Franco (2002) assevera que a criminalidade de massa, programada, planejada e executada de forma profissional é fruto do processo de globalização. Porém, na medida em que esse fenômeno ultrapassa os limites territoriais de um Estado, ele vem se distanciando "dos padrões de criminalidade que até então tinham sido objeto de consideração penal" (Franco, 2002).

Para amarrar melhor a relação entre o crime organizado e o policiamento inteligente, o texto poderia ser ajustado da seguinte forma:

Embora haja uma tendência a se acreditar que os órgãos de segurança pública e suas estruturas de inteligência dispõem de instrumentos suficientes para controlar e combater o crime organizado, o que se observa, em muitos casos, são ações simbólicas e insuficientes para enfrentar as atividades reais e dinâmicas das

organizações criminosas. O crime organizado impõe desafios que transcendem o espaço físico, explorando o mundo virtual como um novo ambiente de oportunidades, riquezas e influência. Nesse contexto, o policiamento inteligente se torna fundamental, pois permite um monitoramento mais preciso das atividades criminosas, tanto no ambiente físico quanto no ciberespaço, onde as facções buscam novas formas de atuação e comunicação.

O uso de inteligência preditiva, análise de redes sociais e vigilância cibernética são ferramentas que podem antecipar movimentações e desmantelar operações antes mesmo de se concretizarem, além de identificar conexões e padrões que seriam imperceptíveis por métodos tradicionais. Assim, ao integrar tecnologias avançadas e análise de dados, o policiamento inteligente pode tornar-se uma resposta efetiva aos desafios impostos pelo crime organizado, não apenas reagindo a eventos, mas prevenindo e mitigando a influência e o alcance dessas organizações em múltiplos territórios – físicos e virtuais.

2.2.3 OS DESAFIOS SEGURANÇA PÚBLICA NAS CIDADES 4.0

De acordo com Castells (2010), a globalização assumiu uma nova dimensão com o advento das tecnologias da informação, como o computador e a internet, que transformaram as relações sociais, acelerando a integração mundial e promovendo uma nova dinâmica no uso do espaço cibernético.

Em virtude desse cenário, uma nova era da globalização surgiu com o advento das inovações tecnológicas, protagonizadas pela informática, notadamente pelo computador e pela internet. Com isso, as complexas relações sociais e integração mundial ganharam um novo terreno. A rede mundial de computadores gerou uma explosão no tráfego de dados e informações, marcando uma significativa mudança no comportamento das pessoas quanto ao uso do ambiente cibernético, para substituir e/ou incrementar as relações reais e espaciais.

É possível evidenciar as tendências que marcaram essa mudança de comportamento, com impacto na segurança pública, objeto de interesse da inteligência. Por exemplo, as manifestações

públicas agora têm instrumentos para proporcionar o recrutamento, divulgação, organização e funcionamento, ou seja, as redes sociais.

De igual modo, buscando superar dificuldades de ordem financeira e operacional, o Estado tem encontrado, na tecnologia da informação comunicação, a solução para dar maior controle, segurança e celeridade na prestação de serviços, tais como a tramitação de atos e documentos eletrônicos, pagamento de servidores e aposentados, processos de compras (pregão eletrônico), etc.

Cristina Kunrath (2017) aponta que, embora a tecnologia da informação e comunicação traga inúmeros benefícios, ela também gera efeitos colaterais que impactam negativamente a paz social, a ordem pública e econômica. A autora ressalta que o cibercrime tem se tornado um fenômeno global, com o Brasil destacando-se como um dos países mais afetados, sendo considerado um "paraíso da pirataria virtual". Desde a criação da *internet*, na década de 1960, os ilícitos cibernéticos têm crescido de forma exponencial, acompanhando a expansão da web em escala global. Em países com elevado nível tecnológico, o cibercrime é uma realidade inevitável, e, no caso do Brasil, o estágio atual de desenvolvimento tecnológico tem favorecido uma alta incidência de ataques cibernéticos.

Como aponta Kunrath (2017), o ciberespaço tem se tornado palco de crimes, que vão desde fraudes financeiras e espionagem industrial até atividades ilícitas como tráfico de pessoas e pornografia infantil. Nesse sentido, a internet profunda tem sido utilizada por organizações criminosas para expandir suas operações ilícitas de forma global (Smith, 2020).

Kunrath (2017) ainda observa que, no ciberespaço, ocorrem crimes que consistem essencialmente na exteriorização de comportamentos ilícitos por parte dos usuários das tecnologias da informação e internautas. Essas ações criminosas visam principalmente fraudes em instituições financeiras, desvio de dinheiro em empresas, espionagem industrial, além de outras práticas como pirataria de programas, pornografia infantil, tráfico de bens e mercados ilícitos, intolerância racial, entre outras condutas.

A internet profunda, composta por áreas não indexadas pelos motores de busca convencionais e de difícil acesso para usuários comuns, abriga um mercado ilícito vasto. Criminosos organizados aproveitam esse ambiente para realizar atividades ilegais como tráfico

de drogas, armas, pessoas e órgãos humanos, além de fraudar transações financeiras e comercializar pornografia infantil (Smith, 2020). Essas operações, fora do alcance das autoridades tradicionais, comprometem a segurança pública e exigem uma resposta mais eficaz das instituições responsáveis.

Mais do que nunca, a atividade de inteligência, ao lado das ações de investigação policial, tem sido o caminho para fazer frente a esse mundo complexo, com exorbitante tráfego de dados, em especial para prevenir e controlar as ações das organizações criminosas no ambiente cibernético.

Anteriormente foi falado sobre o modelo explicativo de emprego da ISP como instrumento para assessorar o decisor nas ações de preservação ordem pública, da proteção de pessoas e seus bens. Para além disso, ficou evidenciada a dimensão da complexidade, dos desafios, obstáculos do trabalho hercúleo para o controle e enfrentamento dos crimes organizados no mundo virtual. (Kunrath, 2017).

Nesse sentido, é possível elencar alguns dos principais contratempos impostos ao policiamento ostensivo na prevenção e na resposta imediata, como aos atos de investigação sobre o crime organizado no ambiente cibernético (Akhgar; Straniforth; Bosco, 2014; Wendt e Barreto, 2013), dentre eles o aumento exponencial das relações humanas em escala global proporcionada pela internet, criação de uma realidade virtual sem barreiras delimitação territorial, dentre outros. Soma-se ainda o uso indiscriminado, sem fiscalização e controle de ferramentas para ocultar a origem do endereço IP ou esconder mensagens, com uso de criptografia, inexistência limitação na estrutura e aptidão dos profissionais de segurança pública, inclusive no campo da inteligência, para prevenir e enfrentar as ações ilícitas mundo virtual, sensação de anonimato e de liberdade no ciberespaço, proporcionada pela ausência ou ineficiência de regras de conduta, fiscalização e responsabilização, inclusive na esfera judicial, bem como um conjunto de normas legais ineficientes, insuficientes e meramente simbólicas para regular conduta, fiscalização e responsabilização de atos no ambiente cibernético.

Importante salientar que o endereço IP, sigla de "Internet Protocol" (protocolo de internet), é um identificador único que distingue um dispositivo em uma rede local ou na internet. Ele é

fundamental para o protocolo da internet, que define as regras e o formato dos dados transmitidos entre dispositivos, permitindo a comunicação eficiente em uma rede (Kaspersky, 2024).

No que tange aos atos normativos, é crucial evidenciar o longo e complexo processo de aprovação de projetos de lei no parlamento brasileiro, especialmente aqueles que afetam a segurança pública e a atividade de Inteligência. Um exemplo relevante é o Projeto de Lei - PL nº 2.310/2022, de autoria dos Deputados Subtenente Gonzaga e Capitão Derrite. Esse PL nº 2.310/2022 trata das ações de inteligência exercidas pelas instituições previstas no artigo 144 da Constituição Federal, como as Polícias Militares, Rodoviárias Federais e Penais. O projeto visa regulamentar a produção, coleta e tratamento de informações necessárias para a prevenção de crimes e violência, garantindo a preservação da ordem pública e a segurança de pessoas e bens.

A justificativa do projeto argumenta que, apesar de as Polícias Militares já atuarem na coleta de informações, muitas vezes esse conhecimento não é formalmente reconhecido e acaba descartado por ser considerado usurpação da função das polícias judiciárias. A proposta busca legitimar essas ações como "ações de inteligência", diferenciando-as da investigação criminal, de competência exclusiva das polícias civis e federais. A aprovação dessa legislação seria um passo importante para oficializar e maximizar a utilização da inteligência policial em ações preventivas e operacionais.

Neste projeto, a regulamentação das ações de inteligência das Polícias Militares e outros órgãos seria um avanço para fortalecer as políticas públicas de segurança, adaptando-as às realidades tecnológicas e urbanas contemporâneas. Ao regulamentar essas ações, o projeto contribui para a criação de um arcabouço legal mais robusto que integra esse processamento de informações estratégicas à rotina das forças de segurança pública, aumentando a eficiência na prevenção de crimes e a proteção da ordem pública.

O Projeto de Lei nº 2.310/2022, que trata das ações de inteligência exercidas por instituições previstas no artigo 144 da Constituição Federal, atualmente está sob análise na Comissão de Assuntos Econômicos (CAE) do Senado. O relator designado é o Senador Fernando Farias, que emitirá parecer sobre a matéria. O projeto busca regulamentar as ações supramencionadas das Polícias Militares e outros órgãos, e está aguardando novas deliberações (Senado Federal).

Esse projeto é relevante, pois visa estruturar a utilização da inteligência nas forças de segurança pública, promovendo eficiência e prevenção em um contexto de Cidades 4.0.

Outro exemplo claro disso é o Projeto de Lei nº 1.864/2019, que propõe medidas contra o crime organizado e crimes violentos. A proposta visa alterar normativos como o Código Penal - CP, Código de Processo Penal - CPP, e a Lei dos Crimes Hediondos, entre outros. No entanto, essa proposta ainda encontra resistência no parlamento e passa por diversas discussões e emendas.

Ainda que haja boa intenção, o projeto enfrenta desafios conceituais, especialmente no que diz respeito às definições de Inteligência de Segurança Pública. É importante que as atribuições das instituições de segurança pública sejam claramente definidas para evitar confusões legais e garantir a segurança jurídica dos profissionais envolvidos.

O Projeto de Lei do Senado nº 2719/2019, proposto pelo Senador Major Olímpio, busca estabelecer um marco regulatório para a Atividade de Inteligência Brasileira. Esse projeto tem por objetivo disciplinar a produção, difusão e salvaguarda de informações sensíveis com o intuito de proteger a sociedade e o Estado. Ele também propõe a cooperação entre diversos órgãos de inteligência, como as polícias, departamentos penitenciários, Forças Armadas, ABIN, Ministério Público, e outros órgãos relacionados à segurança nacional.

Atualmente, o projeto se encontra em tramitação nas comissões do Senado Federal, tendo sido discutido na Comissão de Relações Exteriores e Defesa Nacional (CRE) e na Comissão de Constituição, Justiça e Cidadania (CCJ). Até 2022, o projeto passou por diversas análises, incluindo a rejeição de algumas emendas e a necessidade de designação de um novo relator para continuar seu trâmite. A matéria aguarda novas deliberações.

Este projeto é altamente relevante sobretudo para os temas relacionados à segurança pública e à inteligência nas Cidades 4.0. A regulamentação da atividade de inteligência é um ponto central para a modernização das políticas de segurança, que precisam se adaptar às novas demandas da era digital, onde o cibercrime e a criminalidade organizada atuam de forma cada vez mais sofisticada. O PL nº 2719/2019 contribui diretamente para o fortalecimento das capacidades do Estado em termos de gestão informacional de segurança pública, que

é uma das ferramentas essenciais para prevenir e combater crimes, além de promover a segurança e ordem pública em um ambiente cada vez mais interconectado.

Apesar das dificuldades, a proposta visa fornecer maior suporte e segurança aos agentes de inteligência, com impacto direto na segurança pública. O ciberterritório já se mostra um terreno fértil para a proliferação de crimes organizados, destacando a urgência dessas medidas legislativas.

O Projeto de Lei nº 1.864/2019, de autoria da Senadora Eliziane Gama, visa estabelecer medidas contra a corrupção e o crime organizado, com foco em crimes violentos. Esse projeto propõe alterações importantes em diversas legislações, como o Código Penal, Código de Processo Penal, e a Lei de Execução Penal, além de outras leis relevantes para a segurança pública. A proposta envolve medidas para aprimorar a atuação das forças de segurança, especialmente no que tange à cooperação entre diferentes órgãos de inteligência e segurança.

Atualmente, o projeto está em tramitação na Comissão de Constituição, Justiça e Cidadania (CCJ) do Senado e aguarda designação de um novo relator, após a conclusão da legislatura de 2022. Diversas emendas foram apresentadas ao longo do processo, refletindo a complexidade e o impacto potencial da proposta, que abrange temas como interceptação de comunicações eletrônicas, prisão por condenação em órgão colegiado, e atuação de agentes policiais disfarçados.

Este projeto também é extremamente relevante, pois oferece um marco normativo que pode fortalecer a capacidade das forças de segurança de agir de forma preventiva e repressiva contra o crime organizado, utilizando mecanismos de inteligência e cooperação interinstitucional. A proposta também aborda a atuação em ambientes cada vez mais digitais, conectando-se com os desafios contemporâneos de governança em cidades inteligentes.

Nesse ínterim e diante das transformações proporcionadas pela era digital e o avanço das Cidades 4.0, a inteligência corrente torna-se um pilar fundamental para a segurança pública, especialmente no âmbito da Polícia Militar. Este estudo evidencia a sua relevância como ferramenta de assessoramento na tomada de decisões, destacando seu papel na prevenção e repressão ao crime. No contexto das cidades

inteligentes, a utilização da tecnologia e da coleta de informações em tempo real potencializa a capacidade das forças de segurança de atuar de forma mais eficiente e eficaz.

No entanto, os desafios que surgem com o crescimento do ciberespaço exigem novas abordagens. A complexidade das ameaças digitais e a dificuldade em identificar e reprimir atividades criminosas dissimuladas no ambiente virtual impõem uma necessidade de evolução contínua dos mecanismos de inteligência de segurança pública. A integração entre as forças de segurança e a criação de um marco normativo adequado são fundamentais para garantir que a mesma seja utilizada de forma eficaz para proteger a ordem pública.

Em suma, a inteligência de segurança pública, alinhada com as inovações tecnológicas e as novas demandas das Cidades 4.0, desponta como um elemento imprescindível para o enfrentamento dos desafios contemporâneos. A modernização das estratégias de segurança, bem como o fortalecimento dos agentes envolvidos, é essencial para assegurar a paz social e a confiança da população nas instituições de segurança.

Pergunta-se ainda quais as principais dificuldades que as Agências de Inteligência de Segurança Pública enfrentam para prevenir e controlar o crime organizado no ambiente cibernético? Diante de uma abordagem multidisciplinar, identificou-se que o espaço físico deixou de ser o único ambiente explorado pelas organizações criminosas, diante das vulnerabilidades do ambiente virtual, insegurança jurídica, insuficiência de mecanismos controle, fiscalização e responsabilização adequada aos agentes criminosos. O resultado desse estudo evidenciou uma série de obstáculos para os profissionais de inteligência de segurança pública.

É preciso, portanto, buscar um caminho para o bem comum, com trabalho conjunto entre o Poder Público, a sociedade e os profissionais envolvidos, a fim de construir uma comunidade livre, justa e solidária. É necessário discutir o assunto de forma profícua e envolver todos os setores das sociedades civil e política.

O debate não se exaure aqui, exigindo estudos sobre os impactos dos instrumentos de inteligência e da esperada conversão, com os devidos ajustes, dos Projetos de Lei apresentados, bem como promover a iniciativa de novas propostas que visem a trazer maior engajamento para um verdadeiro combate ao crime organizado.

A segurança pública, no Brasil, é atribuída a diversas instituições, entre elas a Polícia Militar (PM), que possui a missão constitucional de preservar a ordem pública e garantir a incolumidade das pessoas e do patrimônio (Constituição Federal, 1988). Esse conceito é definido na teoria jurídica como a garantia de estabilidade, proteção e manutenção da ordem pública interna (Lenza, 2022). A Polícia Militar desempenha um papel fundamental ao atuar preventivamente para evitar a ocorrência de crimes e também de forma repressiva quando a ordem é perturbada. A Polícia Militar do Distrito Federal - PMDF, especificamente, além dessas funções, tem a responsabilidade de proteger os poderes constituídos do país, o que evidencia sua relevância para a estabilidade política e social no Distrito Federal (Alves, 2018).

A importância da Polícia Militar se reflete também em pesquisas científicas que buscam compreender melhor os desafios e a atuação dessas instituições. Estudos sugerem que a polícia contribui para o bom desenvolvimento do Estado ao garantir segurança à população, além de apoiar na formulação de políticas públicas mais eficazes (Faiad *et al.*, 2022). Essas pesquisas fornecem subsídios técnico-científicos essenciais para a melhoria contínua da atividade policial, seja no desenvolvimento de ações práticas que visam a redução da criminalidade, seja no aperfeiçoamento do ambiente de trabalho para os profissionais da segurança pública.

2.3 CIDADES 4.0

2.3.1 A TECNOLOGIA NAS CIDADES 4.0

O conceito de cidades inteligentes, também conhecido como *smart cities*, envolve a aplicação de tecnologias avançadas para melhorar a eficiência dos serviços públicos, aumentar a qualidade de vida dos cidadãos e promover um desenvolvimento sustentável. A transição das cidades convencionais para as Cidades Inteligentes, como destacado por Carlos T. Calafate *et al*. (2020), integra tecnologias de ponta, como a IoT e a análise intensiva de *big data*, para aprimorar a gestão urbana. Neste contexto, a segurança pública é uma área de grande relevância, onde a inteligência corrente e o policiamento orientado pela inteligência (*Intelligence-Led Policing* - ILP) se tornam fundamentais para a eficiência das operações policiais.

Schuurman, Baccarne, De Marez e Mechant (2012) destacam que, desde os primórdios das civilizações, as cidades surgiram como uma resposta natural às condições de vida, desempenhando um papel fundamental no fortalecimento das diversas dimensões da existência humana e representando uma consequência duradoura da evolução humana.

Historicamente, as cidades passaram por grandes transformações. Na era pré-industrial, muitas cidades eram autossuficientes, baseadas na agricultura e habilidades técnicas. Com a Revolução Industrial, as cidades se tornaram centros de fabricação, influenciadas por empresários, matérias-primas e fontes de energia (Musterd, Ostendorf, 2003).

Após a Segunda Guerra Mundial, surgiram novos modelos urbanos, expandindo-se e conectando-se internacionalmente, dominados pelos setores de serviços (ibid., 2003). Hoje, as cidades enfrentam desafios relacionados à inclusão social, desenvolvimento econômico, segurança, sustentabilidade e mobilidade. O advento das TIC permitiu maior participação cidadã na inovação urbana (Caragliu, Del Bo, Nijkamp, 2009).

As cidades inteligentes, utilizando TIC, visam melhorar a qualidade de vida e promover o desenvolvimento sustentável (Capdevila, Zarlenga, 2015). A tecnologia deve ser aplicada de forma holística, descentralizada e colaborativa (Rizzon, Bertelli, Matte, Graebin, Macke, 2017). No entanto, a transição digital também pode gerar desafios, como a falta de inovação responsável (Garnett, Van Calster, Reins, 2018). É crucial evoluir de "transições nas cidades" para "transições das cidades" (Griffiths, Sovacool, 2020).

Explora-se em parte desse estudo, conceitos e tendências das cidades inteligentes, incluindo a relevância do estudo de Giffinger *et al*. (2007) sobre as seis dimensões de uma cidade inteligente.

O conceito de Cidade Inteligente surgiu nos anos 90, para classificar o desenvolvimento urbano dependente de inovação, tecnologia e globalização, principalmente em uma perspectiva econômica (Gibson, Kozmetsky, Smilor, 1992).

Atualmente, uma cidade inteligente é caracterizada pelo uso extensivo das TIC em infraestruturas e na participação ativa do capital humano e social (Caragliu, Del Bo, Nijkamp, 2009). Segundo Lee *et al*.

(2013), essa abordagem garante a qualidade ambiental e a sustentabilidade urbana. Além disso, uma cidade inteligente conecta infraestruturas físicas, sociais e empresariais para alavancar a inteligência coletiva (Harrison *et al*., 2010).

O objetivo final de uma cidade inteligente é melhorar a gestão e o uso dos recursos públicos, aumentar a qualidade dos serviços oferecidos aos cidadãos e reduzir os custos operacionais (Zanella, Bui, Castellani, 2014). Elas utilizam tecnologias de computação inteligente para oferecer serviços essenciais de forma eficiente e interconectada (Washburn *et al*., 2010).

Diversos conceitos são frequentemente conectados ao de cidade inteligente, todos concentrados no uso das TIC em ambientes urbanos (Capdevila, Zarlenga, 2015).

Quadro 1 – Conceitos habitualmente conectados ao de Cidade Inteligente

Conceito	Autores
intelligent city	Komninos, 2002
information city	Castells, 1996
wired city	Dutton, 1987
knowledge city	Yigitcanlar et al., 2008; Edvinsson, 2006;
	Ergazakis et al., 2007; Dvir & Pasher, 2004
digital city	Yovanof & Hazapis, 2009
ubiquitous city	Lee et al., 2013

Fonte: (Rizzon, Bertelli, Matte, Graebin, Macke, 2017)

A definição de Giffinger *et al*. (2007) identificam seis dimensões para avaliar quão inteligente uma cidade é.

Quadro 2 – Dimensões da operacionalização do conceito de Cidade Inteligente e respetivos indicadores demonstrativos

Dimensões	Exemplo de indicadores
Smart People	Educação

Smart Economy	Empreendedorismo
Smart Governance	Governos participativos
Smart Environment	Proteção ambiental
Smart Mobility	Acessibilidades
Smart Living	Cultura

Fonte: autoria própria com base em (Selada; Silva, 2020).

As seis dimensões incluem:

a) ***Smart People*: Avalia a educação, preço da habitação e emprego.**
b) ***Smart Economy*: Avalia a qualidade das empresas e o ambiente para empreendedorismo.**
c) ***Smart Governance*: Relaciona-se com a participação cidadã na vida pública.**
d) ***Smart Environment*: Envolve a gestão de recursos naturais e proteção ambiental.**
e) ***Smart Mobility*: Refere-se à acessibilidade e rede de TIC.**
f) ***Smart Living*: Inclui saúde, segurança, cultura e habitação**

(Selada, Silva, 2020).

Componentes-chave para uma cidade inteligente incluem tecnologia, cidadãos e instituições (Mendes, Correia, Serra, 2021). Se faz necessário investir em capital humano e social junto com infraestruturas TIC para fomentar um crescimento sustentável (Nam, Pardo, 2011).

Esforços relacionados à sustentabilidade urbana geram tensão entre o ideal ambiental e a realidade de cidades poluentes e em expansão. É fundamental equilibrar o conceito de cidade inteligente com os três pilares da sustentabilidade: ambiente, sociedade e economia (Joss, Molella, 2013; Ahvenniemi *et al*., 2017).

Nas últimas duas décadas, surgiram inúmeras cidades inteligentes devido a imperativos demográficos, ambientais, econômicos e sociais. Na Europa, projetos de renovação urbana inteligente são proeminentes, com Amsterdã como exemplo líder. Em 2013, havia 143 projetos de cidades inteligentes em todo o mundo, incluindo Ásia, Europa, América do Norte, América do Sul e Oriente Médio. África também começou a desenvolver projetos (Mendes,

Correia, Serra, 2021). Barcelona é outro exemplo notável, reconhecida como Capital Europeia da Inovação em 2014, com o projeto "Barcelona as a people city" focado em crescimento econômico e bem-estar (Capdevila; Zarlenga, 2015).

Em relação a *eco-cities*, a cidade de Masdar é destaque, situada no deserto próximo a Abu Dhabi (Yigitcanlar *et al*., 2019).

O Caso de Estudo da Cidade de Masdar – Abu Dhabi. Masdar, projetada em 2006, é uma cidade sustentável, inteligente e sem pegada de carbono, utilizando energia renovável e recursos eficientes (Lau, 2012). Desenvolvida pela companhia de energia de Abu Dhabi, a cidade visa reduzir desperdícios e emissões de carbono, com foco em energia solar e dessalinização de água.

Masdar é um modelo para futuras cidades sustentáveis, sendo projetada com tecnologia avançada para alcançar alta sustentabilidade (Adfec, 2010). A cidade utiliza energia solar intensivamente, com a maior planta solar fotovoltaica do Oriente Médio.

Mas, por uma perspectiva crítica, Masdar enfrenta problemas quanto à perda de privacidade e autodeterminação, devido à vigilância por empresas de alta tecnologia (Ferreira; Oliveira, 2020). A viabilidade financeira é outra preocupação, considerando o alto custo de US$ 22 bilhões. Questões políticas também são levantadas, dado o regime dos Emirados Árabes Unidos.

As cidades inteligentes são uma aposta crescente para um futuro sustentável. Masdar é um exemplo de eco-city, representando um modelo de cidade 100% sustentável. No entanto, a capacidade financeira dos Emirados Árabes Unidos é uma barreira para replicação em economias menos favorecidas.

Governos locais devem estruturar padrões de sustentabilidade e medir o desempenho de projetos de *eco-cities*. A questão do uso de dados dos cidadãos requer transparência e consentimento. A participação cidadã é crucial para o sucesso das cidades inteligentes.

Com relação à segurança pública, autores como Hollands (2008) e Kitchin (2014) fornecem análises críticas sobre o papel das cidades inteligentes na melhoria da segurança pública, destacando o uso de tecnologias emergentes como um fator transformador na gestão urbana. Hollands (2008) questiona a narrativa convencional de que as

cidades inteligentes, por meio de suas infraestruturas tecnológicas, podem resolver automaticamente os problemas urbanos, incluindo questões de segurança. Ele enfatiza que, embora a integração de sensores e sistemas de monitoramento possa aumentar a eficiência na resposta a incidentes, é fundamental que essas tecnologias sejam implementadas de maneira inclusiva e orientada para o bem-estar social. O autor argumenta que as cidades inteligentes devem ir além de interesses corporativos, priorizando soluções que atendam às necessidades reais dos cidadãos.

Kitchin (2014), por sua vez, explora como o uso de *big data* em tempo real pode revolucionar o urbanismo inteligente, especialmente no que se refere à segurança pública. Ele explica que a coleta e análise contínua de dados provenientes de sensores e dispositivos conectados oferecem uma oportunidade sem precedentes para monitorar o ambiente urbano e prever possíveis incidentes. Segundo Kitchin, essa abordagem permite uma gestão proativa da segurança, na qual as forças de segurança podem responder rapidamente a ameaças emergentes. No entanto, ele também alerta sobre os riscos associados a essas tecnologias, como a potencial violação da privacidade e o uso inadequado de dados pessoais. Esse autor destaca a necessidade de uma governança responsável e de políticas que assegurem o equilíbrio entre segurança e direitos individuais.

A partir dessas perspectivas, fica claro que a aplicação de tecnologias inteligentes na segurança pública das Cidades 4.0 oferece tanto oportunidades quanto desafios. A efetividade de sistemas integrados de monitoramento depende de uma implementação ética e de uma infraestrutura tecnológica que garanta a proteção dos dados dos cidadãos. Assim, o debate iniciado por Hollands e Kitchin continua relevante, principalmente à medida que as cidades se tornam cada vez mais dependentes de soluções tecnológicas para promover a segurança urbana.

2.3.2 INTELIGÊNCIA CORRENTE NA POLÍCIA MILITAR E OS DESAFIOS NAS CIDADES 4.0

A transformação digital e o desenvolvimento tecnológico têm proporcionado uma revolução no conceito de Cidades 4.0, com implicações diretas na segurança pública, na melhoria da gestão e operacionalização de efetivo para a redução da criminalidade. A Polícia Militar (PM) vem adotando práticas inovadoras de inteligência corrente

e policiamento orientado pela inteligência para promover políticas públicas de segurança mais eficazes, como a Operação Antena mencionada anteriormente.

O tema de inteligência corrente na Polícia Militar em cidades digitais é fundamental para entender como a informação pode ser transformada em processamento de informações estratégicas úteis para a tomada de decisões. Abaixo será observada a teoria da inteligência e sua aplicação prática, abordando conceitos como pesquisa de inteligência, distinção entre informação e inteligência, e o processo de inteligência. Além disso, explora-se os desafios que surgem na implementação de inteligência corrente em contextos de Cidades 4.0.

A pesquisa de inteligência é uma área complexa e cheia de nuances, onde se busca transformar dados brutos em informações úteis para a tomada de decisão. A importância dessa ferramenta analítica é destacada pela sua capacidade de proporcionar controle sobre uma situação, conferindo poder àqueles que a detêm (Cohen, 1986). A inteligência, portanto, não é uma forma de prever o futuro, mas uma ciência exata baseada em métodos de pesquisa quantitativos e qualitativos. (Prunckun, 2015)

Segundo Prunckun (2015) existem várias definições de inteligência, mas essas definições podem ser resumidas em quatro significados principais: 1. Ações ou processos usados para produzir conhecimento; 2. O corpo de conhecimento assim produzido; 3. Organizações que lidam com conhecimento; 4. Relatórios e briefings produzidos para tomadores de decisão.

Essas definições ocorrem no contexto de sigilo, diferenciando-se assim de outras formas de pesquisa (Lowenthal, 2009).

Seguindo esse raciocínio, a inteligência, enquanto corpo de conhecimento, trata de adversários, potenciais adversários ou áreas de operação, úteis para gestores planejarem e executarem suas funções. Exemplos práticos incluem contextos de segurança nacional, militar, policial, empresarial e do setor privado, onde essa ferramenta analítica pode alertar sobre atividades e planejamentos específicos de interesse (Lowenthal, 2009).

O processo de inteligência, tradicionalmente chamado de ciclo de inteligência, envolve sete etapas principais: 1. Definição de direção

(formulação do problema e planejamento); 2. Coleta de informações; 3. Colação de dados; 4. Manipulação e processamento de dados; 5. Análise de dados; 6. Redação de relatórios e 7. Disseminação para tomadores de decisão. Esse ciclo pode ser repetido ou ajustado conforme necessário, com a análise contínua de novos dados para gerar processamento de informações estratégicas relevantes (Gill, Marrin e Phythian, 2009).

Gráfico 1 – Ciclo de Inteligência

Fonte: Elaboração própria adaptado de Gill, Marrin e Phythian (2009).

Em Inteligência versus Investigação, a diferença fundamental entre a primeira e investigação é que a investigação busca identificar e processar os responsáveis por um evento, enquanto a inteligência visa proporcionar *insights* para reduzir incertezas. Embora essa ferramenta analítica possa auxiliar em investigações, seu foco principal é fornecer informações para a tomada de decisões estratégicas (Gill, Marrin e Phythian, 2009).

A teoria da inteligência, apesar de ser discutida há décadas, ainda carece de consenso entre os estudiosos. No entanto, ela é essencial para entender e testar fenômenos relacionados à inteligência. A teoria proposta por Gill, Marrin e Phythian (2009) sugere que a inteligência deve ser defensiva ou ofensiva, oportuna e defensável.

A inteligência defensiva busca compreender em como lidar com ameaças, vulnerabilidades e riscos. Já a inteligência ofensiva apoia a execução de missões proativas, como a seleção de alvos em operações militares. Ambas são cruciais para a eficácia das operações de inteligência (Gill, Marrin e Phythian, 2009).

A inteligência deve ser fornecida de forma oportuna para ser útil e defensável, garantindo que os métodos utilizados sejam transparentes e replicáveis. Isso permite que os resultados sejam revisados e validados, assegurando a integridade das conclusões (Walsh, 2011).

A implementação de inteligência corrente em Cidades 4.0 apresenta desafios específicos, como a necessidade de integrar grandes volumes de dados de diversas fontes e a proteção de privacidade dos cidadãos. Além disso, a coordenação entre diferentes agências e a adaptação a tecnologias emergentes são aspectos críticos que precisam ser geridos para assegurar a eficácia das operações de inteligência na segurança pública.

A inteligência corrente na Polícia Militar do Distrito Federal (PMDF) oferece percepções estratégicas e operacionais que auxiliam na tomada de decisões em tempo real. Diferentemente de outras abordagens de inteligência, como a inteligência estratégica, que foca no planejamento de longo prazo, a inteligência corrente tem como objetivo fornecer informações atualizadas e relevantes para o apoio imediato às operações policiais e à gestão de crises. Essa modalidade é caracterizada pelo uso contínuo de dados coletados de fontes diversas, incluindo tecnologias avançadas como câmeras de monitoramento, sensores IoT e sistemas de georreferenciamento, permitindo um monitoramento eficaz e uma resposta ágil a incidentes de segurança.

Além disso, a inteligência corrente desempenha um papel crucial na identificação e mitigação de ameaças, agindo de forma preventiva e reativa. De acordo com a Carta Brasileira para Cidades Inteligentes, o desenvolvimento centrado no cidadão e a inclusão digital são pilares fundamentais para o sucesso das cidades inteligentes (cartacidadesinteligentes.org.br, 2023). Nesse sentido, a transformação digital, quando aliada ao policiamento orientado pela inteligência, fortalece a capacidade da PMDF de operar em um ambiente urbano dinâmico, característico das Cidades 4.0. Essa integração entre

tecnologia, dados e práticas policiais contribui para criar um ambiente mais seguro, resiliente e adaptado às necessidades da população.

Segundo a Doutrina da Atividade de Inteligência de 2023, a inteligência corrente visa manter as autoridades informadas de maneira contínua sobre eventos e situações em curso, bem como sobre suas evoluções. Esse tipo de ferramenta analítica é caracterizado por um enfoque objetivo, descritivo e interpretativo, concentrando-se em fatos e atores significativos no contexto do acompanhamento e seus desenvolvimentos subsequentes. Para isso, a Inteligência Corrente considera toda a produção prévia relacionada à situação monitorada, buscando identificar os atores envolvidos, as variáveis relevantes e a interação entre eles (Brasil, 2023).

O produto resultante dessa inteligência é um relatório descritivo, conciso, direto e periódico, que relata a evolução da situação ou evento em questão. Quando possível, também inclui uma análise interpretativa que aponta a tendência de evolução no curto prazo. Exemplos de Inteligência Corrente incluem o monitoramento de manifestações e paralisações com potencial para perturbar a ordem nacional, informações sobre acessos não autorizados a redes de infraestrutura estratégica, a supervisão de emergências e o acompanhamento de crises econômicas e ambientais, tanto no Brasil quanto no exterior (Brasil, 2023).

Nesse ínterim, essa ferramenta analítica baseada em dados em tempo real é essencial na gestão da segurança pública em Cidades 4.0. Ela permite a coleta, análise e disseminação de informações em tempo real, oferecendo aos gestores públicos uma visão clara das necessidades e desafios da segurança. A integração de tecnologias avançadas como a IoT, *big data* e IA potencializa essa capacidade, permitindo uma resposta mais rápida e eficaz às ocorrências.

A inteligência corrente não só melhora a eficiência das operações policiais, mas também contribui para a elaboração de políticas públicas mais alinhadas às reais necessidades da sociedade. Segundo Tavares (2024), o uso de dados para a tomada de decisão é fundamental para a construção de cidades inteligentes, pois permite o planejamento urbano e tecnológico com base em evidências concretas.

O ILP é uma abordagem moderna que utiliza a inteligência para orientar o planejamento e a tomada de decisões nas atividades

policiais. De acordo com a Organização para a Segurança e Cooperação na Europa (OSCE), o ILP visa identificar e planejar medidas corretivas para combater ameaças, como o terrorismo e o crime organizado, além de ser aplicado no planejamento diário das operações policiais (OSCE, 2017). Silva *et al*. (2020) afirmam que o ILP, adotado inicialmente no Reino Unido, transforma a abordagem tradicional reativa em uma estratégia proativa e preventiva. A adoção do ILP pela PMDF tem produzido em muitas situações pela inteligência corrente e exemplifica, como na Operação Atena, a aplicação prática de políticas públicas de segurança orientadas por dados.

2.3.3 A IMPORTÂNCIA DA INTEGRAÇÃO TECNOLÓGICA

A integração de tecnologias avançadas, como a IA e a IoT, no contexto das cidades inteligentes e 4.0, é essencial para a eficácia da segurança pública. Essas tecnologias permitem a coleta e análise de grandes volumes de dados, proporcionando uma visão detalhada das atividades urbanas e facilitando a tomada de decisões baseadas em evidências. A análise de *big data*, por exemplo, permite identificar padrões de comportamento e prever possíveis incidentes de segurança, possibilitando uma atuação preventiva das forças policiais. (Centro de Gestão e Estudos Estratégicos, 2022)

A PM tem implementado diversas estratégias para utilizar essas tecnologias na promoção da segurança pública. A adoção de sistemas de monitoramento, como por exemplo, a Operação Atena na PMDF, e a análise de dados coletados por dispositivos conectados permitem uma resposta mais rápida e eficiente a incidentes. Além disso, a colaboração entre diferentes órgãos de segurança e a integração de dados entre plataformas tecnológicas são fundamentais para o sucesso das operações.

2.3.4 POLÍTICAS PÚBLICAS E SEGURANÇA EM CIDADES INTELIGENTES

A implementação de políticas públicas eficazes é crucial para o sucesso das cidades inteligentes. O desenvolvimento de um plano estratégico que contemple a inclusão digital, a sustentabilidade e a segurança pública são essenciais para criar um ambiente urbano seguro e eficiente. Segundo Tavares (2023), o planejamento urbano e tecnológico, a mobilidade e o transporte público são fatores primordiais

para tornar as cidades inteligentes e conectadas. A utilização de dados coletados por meio de tecnologias avançadas permite aos gestores públicos traçar diretrizes e metas para a construção colaborativa de uma cidade inteligente.

A segurança pública é um dos principais desafios enfrentados pelas cidades inteligentes. A violência urbana e o crime organizado exigem uma atuação eficiente das forças de segurança. A adoção de políticas públicas que promovam a integração tecnológica e a utilização de inteligência corrente é essencial para a eficácia das operações policiais. A PMDF, buscando diuturnamente a utilização de tecnologias avançadas e a colaboração com diferentes órgãos de segurança, tem se destacado na promoção da segurança pública no Distrito Federal.

Dessa forma a transição para cidades inteligentes em 4.0 representa um avanço significativo na gestão urbana, oferecendo novas oportunidades para a promoção da segurança pública. A utilização de tecnologias avançadas, como a IA e a IoT, aliada ao POI e inteligência corrente, permite uma atuação mais eficiente e proativa das forças de segurança. A implementação de políticas públicas eficazes e a integração de dados entre diferentes plataformas tecnológicas são fundamentais para o sucesso das operações policiais.

A PMDF desempenha um papel relevante na promoção da segurança pública no Distrito Federal, utilizando a inteligência corrente e a integração tecnológica para identificar e mitigar ameaças. Nesse cenário, a colaboração entre diferentes órgãos de segurança e a utilização de dados coletados por meio de tecnologias avançadas são essenciais para criar um ambiente urbano mais seguro e resiliente. A eficácia dessa ferramenta analítica baseada em dados em tempo real pode ser significativamente aumentada através de investimentos em tecnologia e capacitação, além de mudanças culturais nas instituições policiais.

A PMDF tem utilizado a esse instrumento para promover políticas públicas de segurança que visam a redução da criminalidade e a melhoria da qualidade de vida da população. A integração de sistemas de informação e a análise de grandes volumes de dados permitem uma abordagem mais assertiva na prevenção e combate ao crime. De acordo com o Anuário Brasileiro de Segurança Pública (2023), a aplicação de tecnologias de ponta em segurança pública tem sido

fundamental para a redução dos índices de violência em diversas regiões.

As políticas públicas de segurança em cidades inteligentes devem ser orientadas pela inteligência e integradas a outros setores da administração pública. A Carta Brasileira para Cidades Inteligentes de 2023 enfatiza a importância de um desenvolvimento centrado no cidadão, onde a segurança pública é um componente essencial. A promoção de um ambiente urbano seguro e resiliente depende da capacidade de integrar tecnologias avançadas e práticas de inteligência na gestão pública.

A transformação digital e o desenvolvimento das cidades inteligentes oferecem oportunidades significativas para a melhoria da segurança pública. A utilização da inteligência corrente e do POI pela PMDF demonstra como a integração de tecnologias pode resultar em operações policiais mais eficazes e políticas públicas de segurança mais alinhadas às necessidades da sociedade. A implementação dessas práticas deve continuar a ser uma prioridade para garantir a proteção e o bem-estar da população no Distrito Federal.

2.3.5 AERONAVES REMOTAMENTE PILOTADAS: INSTRUMENTOS PARA SEGURANÇA PÚBLICA

As Aeronaves Remotamente Pilotadas (RPAs), mais conhecidas como drones, desempenham um papel fundamental nas operações de segurança pública, especialmente nas Cidades 4.0, que integram tecnologia e inteligência para melhorar a segurança e o bem-estar dos cidadãos. As RPAs permitem monitoramento em tempo real, coleta de dados e mapeamento de áreas críticas, complementando as atividades tradicionais de policiamento e vigilância (ANAC, 2024).

A Agência Nacional de Aviação Civil (ANAC) regulamenta o uso dessas aeronaves no Brasil, classificando-as de acordo com suas capacidades e finalidades operacionais. As RPAs são categorizadas como aeronaves não tripuladas controladas remotamente por um piloto, com diferentes níveis de autonomia, que variam desde as operações de linha de visada (VLOS) até operações mais complexas além da linha de visada visual (BVLOS) (ANAC, 2024).

A regulamentação de RPAs no Brasil é rígida e visa garantir a segurança pública, além de proteger a privacidade dos cidadãos. O

Departamento de Controle do Espaço Aéreo (DECEA) e o Sistema de Aeronaves Remotamente Pilotadas (SARPAS) são os responsáveis pela concessão de autorizações para voos de drones em áreas controladas e urbanas (DECEA, 2023). A ANAC, por sua vez, estabelece as normas operacionais, permitindo que as RPAs sejam utilizadas em missões de segurança pública, desde que sigam os regulamentos, incluindo limites de altura, peso e locais permitidos (ANAC, 2024).

As RPAs têm sido amplamente adotadas pelas forças policiais em diferentes estados brasileiros, incluindo a Polícia Militar do Distrito Federal (PMDF), que utiliza drones para monitoramento de manifestações públicas, controle de trânsito, patrulhamento de áreas de difícil acesso e apoio em operações contra o crime organizado (Farias, 2021). Esses dispositivos também são empregados em operações táticas, permitindo que a polícia tenha uma visão estratégica de áreas perigosas sem colocar vidas humanas em risco.

Além disso, o uso de drones em atividades de busca e salvamento, especialmente em áreas de desastre natural, tem sido crucial. Eles fornecem imagens em tempo real, ajudam na localização de vítimas e monitoram áreas perigosas que seriam inacessíveis por meios tradicionais (Werneck, 2021).

Apesar dos benefícios evidentes, a implementação de drones nas operações de segurança pública enfrenta desafios operacionais e legais. A principal dificuldade reside na falta de regulamentação específica para certas situações emergenciais e na resistência de alguns setores das forças de segurança em adotar novas tecnologias. Outro desafio é a formação e capacitação de operadores para uso dessas aeronaves de forma eficiente e segura (DECEA, 2023; ANAC, 2024).

Além disso, a privacidade dos cidadãos e a proteção de dados são questões sensíveis que precisam ser abordadas. O uso de drones para vigilância pode gerar preocupações sobre a violação de direitos civis, sendo necessário um marco regulatório claro que garanta o uso ético dessas tecnologias (Prunckun, 2015).

Com a constante evolução tecnológica, o uso de Aeronaves Remotamente Pilotadas (RPAs) se expande rapidamente, especialmente no contexto das Cidades 4.0. Essas cidades, integradas com sistemas de monitoramento em tempo real, utilizam RPAs como parte de um ecossistema mais amplo de segurança pública. Esse

ecossistema inclui câmeras de vigilância, sensores IoT e plataformas de análise de dados em tempo real, o que possibilita a integração eficaz das RPAs em atividades críticas, como gestão de emergências, controle de fronteiras e monitoramento ambiental.

Portanto, as RPAs representam um avanço significativo para a segurança pública, pois permitem monitoramento contínuo e intervenções precisas, facilitando a coleta de dados que podem ser usados em tempo real para decisões operacionais. O DECEA e a ANAC regulamentam o uso seguro dessas aeronaves, promovendo o desenvolvimento de uma infraestrutura legal e técnica robusta para garantir que suas operações não interfiram com a aviação civil ou causem riscos à segurança pública (DECEA, 2020; ANAC, 2019).

A adoção de RPAs em operações cotidianas de segurança pública também pode levar a uma redução significativa de custos operacionais e otimização de recursos humanos, uma vez que as aeronaves podem cobrir grandes áreas de vigilância com menos pessoal envolvido. Essa tecnologia representa um grande passo em direção à modernização das forças de segurança e à criação de uma infraestrutura urbana mais segura e eficiente (SARPAS, 2023).

As Aeronaves Remotamente Pilotadas (RPA), surgiram inicialmente como ferramentas de uso militar, mas ao longo dos anos, sua aplicação se expandiu para várias áreas, incluindo a segurança pública e o policiamento. Nas Cidades 4.0, que integram tecnologias avançadas de dados e conectividade, o uso de drones oferece novas capacidades para as forças de segurança. Dessa forma, busca-se entender como essas aeronaves são utilizadas no contexto da segurança pública, com foco em sua contribuição para a inteligência policial e os desafios enfrentados nesse novo cenário urbano tecnológico. (Sobral; Santos, 2019)

As RPAs têm ganhado destaque em operações de segurança pública, oferecendo aos órgãos policiais uma capacidade de vigilância e monitoramento sem precedentes. Equipadas com câmeras de alta resolução, sensores térmicos e tecnologia de transmissão ao vivo, essas aeronaves permitem o acompanhamento em tempo real de eventos críticos, como manifestações, operações de resgate, e ações contra o crime organizado (DECEA, 2024). Além disso, sua capacidade de alcançar áreas inacessíveis ou perigosas para os agentes em solo faz dos drones ferramentas estratégicas em operações de inteligência.

Nesse cenário, a inteligência corrente, ou seja, a coleta e análise de dados em tempo real, é um dos pilares das operações modernas de segurança pública. As RPAs potencializam essa capacidade, permitindo a captura de imagens e dados que podem ser imediatamente processados pelos centros de comando e controle das forças de segurança. Esses dados podem incluir desde a movimentação de suspeitos até a identificação de objetos ou comportamentos incomuns em grandes eventos (ANAC, 2024).

Essa integração entre drones e inteligência corrente é essencial nas Cidades 4.0, onde a quantidade de informações geradas por dispositivos conectados requer uma análise rápida e eficaz. A possibilidade de utilizar drones para coletar e transmitir dados instantaneamente permite às forças de segurança uma vantagem estratégica, pois permite que ações sejam coordenadas de maneira mais eficiente e precisa (Werneck, 2021).

Embora as RPAs ofereçam muitas vantagens operacionais, seu uso também apresenta desafios. Em termos de regulamentação, a ANAC e o DECEA estabelecem normas rigorosas para a operação dessas aeronaves, incluindo requisitos de licenciamento, delimitação de zonas de voo, e controle do tráfego aéreo (DECEA, 2024). O Sistema de Solicitação de Acesso ao Espaço Aéreo por RPAS (SARPAS) foi criado para simplificar e regulamentar o uso do espaço aéreo pelas RPAs de forma segura e eficiente.

À medida que as Cidades 4.0 evoluem, espera-se a expansão das RPAs nas operações de inteligência policial. As tecnologias emergentes, como a IA e o aprendizado de máquina, podem ser integradas aos drones para melhorar a análise de dados em tempo real, aumentando a capacidade das forças de segurança de prever e prevenir crimes (Sarte, 2024).

Os drones não serão apenas ferramentas de vigilância, mas também plataformas móveis para a coleta de grandes volumes de dados, que serão processados por sistemas inteligentes para gerar *insights* sobre padrões criminais e potenciais ameaças à segurança pública. O uso de RPAs com IA poderá, por exemplo, identificar automaticamente comportamentos suspeitos ou rastrear veículos em tempo real, otimizando ainda mais as operações de inteligência. (DECEA, 2015)

Dessa forma, as RPAs estão se consolidando como instrumentos essenciais para as operações de segurança pública nas cidades inteligentes. A sua capacidade de coleta e análise de dados em tempo real também fortalece a inteligência corrente, permitindo uma resposta mais rápida e eficiente às ameaças à segurança. No entanto, a expansão de seu uso traz desafios, especialmente em termos de regulamentação e privacidade, que precisam ser cuidadosamente gerenciados pelas autoridades. O futuro aponta para uma maior integração dessas aeronaves com tecnologias avançadas, tornando-as ferramentas indispensáveis para a manutenção da segurança nas Cidades 4.0.

Em virtude da constante evolução tecnológica, o uso de RPAs (Aeronaves Remotamente Pilotadas) está se expandindo, especialmente no contexto das Cidades 4.0. Essas cidades, integradas com sistemas de monitoramento em tempo real, utilizam essas aeronaves como parte de um ecossistema mais amplo de segurança pública, que inclui câmeras de vigilância, sensores IoT e plataformas de análise de dados em tempo real. As RPAs estão sendo implementadas em diversas áreas da segurança pública, como gestão de emergências, controle de fronteiras e monitoramento ambiental (Costa; Reis Filho, 2019).

A inteligência corrente envolve a coleta e análise contínua de informações para fornecer dados precisos e oportunos às autoridades, permitindo decisões estratégicas rápidas. Nesse contexto, as RPAs desempenham um papel essencial, proporcionando visibilidade em tempo real de locais e situações que poderiam ser inacessíveis ou perigosos para humanos (Klauser, 2021). Um exemplo de uso bem-sucedido de RPAs foi identificado por Klauser (2021), ao analisar o impacto dos drones no policiamento na Suíça, onde se observa a criação de uma nova "geopolítica volumétrica", transformando a maneira como as autoridades de segurança lidam com o espaço aéreo urbano.

As RPAs proporcionam uma série de vantagens à segurança pública, especialmente nas Cidades 4.0. Essas aeronaves conseguem cobrir áreas urbanas e rurais de forma rápida e eficiente, podendo ser empregadas em operações de busca e resgate, vigilância contínua e controle de áreas de risco. Costa (2019) enfatiza que o uso de drones em operações de segurança pública tem se mostrado uma ferramenta eficaz em situações de emergência, auxiliando na detecção de

incidentes climáticos extremos e no monitoramento de atividades criminosas. Além disso, Reis Filho (2019) destaca que as RPAs são particularmente úteis em operações noturnas, quando as condições de visibilidade para as forças terrestres são limitadas.

Embora as RPAs ofereçam inúmeras vantagens, sua utilização também traz desafios relacionados à segurança do espaço aéreo e à privacidade. No Brasil, o DECEA e a ANAC têm implementado regulamentações rigorosas para o uso de drones, estabelecendo parâmetros para sua operação segura. A plataforma SARPAS, desenvolvida pelo DECEA, permite que operadores de drones solicitem autorização para voos em áreas controladas, garantindo que os RPAs não entrem em conflito com aeronaves tripuladas. Segundo Reis Filho (2019), a regulamentação clara e atualizada é fundamental para garantir que o uso de drones continue crescendo de maneira segura e eficiente.

Nas Cidades 4.0, as RPAs são integradas a sistemas de vigilância mais amplos, que incluem câmeras de segurança e sensores IoT, criando um ecossistema completo de monitoramento. Essa integração tecnológica, segundo Klauser (2021), permite que as forças de segurança coletem, processem e analisem dados em tempo real, aprimorando sua capacidade de prevenir crimes e mitigar riscos antes que se tornem ameaças maiores. Costa (2019) complementa que essa abordagem de segurança pública integrada, utilizando drones e outros dispositivos tecnológicos, está transformando a maneira como as cidades gerenciam crises e eventos inesperados.

As Aeronaves Remotamente Pilotadas estão se tornando uma ferramenta indispensável para a inteligência corrente e a segurança pública nas cidades inteligentes. Sua capacidade de monitoramento em tempo real, aliada à sua flexibilidade de uso e baixo custo operacional, está redefinindo a maneira como as autoridades lidam com questões de segurança. No entanto, para que as RPAs sejam utilizadas de forma eficaz e segura, é essencial que haja uma regulamentação robusta, garantindo que sua implementação respeite os limites de privacidade e segurança aérea (Reis Filho; Costa, 2019; Klauser, 2021). Assim, as RPAs continuarão desempenhando um papel crucial no futuro das cidades da quarta revolução industrial, contribuindo para a criação de ambientes urbanos mais seguros e resilientes.

A constante evolução dos crimes violentos contra o patrimônio demanda a utilização de tecnologias avançadas para melhorar a eficiência das operações de segurança pública. Um exemplo notável é o uso de aeronaves remotamente pilotadas (RPAs), que têm sido aplicadas pela Polícia Militar do Paraná no combate a crimes violentos, como o "novo cangaço". O estudo de Marty (2022) demonstra que o uso das RPAs proporciona resultados significativos tanto no policiamento ostensivo quanto nas operações de inteligência.

Essas aeronaves desempenham um papel crucial ao aumentar a capacidade de monitoramento aéreo em tempo real, o que permite às forças policiais antecipar e responder rapidamente a incidentes. De acordo com Marty (2022), as RPAs facilitam o recobrimento das ações policiais com uma tecnologia inovadora, que permite ganhos operacionais substanciais, particularmente no combate a crimes violentos contra instituições financeiras.

As RPAs também se destacam pela capacidade de monitorar grandes áreas com sensores térmicos e câmeras de alta resolução, ferramentas essenciais no enfrentamento de grupos criminosos organizados, que utilizam técnicas sofisticadas para desviar a ação policial. Com o uso de RPAs, os agentes podem rastrear criminosos em áreas de difícil acesso, como florestas e zonas rurais, otimizando o emprego de efetivos e assegurando a integridade dos envolvidos.

Além disso, as RPAs têm mostrado potencial na produção de informações críticas em missões de inteligência, auxiliando na coleta de dados para operações futuras e prevenindo crimes antes de sua ocorrência. Marty (2022) também sugere que o uso de equipamentos mais modernos, com maior autonomia de voo e capacidade de detecção, pode ampliar ainda mais a eficácia dessas operações.

O uso de drones pela a Polícia Militar de Minas Gerais (PMMG) também é destacado no estudo conduzido por Silva (2018), que detalhou as operações antidrogas em áreas urbanas complexas e de difícil acesso. Nesse diapasão, a PMMG foi pioneira na implementação de Aeronaves Remotamente Pilotadas (RPAs) para reforçar as operações de segurança pública, particularmente no combate ao tráfico de drogas. Esse autor evidencia como a tecnologia pode transformar a maneira como as forças de segurança conduzem suas operações.

Segundo Silva, 2018, esses dispositivos foram empregados para:

1. Coleta de Imagens Aéreas: As RPAs captaram imagens detalhadas de áreas sob investigação, permitindo o mapeamento de rotas de fuga, identificação de esconderijos e monitoramento de movimentações suspeitas em tempo real.

2. Produção de Inteligência: As imagens coletadas foram analisadas por equipes de inteligência para produzir relatórios estratégicos, agregando dados como localização de pontos de venda de drogas, veículos suspeitos e modus operandi dos envolvidos.

3. Apoio em Operações Táticas: Durante as incursões em aglomerados urbanos, os drones auxiliaram na vigilância das áreas periféricas e na antecipação de ameaças, reduzindo a exposição dos policiais em campo.

Com relação aos impactos operacionais segundo o autor supramencionado, a aplicação de RPAs pela PMMG trouxe benefícios operacionais como:

1. **A Segurança das Equipes: os drones permitiram a visualização antecipada do cenário de atuação, identificando possíveis ameaças antes da abordagem e reduziu-se significativamente o risco de emboscadas e confrontos diretos em zonas de alta criminalidade;**
2. **Precisão nas Ações: as informações aéreas permitiram intervenções pontuais e assertivas, com base na análise precisa das movimentações criminosas;**
3. **Otimização de Recursos: os drones substituíram, em diversas situações, o uso de helicópteros, reduzindo os custos operacionais sem comprometer a eficácia;**
4. **Resultados Concretos: no estudo documentado por Silva (2018), houve aumento no número de apreensões de drogas e prisões de suspeitos devido ao uso de informações fornecidas pelas RPAs.**

Uma operação específica relatada nesse estudo, uma operação antidrogas, envolveu o uso de drones para monitorar um aglomerado urbano conhecido por abrigar atividades ilícitas. Durante o planejamento, os drones mapearam rotas de entrada e saída utilizadas pelos traficantes, além de esconderijos em áreas de difícil acesso. As imagens coletadas permitiram que a equipe planejasse uma incursão tática, resultando na apreensão de entorpecentes e prisão de membros de uma organização criminosa, sem riscos adicionais para os policiais.

Apesar dos resultados positivos, o estudo feito por Silva (2018) também destacou alguns desafios, como a capacitação dos Operadores de RPAs, sendo necessário o recrudescimento de treinamento especializado para manusear e operar RPAs eficazmente. Foi constatado ainda, a Interoperabilidade com Sistemas de Inteligência, pois a integração das imagens e dados coletados aos sistemas existentes ainda requer melhorias além de Regulamentação, por causa das restrições impostas pela ANAC e pelo DECEA, especialmente em áreas urbanas densas.

Portanto, o estudo realizado por Silva (2018) no contexto da PMMG fundamenta a afirmação de que o uso de drones aumenta a precisão e a segurança em operações policiais.

Assim, a integração das RPAs no combate aos crimes violentos contra o patrimônio, contra o tráfico de drogas e nas missões acima mencionadas representa um avanço significativo para a segurança pública, otimizando o tempo de resposta das forças policiais e reduzindo as estatísticas de crimes violentos em áreas vulneráveis.


3

3 DESENHO DA PESQUISA

Esse trabalho, salienta a inteligência na segurança pública em Cidades 4.0, e neste momento, pretende-se incluir a análise dos dados qualitativos coletados através de revisão bibliográfica e análise documental, ou seja, a apresentação dos dados coletados e a descrição detalhada dos resultados obtidos através das metodologias de pesquisa aplicadas.

3.1 ESTUDOS ACADÊMICOS DE REFERÊNCIA

Ao longo da pesquisa, várias fontes acadêmicas, normativas e estudos de caso foram analisados, com foco em inteligência, segurança pública, policiamento, cidades inteligentes e o uso de RPAs. Esses temas, embora distintos, estão profundamente interligados e convergem para um objetivo comum: aprimorar a capacidade das instituições de segurança pública de enfrentar os desafios contemporâneos através da inteligência, especialmente no contexto das Cidades 4.0, utilizando tecnologias emergentes.

Nesse ínterim, diversas leis, decretos, projetos de lei e resoluções foram examinados, buscando-se compreender o arcabouço legal que orienta as atividades de inteligência, segurança pública e o uso de novas tecnologias no Brasil. Essa investigação legislativa foi motivada pela necessidade de consolidar o entendimento sobre como o ordenamento jurídico brasileiro tem acompanhado as transformações tecnológicas e os desafios de segurança, sobretudo no contexto das cidades inteligentes e das práticas de inteligência no combate à criminalidade organizada. Foram analisadas normativas específicas que cobrem áreas-chave da segurança pública, desde a atuação das polícias até o uso de sistemas de inteligência, conforme exposto no quadro acima.

As escolhas legislativas refletem a relevância de normas complementares que oferecem bases sólidas para a atuação das instituições de segurança pública, com destaque para três principais temas: a) as disposições constitucionais e penais que estruturam o papel da polícia e da repressão criminal; b) os sistemas de inteligência, regulados por leis e resoluções, que orientam a coleta, análise e uso de

dados no combate ao crime; e c) os projetos de lei que visam modernizar a legislação frente ao avanço do crime organizado e ao uso de novas tecnologias.

De forma adicional, os dispositivos legais ora mencionados são fundamentais para a construção de um sistema de segurança pública eficiente, que se utiliza de inteligência de forma integrada e respeita os direitos constitucionais, assegurando, assim, a ordem social e a proteção dos direitos fundamentais. Essas legislações também apontam para a importância da atuação coordenada entre diferentes órgãos de segurança, bem como para a necessidade de adaptação da legislação às realidades digitais e urbanas contemporâneas, como no caso das Cidades 4.0. Ao compilar e analisar esses marcos legais, a presente pesquisa busca contribuir para o entendimento de como a legislação pode amparar práticas inovadoras e eficazes de segurança pública no Brasil.

Esses dispositivos legais consolidam conceitos essenciais para o avanço da segurança pública no Brasil e para a aplicação da inteligência em um contexto de crescente urbanização e complexidade social, reforçando o papel do Estado na garantia de proteção e ordem em um cenário de cidades conectadas e tecnologicamente avançadas.

3.2 OBJETO DA PESQUISA

O objetivo geral desta dissertação é investigar como a inteligência corrente pode ser usada para melhorar a segurança pública no contexto das cidades inteligentes, explorando como a integração de tecnologias como RPAs e ferramentas de *big data* pode otimizar as operações policiais e a proteção da sociedade.

Quadro 3 – Objetivos Específicos
Os objetivos específicos incluem:
1. Avaliar a aplicação da inteligência nas operações policiais e sua contribuição para a eficiência da segurança pública;
2. Explorar o uso de tecnologias como ferramentas estratégicas no monitoramento e controle de áreas urbanas complexas;

3. Analisar a adaptação das políticas públicas às Cidades 4.0 e identificar as aplicações práticas da inteligência nas operações da Polícia no contexto das Cidades 4.0;
4. Explorar os principais desafios enfrentados pela Segurança Pública no uso da inteligência para lidar com a complexidade das Cidades 4.0 e propor soluções para superá-los, identificando as implicações do uso de dados em tempo real;

Fonte: Elaboração própria (2024)

Gráfico 2 – Integração entre inteligência, segurança pública, operações policiais e tecnologias emergentes

Fonte: Elaboração própria (2024)

Este gráfico acima demonstra a convergência entre inteligência, segurança pública e as tecnologias emergentes (RPAs). A inteligência corrente (uma ferramenta da Inteligência), no centro, coordena o uso de dados e tecnologias avançadas para otimizar as operações policiais e a segurança urbana, especialmente no contexto das cidades inteligentes.

Quadro 4 – Objetivos Específicos e Tecnologias Correspondentes		
Objetivo Específico	**Tecnologia Correlacionada**	**Resultados Esperados**
Avaliar a aplicação da inteligência corrente em operações policiais	Big Data, IA	Otimização da alocação de recursos policiais, maior precisão nas operações.
Explorar o uso de tecnologias emergentes para monitoramento e controle urbano	RPAs e Sensores Inteligentes	Melhoria no monitoramento de grandes áreas urbanas e zonas de difícil acesso, aumento da eficiência operacional.
Analisar a adaptação das políticas públicas às Cidades 4.0	Ferramentas de Governança Inteligente	Integração das tecnologias emergentes nas estratégias de segurança pública, legislação mais adaptada.
Identificar as implicações do uso de dados em tempo real	Big Data e Analytics	Melhor tomada de decisões, prevenção mais eficaz de incidentes e crimes em tempo real.

Fonte: Elaboração própria (2024)

Os quadros e gráfico demonstram como os elementos abordados na pesquisa, desde a inteligência até o uso de RPAs, se conectam ao contexto de Cidades 4.0, possibilitando um aprimoramento significativo das operações policiais. O uso dessas tecnologias, quando combinado com a coleta e análise de dados em tempo real, permite que as forças de segurança pública atuem de maneira mais eficaz, promovendo uma resposta mais rápida e precisa às ameaças e garantindo a segurança dos cidadãos.

Essa abordagem inovadora evidencia a importância da adaptação das políticas públicas ao avanço tecnológico e reforça o papel central da inteligência como um instrumento de transformação da segurança pública no Brasil.

Quadro 5 – Relação entre Tecnologias e Benefícios Operacionais na Segurança Pública		
Tecnologia	**Benefícios**	**Desafios**
Câmeras de Vigilância	Monitoramento constante de áreas urbanas	Proteção de privacidade
RPAs (Drones)	Monitoramento aéreo de áreas difíceis, aumento da segurança	Capacitação e regulamentação tecnológica
Big Data e IA	Análise preditiva de ameaças e planejamento de operações policiais	Integração entre diferentes agências de segurança
Sensores Inteligentes	Coleta de dados em tempo real para a tomada de decisões rápidas	Necessidade de manutenção e custo elevado

Fonte: Elaboração própria (2024)

A presente dissertação oferece **contribuições significativas para novos estudos acadêmicos** ao analisar criticamente o uso da **inteligência corrente** nas **operações de segurança pública** no contexto das **Cidades 4.0**. A pesquisa destaca a necessidade de integrar tecnologias emergentes com as operações tradicionais de segurança, explorando como o uso de dados em tempo real e ferramentas avançadas pode **aumentar a eficácia do policiamento**. Além disso, a dissertação identifica lacunas importantes, como a **falta de regulamentação e capacitação** no uso de tecnologias como RPAs, sugerindo que essas áreas precisam ser mais bem exploradas para garantir que as forças policiais estejam preparadas para os desafios futuros.

A pesquisa também contribui para o desenvolvimento de **políticas públicas** mais eficazes, sugerindo que a adaptação às tecnologias emergentes é essencial para melhorar a segurança pública. A **inteligência corrente**, com seu potencial de transformar dados em informações estratégicas, oferece um caminho promissor para que as cidades possam lidar com a **complexidade urbana** e os **novos riscos associados à criminalidade.**

Este trabalho, portanto, serve como **auxiliar futuros estudos acadêmicos**, abrindo espaço para novas discussões sobre o **uso da**

tecnologia na segurança pública e a **necessidade de aprimorar a governança nas Cidades 4.0.**

3.3 METODOLOGIA

Este tópico tem como objetivo detalhar o percurso metodológico adotado para a realização da pesquisa, desde revisão bibliográfica até a análise documental e a aplicação de métodos qualitativos. A pesquisa visou investigar o uso de tecnologias emergentes, na inteligência, no contexto da segurança pública nas Cidades 4.0. Foram exploradas as implicações dessas tecnologias na melhoria da eficiência das operações policiais e na capacidade de resposta a desafios contemporâneos.

Além de expor o processo metodológico, aborda-se os principais desafios encontrados durante a pesquisa, como a coleta de dados dispersos, a dificuldade de integração tecnológica entre diferentes sistemas, e o tratamento ético de informações sensíveis, especialmente no campo da segurança pública.

A revisão bibliográfica foi fundamental para a construção do referencial teórico que sustentou a pesquisa. Ela se concentrou em três grandes áreas: inteligência, segurança pública e tecnologias emergentes aplicadas às Cidades 4.0. A pesquisa bibliográfica envolveu uma análise extensa de artigos científicos, dissertações, livros e relatórios técnicos, com o objetivo de traçar um panorama das abordagens contemporâneas sobre o uso de tecnologias na segurança pública.

Os principais autores estudados, como Marco Cepik (espionagem e inteligência no Brasil), Manuel Castells (sociedade em rede), e Caragliu, Del Bo e Nijkamp (cidades inteligentes na Europa), dentre outros, forneceram uma base sólida para entender o impacto das tecnologias digitais no policiamento e na governança urbana. Além disso, documentos institucionais, como relatórios da ONU sobre violência e estudos sobre segurança urbana em países em desenvolvimento, ajudaram a contextualizar a pesquisa no cenário internacional.

Quadro 6 – Ordem da estrutura da revisão bibliográfica	
1. Inteligência Corrente e Segurança Pública	O objetivo foi definido na literatura sobre a aplicação de inteligência no combate ao crime e nas operações policiais.
2. Cidades Inteligentes	A análise foi direcionada aos avanços tecnológicos nas Cidades 4.0 e o impacto dessas inovações na segurança pública.
3. Tecnologias Emergentes	Perscrutou-se o uso de big data, RPAs, e IA, e como essas tecnologias estão sendo implementadas na segurança pública.

Fonte: Elaboração própria (2024)

A revisão bibliográfica também revelou lacunas, principalmente em relação à integração dessas tecnologias em um sistema de segurança pública coeso. Muitos estudos exploraram o uso de *big data* e IA, mas poucos focaram na coordenação entre tecnologias, como RPAs e sensores inteligentes, e sua regulamentação em cidades altamente urbanizadas.

Quadro 7 – As quatro fases principais do processo de pesquisa - estrutura		
Objetivo Específico	**Tecnologia Correlacionada**	**Resultados Esperados**
Fase 1:	Levantamento Teórico e Construção do Referencial	A primeira fase consistiu na revisão da literatura e na seleção de textos, artigos e documentos técnicos. Nessa etapa, foram coletadas informações de fontes acadêmicas e institucionais sobre o uso de inteligência corrente e tecnologias emergentes aplicadas à segurança pública. A construção do referencial teórico envolveu a categorização dos temas em três frentes principais: inteligência aplicada, segurança pública e Cidades 4.0.
Fase 2:	Análise Documental	A análise documental envolveu a consulta a relatórios governamentais sobre o uso de tecnologias de monitoramento em segurança pública, além de documentos técnicos que regulamentam a utilização de RPAs e big data. Entre os documentos analisados, destacam-se os relatórios do Ministério da Justiça sobre o uso de

		RPAs nas operações policiais e os dados do Atlas da Violência sobre a evolução da criminalidade no Brasil. A análise documental foi conduzida utilizando-se métodos de categorização temática, onde os documentos foram organizados em grupos, de acordo com os temas centrais: legislação, operação e implementação tecnológica.
Fase 3:	Coleta de Dados Qualitativos	Nesta fase, foram realizadas buscas na literatura e documentos oficiais da área de segurança pública, com foco em segurança pública e tecnologia emergentes. A coleta de dados qualitativos envolveu o levantamento sobre o uso de RPAs na polícia em grandes centros urbanos e o impacto da inteligência corrente nas operações de campo.
Fase 4:	Análise dos Resultados e Integração Tecnológica	A última fase consistiu na análise e interpretação dos resultados, com base na interligação das tecnologias emergentes estudadas. Foi criada uma estrutura analítica que permitiu integrar os dados coletados, mostrando como cada tecnologia contribui para a melhoria das operações de segurança pública nas cidades inteligentes. A integração das tecnologias foi analisada por meio de ferramentas analíticas, como a nuvem de palavras e gráficos comparativos de evolução tecnológica.

Fonte: Elaboração própria (2024)

A análise documental foi uma das etapas fundamentais desta pesquisa, desempenhando um papel crucial na compreensão do contexto e das implicações do uso de tecnologias emergentes na segurança pública, especialmente no âmbito das Cidades 4.0. O método consistiu na revisão e análise de documentos oficiais, como relatórios, legislações, políticas públicas, e estudos institucionais de segurança, bem como de regulamentos técnicos relacionados ao uso de drones, RPAs, *big data* e inteligência corrente. Os objetivos da análise documental estão descritos abaixo como:

Quadro 8 – Objetivos da análise documental	
Objetivos	Identificar a regulamentação existente sobre o uso de tecnologias emergentes em segurança pública.
	Analisar a implementação de políticas públicas que regem a adoção dessas tecnologias nas operações policiais, com foco em documentos de órgãos como o Ministério da Justiça, Secretarias de Segurança Pública e relatórios nacionais e internacionais.
	Compreender os desafios e oportunidades expressos em relatórios técnicos e estudos sobre a integração de tecnologias emergentes no contexto de cidades urbanizadas e densamente povoadas.
	Explorar a adoção de legislações específicas sobre o uso de tecnologias como RPAs e drones em operações de segurança, levando em consideração a privacidade dos cidadãos e o controle do espaço aéreo.

Fonte: Elaboração própria (2024)

A metodologia aplicada na análise documental seguiu as etapas de coleta, categorização e análise qualitativa. Na coleta de documentos, estes foram extraídos coletados a partir de diversas fontes institucionais, incluindo:

Quadro 9 – Documentos extraídos	
Documentos coletados	Relatórios anuais do Ministério da Justiça sobre a evolução das tecnologias de segurança pública;
	Estudos técnicos sobre a aplicação de drones e RPAs no Brasil, com dados de instituições como a ABIN e Secretarias Estaduais de Segurança Pública;
	Relatórios legislativos que incluem leis, decretos e resoluções, como a Lei nº 9.883 de 1999, que criou o Sistema Brasileiro de Inteligência (SISBIN), e o Projeto de Lei nº 2.310 de 2022, que regulamenta as ações de inteligência;
	Documentos internacionais de referência sobre cidades inteligentes e o impacto das tecnologias emergentes no policiamento, incluindo relatórios da ONU e do Banco Interamericano de Desenvolvimento (BID);

Fonte: Elaboração própria (2024)

Na sequência, através da categorização, os documentos foram classificados em três grandes partes:

Quadro 10 – Categorização dos documentos	
1. Legislação e Regulamentação	Incluiu a análise de leis e resoluções sobre a regulamentação de tecnologias na segurança pública, como o uso de drones e RPAs. A partir dessa categorização, foi possível identificar os principais desafios relacionados à implementação dessas tecnologias e a necessidade de atualização legal, especialmente em relação à privacidade e à segurança no espaço aéreo.
2. Políticas Públicas e Relatórios Técnicos	Essa categoria abrangeu a análise de documentos governamentais e institucionais que tratam das políticas de segurança pública e da aplicação de inteligência corrente, big data e análise preditiva nas operações policiais. Foram exploradas as barreiras institucionais para a adoção dessas tecnologias, bem como os avanços já observados em algumas cidades.
3. Estudos de Caso e Relatórios Operacionais	Documentos de estudos de caso sobre o uso de tecnologias emergentes em segurança pública, tanto no Brasil quanto em outros países. Essa análise permitiu comparar as práticas adotadas em diferentes contextos urbanos e verificar como tecnologias como RPAs e big data estão sendo implementadas em outras cidades inteligentes ao redor do mundo.

Fonte: Elaboração própria (2024)

Após a coleta e categorização dos documentos, foi realizada uma análise qualitativa. Isso envolveu a leitura e interpretação detalhada dos documentos, identificando padrões, diretrizes e lacunas no uso de tecnologias emergentes. Foram destacadas as principais barreiras institucionais e legais para a implementação de drones, RPAs e *big data*, além da análise do impacto dessas tecnologias no cotidiano das operações de segurança pública.

A análise qualitativa buscou entender como a legislação vigente se posiciona em relação ao uso de tecnologias de monitoramento e coleta de dados em tempo real, identificando pontos de convergência e desafios relacionados à governança tecnológica. Esse tipo de análise permitiu não apenas mapear o que já está regulamentado, mas também apontar áreas onde ainda existem lacunas, como a

regulamentação do uso de drones em áreas densamente povoadas e o armazenamento de dados obtidos por *big data*.

Os principais achados obtidos por meio da análise documental foram os seguintes:

Quadro 11 – Achados através da análise documental	
Regulamentação incipiente	Embora algumas legislações, como a Lei nº 9.883 de 1999, tenham criado sistemas de inteligência como o SISBIN, ainda há uma lacuna significativa na regulamentação do uso de tecnologias emergentes em segurança pública, especialmente drones e RPAs. O Projeto de Lei nº 2.310 de 2022 é um avanço nesse sentido, mas ainda precisa ser consolidado.
Políticas públicas desatualizadas	A pesquisa documental mostrou que, em muitos estados, as políticas públicas de segurança ainda não contemplam plenamente o uso de big data e análise preditiva. Esses dados são essenciais para uma atuação policial mais eficaz em Cidades 4.0, onde a complexidade urbana exige respostas rápidas e inteligentes.
Integração tecnológica limitada	Outro achado importante foi a constatação de que as tecnologias de inteligência corrente, RPAs, drones e big data ainda não estão totalmente integradas. Os relatórios operacionais revelaram que a maioria das cidades ainda implementa essas ferramentas de maneira fragmentada, o que dificulta o pleno aproveitamento de seu potencial.
Privacidade e governança de dados	O uso de tecnologias de monitoramento em cidades inteligentes levanta preocupações com privacidade e proteção de dados. Documentos internacionais destacaram a importância de garantir que as informações coletadas sejam utilizadas de forma ética, e as leis de proteção de dados precisam ser fortalecidas para acompanhar o crescimento do uso de big data e análise preditiva.

Fonte: Elaboração própria (2024)

A análise documental desempenhou um papel central ao fornecer um entendimento profundo sobre as barreiras institucionais e legais que impactam a implementação de tecnologias emergentes nas operações de segurança pública. Embora a adoção de tecnologias como RPAs (drones), *big data* aliadas à inteligência corrente esteja em expansão, ainda há desafios consideráveis relacionados à regulamentação, integração tecnológica e proteção de dados.

Este trabalho revelou que, para que essas tecnologias sejam efetivamente integradas no contexto das Cidades 4.0, é essencial que haja uma revisão das políticas públicas e atualizações legislativas. A análise documental contribuiu para a identificação dessas lacunas e para a proposta de caminhos que possam melhorar a governança dessas tecnologias nos próximos anos.

Esses achados são fundamentais para informar a elaboração de políticas mais robustas, permitindo que as Cidades 4.0 sejam seguras e inteligentes, garantindo tanto a eficiência nas operações de segurança pública quanto a proteção dos direitos fundamentais dos cidadãos.

Dessa forma, o objeto desta pesquisa foi o uso de inteligência corrente e tecnologias emergentes (RPAs (drones), *big data* e sensores inteligentes) nas operações de segurança pública em Cidades 4.0. O estudo focou em entender como essas tecnologias podem ser integradas para otimizar as operações policiais, melhorar o monitoramento urbano e reduzir o tempo de resposta a incidentes. A pesquisa também investigou as barreiras tecnológicas e regulatórias encontradas na implementação dessas ferramentas em grandes centros urbanos.

A implementação de tecnologias como RPAs foi um dos principais focos, devido ao seu potencial de monitoramento aéreo em áreas de difícil acesso e de auxílio em operações policiais complexas. Além disso, a utilização de *big data* foi investigada no contexto de análise preditiva e tomada de decisões estratégicas em tempo real.

3.4 COLETA DE DADOS

3.4.1 NUVEM DE PALAVRAS: ANÁLISE DE FREQUÊNCIA

A nuvem de palavras é uma ferramenta importante na análise qualitativa de dados. Ela permite visualizar termos relevantes em grandes volumes de texto de forma acessível e compreensível. Ao aumentar o destaque das palavras mais recorrentes, seja por meio de tamanho ou cor, a nuvem facilita a comunicação dos resultados da pesquisa e reforça a interpretação dos achados. Isso torna as informações complexas mais acessíveis a diferentes públicos, incluindo gestores de segurança pública e tomadores de decisão.

Para esta pesquisa, foi utilizado arquivos de texto no formato Word contendo dados extraídos de relatórios de segurança pública e literatura sobre o uso de tecnologias emergentes. O arquivo, representando dados atuais, reflete os desafios iniciais da implementação de drones e RPAs em grandes cidades. Assim como, captura o impacto mais amadurecido dessas tecnologias e sua integração nas operações policiais diárias.

A criação das nuvens de palavras foi feita por meio do site http://www.wordcloud.com. A ferramenta permitiu o upload dos arquivos de texto, onde ajustou-se as configurações visuais, como fontes, cores e formas, para destacar as palavras mais frequentes de maneira clara e atraente. Como parte do processo, eliminamos termos de pouca relevância, como “que” e “de”, para garantir que as palavras mais importantes fossem enfatizadas.

Após a configuração das preferências, foram geradas nuvens de palavras: salvas como imagens no formato PNG. A seguir, é apresentada a figura que representa os termos mais recorrentes no período, permitindo uma visão clara sobre como o uso das tecnologias emergentes evolui ao longo do tempo.

A análise de frequência foi conduzida por meio da criação de uma nuvem de palavras que identificou os termos mais recorrentes nas entrevistas e documentos analisados. As palavras mais frequentes incluíram: inteligência, segurança, cidades, polícia, monitoramento, desafios, RPAs, drones, segurança pública, operações, análise e tecnologia.

Com o intuito de destacar as descobertas e percepções mais significativas desta pesquisa, foi gerada nuvem de palavras que representa visualmente os termos mais frequentes no conjunto de dados analisados. Este método foi escolhido para facilitar a identificação rápida dos principais temas abordados nos textos, permitindo *insights* valiosos sobre o uso de tecnologias emergentes, com inteligência corrente, drones, RPAs e *big data* na segurança pública, particularmente no contexto das Cidades 4.0.

Figura 4 – Nuvem de palavras

Fonte: site: http://www.wordcloud.com, 2024.

A visualização acima destaca as palavras mais frequentes encontradas nos documentos e artigos, representando os principais temas discutidos no contexto das tecnologias emergentes aplicadas à segurança pública.

As nuvens de palavras revelam achados importantes da pesquisa. Em um primeiro momento, os termos mais proeminentes incluem segurança, pública, Cidades, dados, tecnologias, refletindo o foco inicial nas tecnologias emergentes para aumentar a capacidade de vigilância das forças policiais. A palavra inteligência também aparece com destaque, indicando a crescente importância da inteligência corrente nas operações de segurança.

Em um segundo momento, observa-se um aumento na frequência de termos como tecnologias, operação e análise preditiva, sinalizando uma evolução significativa no uso dessas tecnologias para previsão de crimes e tomada de decisões estratégicas. Além disso, termos relacionados ao impacto dessas tecnologias no ambiente urbano, como Cidades 4.0 e inovação, também surgem com relevância, refletindo a incorporação mais madura das ferramentas digitais nas operações diárias.

Além das nuvens de palavras, foi realizada uma análise de incidência de palavras, comparando os termos mais mencionados entre as tecnologias estudadas. O quadro a seguir detalha a evolução no uso de termos-chave, evidenciando o aumento da importância de certas tecnologias e conceitos.

Tabela 2 – Nuvem – palavras principais

2500 palavras	
Peso	**Palavra**
395	segurança
345	inteligência
299	pública
194	Cidades
114	dados
104	uso
102	Tecnologias
97	sobre
93	Análise
93	operações
86	inteligentes

Fonte: Elaboração própria (2024)

Os dados apresentados mostram um aumento significativo no uso de tecnologias como *big data* e inteligência corrente em nos últimos anos, evidenciando a transição de um foco inicial em monitoramento e vigilância para uma integração mais profunda de

análises preditivas e inteligência de dados nas operações de segurança pública. Este crescimento reforça a tese de que, à medida que as tecnologias evoluem, a sua aplicação nas Cidades 4.0 torna-se cada vez mais complexa e integrada, permitindo respostas mais eficazes às ameaças contemporâneas.

Esse tipo de análise reforça uma percepção valiosa obtidos ao longo da pesquisa, permitindo uma visão mais clara das tendências e desafios que surgiram com a implementação das tecnologias emergentes no contexto da segurança pública urbana.


4

4 RESULTADOS E ANÁLISES

Este capítulo apresenta os resultados obtidos a partir da análise qualitativa dos dados documentais e da literatura revisada. Serão detalhadas as implicações das tecnologias emergentes, como drones, big data e sensores inteligentes, no aprimoramento das operações de segurança pública.

Quadro 12 – Categorias dos principais resultados			
Tecnologia e Operações Policiais	A aplicação de drones e RPAs aumentou a capacidade de monitoramento aéreo, especialmente em áreas urbanas complexas e de difícil acesso. Os estudos indicaram que a integração dessas tecnologias nas operações de segurança pública permitiu ações mais precisas e intervenções preventivas, minimizando riscos e otimizando os recursos disponíveis.	**Localização e fundamentação da afirmação no texto (Capítulo 2 - Revisão Bibliográfica):**	**A análise documental e os casos práticos confirmam a eficácia das RPAs na segurança pública. Os drones aumentaram significativamente a capacidade operacional das forças policiais, particularmente nas seguintes dimensões:**
		- Monitoramento em tempo real e coleta de dados:	**1. Monitoramento em Áreas Urbanas Complexas:**

		" coleta de dados e mapeamento de áreas críticas, complementando as atividades tradicionais de policiamento e vigilância" (ANAC, 2024).	Na PMDF, os drones foram utilizados para monitorar manifestações e áreas de alta criminalidade, permitindo a redistribuição estratégica das forças e otimizando os recursos humanos disponíveis (Farias, 2021).
		- Integração em operações táticas: "As RPAs têm sido amplamente adotadas pelas forças policiais, incluindo a Polícia Militar do Distrito Federal (PMDF), que utiliza drones para monitoramento de manifestações públicas, controle de trânsito, patrulhamento de áreas de difícil acesso e apoio em operações contra o crime organizado" (Farias, 2021).	**2. Operações em Áreas de Difícil Acesso:** No contexto das operações antidrogas da PMMG, os drones foram empregados para mapear esconderijos e rotas de fuga, garantindo intervenções mais precisas e reduzindo o risco para os agentes de segurança (Silva, 2018).
		- Precisão e redução de riscos: " A possibilidade de utilizar drones para coletar e transmitir dados instantaneamente permite às forças de segurança uma vantagem estratégica, pois permite que ações sejam coordenadas de maneira mais eficiente e precisa " (Werneck, 2021).	**3. Redução de Riscos Operacionais:** Esses dispositivos também são empregados em operações táticas, permitindo que a polícia tenha uma visão estratégica de áreas perigosas sem colocar vidas humanas em risco
Big Data e IA	O uso de big data foi identificado como uma ferramenta essencial para	**Localização e fundamentação da afirmação no texto (Capítulo 2 - Revisão Bibliográfica):**	Os dados e estudos analisados evidenciam o impacto do big data e da inteligência corrente na eficiência das operações de

	análises preditivas e tomada de decisões rápidas. A revisão de literatura revelou que o maior desafio é a integração dos dados coletados por diferentes fontes, como câmeras de vigilância, sensores urbanos e informações coletadas via inteligência corrente.		segurança pública. A seguir, destacam-se os principais achados:
		1. Importância do big data e da Inteligência Corrente: - "O conceito de cidades inteligentes... integra tecnologias de ponta, como a IoT e a análise intensiva de big data, para aprimorar a gestão urbana" (Calafate et al., 2020). - "A inteligência corrente visa manter as autoridades informadas de maneira contínua sobre eventos e situações em curso... com enfoque objetivo, descritivo e interpretativo" (Brasil, 2023).	**1. Análises Preditivas para Planejamento Urbano:** - A integração de dados de câmeras de vigilância e sensores urbanos, combinada com algoritmos de big data, permitiu identificar padrões de comportamento em áreas de maior criminalidade, otimizando a alocação de recursos policiais (Kitchin, 2014; Calafate et al., 2020).
		2. Desafios da Integração de Fontes de Dados: - " Hulnick (2006) destaca que o uso de tecnologias avançadas permite a detecção precoce de ameaças e a identificação de padrões comportamentais que passariam despercebidos sem o suporte da tecnologia.	**2. Desafios de Integração Tecnológica:** - Silva et al. (2020) descrevem o POI no Distrito Federal através da Operação Atena como uma medida eficaz na coordenação de

		- " Silva et al. (2020) ressaltam que a troca de informações e a coordenação interinstitucional são essenciais para o sucesso das operações de segurança, especialmente em um ambiente urbano complexo."	operações e na prevenção de crimes.
		3. Impacto na Tomada de Decisões e Segurança Pública: - "A coleta e análise contínua de dados provenientes de sensores e dispositivos conectados oferecem uma oportunidade sem precedentes para monitorar o ambiente urbano e prever possíveis incidentes" (Kitchin, 2014). - "O planejamento urbano e tecnológico, a mobilidade e o transporte público são fatores primordiais para tornar as cidades inteligentes e conectadas. A utilização de dados coletados por meio de tecnologias avançadas permite aos gestores públicos traçar diretrizes e metas para a construção colaborativa de uma cidade inteligente. " (Tavares, 2024).	**3. Impacto na Tomada de Decisões Rápidas:** - o POI visa identificar e planejar medidas corretivas para combater ameaças transnacionais, como o terrorismo e o crime organizado, além de ser aplicado no planejamento diário das operações policiais (OSCE, 2017).
Sensores Inteligentes	Os sensores espalhados por toda a cidade possibilitaram a coleta de dados em tempo real, o que, quando integrado à inteligência corrente, aumentou a eficiência do monitoramento urbano. A	**Localização e fundamentação da afirmação no texto (Capítulo 2 - Revisão Bibliográfica):**	**Resultados Obtidos com o Uso de Sensores Inteligentes:**

	análise documental destacou que, embora o uso de sensores seja amplamente adotado em cidades como Nova York, no Brasil sua implementação ainda é limitada.		
		1. Importância dos Sensores para a Coleta de Dados em Tempo Real: - "Além disso, uma cidade inteligente conecta infraestruturas físicas, sociais e empresariais para alavancar a inteligência coletiva" (Harrison et al., 2010).	**1. Eficiência no Monitoramento Urbano:** - Ratcliffe (2016) relata que a análise de dados permitiu identificar áreas críticas e direcionar o patrulhamento de forma mais eficiente. Essa abordagem também facilitou a identificação de redes criminosas e o desmantelamento de gangues.
		2. Uso Internacional e Nacional de Sensores Inteligentes: - " Em Nova York, por exemplo, o uso do POI ajudou a reduzir significativamente a taxa de crimes violentos. Ratcliffe (2016) relata que a análise de dados permitiu identificar áreas críticas e direcionar o patrulhamento de forma mais eficiente. Essa abordagem também facilitou a identificação de redes criminosas e o desmantelamento de gangues."	**2. Limitações no Brasil:** As RPAs estão sendo implementadas em diversas áreas da segurança pública, como gestão de emergências, controle de fronteiras e monitoramento ambiental (Costa; Reis Filho, 2019).

		3. Integração com Inteligência Corrente e Análise de big data: - "Segundo a Carta Brasileira para Cidades Inteligentes, o desenvolvimento centrado no cidadão e a inclusão digital são fundamentais para o sucesso das iniciativas de cidades inteligentes" (cartacidadesinteligentes.org.br, 2023).	**3. Impacto da Integração com Inteligência Corrente:** - O sistema integrado permite o monitoramento contínuo do território municipal através do cruzamento de dados de diferentes fontes. As informações geolocalizadas são utilizadas para produzir diagnósticos constantes e orientar ações operacionais da GCM. A matéria destaca exemplos práticos, como o Programa Guardiã Maria da Penha, que utiliza dados do sistema para planejar visitas e rondas, garantindo a segurança de vítimas de violência doméstica. (Prefeitura de São Paulo, 2023)

Fonte: Elaboração própria (2024)

4.1. PRINCIPAIS DESAFIOS ENCONTRADOS

Durante a pesquisa, diversos desafios foram encontrados, incluindo:

Quadro 13 – Desafios da pesquisa	
Coleta de dados dispersos:	Muitos dados sobre o uso de RPAs (drones) estavam dispersos em diferentes fontes e formatos, o que dificultou a sistematização das informações.
Dificuldade de integração tecnológica:	A falta de integração entre as diversas tecnologias utilizadas pela segurança pública foi um dos principais obstáculos identificados. A revisão bibliográfica revelou a necessidade de um sistema

	unificado que permita a interoperabilidade entre RPAs (drones), big data e sensores inteligentes.
Restrições regulatórias:	A análise documental indicou que a regulamentação do uso de RPAs ainda não acompanha a velocidade das inovações tecnológicas. A falta de diretrizes claras sobre o uso dessas tecnologias em áreas urbanas impede que seu potencial seja plenamente aproveitado.

Fonte: Elaboração própria (2024)


5

5 CONSIDERAÇÕES FINAIS

Ao longo da presente dissertação, explorou-se como a inteligência corrente pode ser aplicada para enfrentar os desafios impostos pela segurança pública no contexto das Cidades 4.0. A pesquisa foi guiada pelo objetivo geral de investigar a utilização da inteligência corrente nas operações da Polícia e avaliar os desafios impostos pela integração de novas tecnologias no ambiente urbano digital. Para isso, buscou-se examinar as ferramentas de monitoramento em tempo real, como câmeras de vigilância conectadas, análise de *big data* e sensores urbanos, e como esses recursos podem melhorar a eficácia das ações policiais.

Nesse cenário, a inteligência corrente é fundamental para fornecer informações em tempo real e apoiar decisões estratégicas em operações de segurança pública. O avanço das Cidades 4.0, com a adoção de tecnologias como a IoT, *big data* e IA, cria novas oportunidades e desafios para a segurança pública. Essas tecnologias permitem monitoramento contínuo, maior integração de dados e análise preditiva, permitindo que as forças policiais ajam de forma proativa, evitando crimes e otimizando os recursos disponíveis

A Polícia, ao aplicar a inteligência corrente, consegue utilizar dados em tempo real para melhorar suas operações. Essa capacidade é especialmente relevante no contexto de Cidades 4.0, onde a complexidade do ambiente urbano exige respostas rápidas e coordenadas. Ferramentas como câmeras de vigilância, sensores e RPAs (Aeronaves Remotamente Pilotadas), por exemplo, têm se mostrado essenciais para o monitoramento de grandes áreas, auxiliando na identificação de ameaças e na coleta de dados estratégicos

Nesse sentido, o uso de Aeronaves Remotamente Pilotadas - RPAs ou drones tornou-se uma peça-chave nas operações de segurança pública, especialmente no combate ao crime em áreas de difícil acesso. Essas tecnologias têm se mostrado eficazes para monitoramento aéreo em tempo real, permitindo às forças policiais responder rapidamente a incidentes e prevenir crimes antes que ocorram. O uso de sensores avançados, como câmeras térmicas e de

alta resolução, amplia a capacidade de ação das forças de segurança, tornando as operações mais ágeis e seguras.

A análise documental mostrou que as normas e regulamentações para o uso de RPAs e inteligência corrente ainda são incipientes no Brasil. Documentos governamentais, como o Projeto de Lei nº 2.310 de 2022, indicam um esforço contínuo para regulamentar o uso de tecnologias no policiamento urbano, mas há lacunas que ainda precisam ser preenchidas, principalmente no que diz respeito ao uso ético e seguro dessas ferramentas em áreas densamente povoadas.

Em virtude desse cenário, a presente dissertação buscou investigar o papel crucial da Inteligência Corrente nas operações policiais em um cenário urbano moldado pela rápida digitalização e expansão das Cidades 4.0. O objetivo principal, como dito alhures, foi compreender como essa ferramenta pode ser aplicada para enfrentar os desafios contemporâneos da segurança pública, otimizando o policiamento e garantindo a proteção da população em ambientes urbanos cada vez mais complexos e dinâmicos.

Ao responder às questões que nortearam este estudo, constatou-se que a Inteligência Corrente, quando corretamente implementada, oferece uma série de benefícios significativos. O uso de tecnologias avançadas, como sistemas de análise de *big data*, câmeras de vigilância conectadas e sensores inteligentes, permite uma coleta e análise contínua de informações. Isso proporciona às forças de segurança uma capacidade inédita de antecipar e reagir rapidamente a ameaças, transformando a abordagem tradicional do policiamento em uma prática mais proativa e preventiva.

Contudo, a dissertação também revelou obstáculos importantes para a implementação eficaz dessa inteligência. Entre os principais desafios estão a falta de integração tecnológica entre diferentes órgãos de segurança e a ausência de formação adequada para os policiais no uso dessas novas ferramentas. Além disso, as políticas públicas ainda precisam evoluir para acompanhar a complexidade das Cidades 4.0, garantindo que as tecnologias sejam usadas de maneira ética e eficaz, sem comprometer os direitos dos cidadãos.

Esse ponto levantado é muito importante, pois é necessário que as políticas públicas sejam ágeis e flexíveis, capazes de acompanhar a rápida evolução tecnológica. A criação de estruturas legais que regulamentem o uso de tecnologias emergentes e a proteção de dados

pessoais é imperativa. Além disso, investir em treinamento contínuo para os agentes de segurança é uma medida que não pode ser negligenciada. Apenas assim será possível aproveitar plenamente o potencial das tecnologias disponíveis, como os RPAs (drones) e sistemas de monitoramento, que têm se mostrado ferramentas valiosas no contexto da segurança pública.

A análise crítica desenvolvida neste trabalho ressaltou que a urbanização digital, apesar de oferecer avanços na gestão urbana, também cria novas vulnerabilidades, como ameaças cibernéticas e o aumento de crimes organizados no ciberespaço. Portanto, o papel das forças de segurança pública deve ser redefinido para incluir a proteção digital e a coordenação interinstitucional, promovendo uma resposta integrada e adaptada aos novos riscos.

A dissertação também procurou explorar como a Inteligência Corrente pode ser aplicada de maneira prática para enfrentar o crime organizado e outras formas de violência. Estudos de caso e exemplos práticos demonstraram que, embora as tecnologias avancem rapidamente, sua eficácia depende da capacidade das forças policiais de adaptarem suas estratégias operacionais. Portanto, a modernização das práticas policiais deve ser vista como um processo contínuo, que exige atualização constante e inovação.

Ao longo desta dissertação, investigou-se a relevância da Inteligência Corrente no contexto da segurança pública contemporânea, com um enfoque especial na aplicação prática das teorias desenvolvidas por autores como Arthur S. Hulnick, Gregory Treverton, Hank Prunckun e Sherman Kent. Esses teóricos fornecem uma base conceitual robusta descrevendo o uso da inteligência de maneira eficaz e ética em um mundo cada vez mais complexo e interconectado.

O papel da Inteligência Corrente é particularmente relevante em ambientes urbanos em rápida transformação, onde a coleta e análise de dados em tempo real se tornaram essenciais. Hulnick (2006), ao criticar o ciclo tradicional de inteligência, destaca que métodos convencionais de processamento de informações muitas vezes falham em oferecer a agilidade necessária para lidar com ameaças emergentes. Essa perspectiva reforça a necessidade de uma abordagem mais dinâmica e responsiva, característica fundamental da Inteligência Corrente. Treverton (2001) complementa essa visão,

enfatizando que a inteligência deve ser flexível para enfrentar as novas realidades informacionais, onde a antecipação de ameaças é tão crucial quanto a resposta imediata.

A influência dessas teorias na prática de segurança pública é evidente no Policiamento Orientado por Inteligência (ILP), que se baseia na coleta de dados para fundamentar decisões estratégicas e operacionais. Prunckun (2015) destaca a importância de integrar diferentes tipos de inteligência para aumentar a eficiência das operações policiais, defendendo ainda o uso de métodos científicos na análise de dados para garantir precisão e confiabilidade.

Alinhado ao estudo de Inteligência, o conceito de Cidades 4.0 representa um novo paradigma urbano em que a tecnologia permeia todos os aspectos da vida, gerando tanto oportunidades quanto desafios para a segurança pública. Essas Cidades dependem de grandes volumes de dados em tempo real para otimizar a segurança, mas também enfrentam riscos, como vulnerabilidades cibernéticas e preocupações com privacidade. A aplicação da Inteligência Corrente neste contexto é crucial, permitindo respostas rápidas e eficazes às ameaças que evoluem dinamicamente. Hollands (2008) e Kitchin (2014) discutem como a integração de sensores e sistemas inteligentes pode aprimorar a segurança, permitindo uma alocação mais eficiente de recursos e prevenindo crises.

Entretanto, a transição para Cidades 4.0 não está isenta de desafios. A integração de tecnologia avançada levanta questões sobre privacidade e segurança cibernética. Nesse cenário, a legislação brasileira, como a Lei Geral de Proteção de Dados (LGPD), e diretrizes internacionais estabelecem regras para o uso ético de dados, garantindo que operações de inteligência sejam transparentes e responsáveis. A Doutrina da Atividade de Inteligência 2023 reforça a importância de práticas éticas e legais, enquanto marcos como a Lei 9.883/1999 e a Política Nacional de Inteligência (PNI) oferecem um framework que equilibra segurança e direitos fundamentais.

O uso de RPAs (drones) exemplifica como as Cidades 4.0 podem se beneficiar de tecnologias emergentes. Drones são utilizados em operações de vigilância, monitoramento e resgate, oferecendo uma perspectiva aérea valiosa com informações em tempo real. A regulamentação pela ANAC garante que essas operações sejam seguras, respeitando tanto o espaço aéreo quanto a privacidade. Além

disso, a IA e *big data* proporcionam novas capacidades analíticas, mas também introduzem riscos, como ataques cibernéticos, exigindo legislação atualizada e medidas preventivas.

Desse modo, esta dissertação enfatiza a importância da coordenação interinstitucional para maximizar os benefícios das tecnologias emergentes. A colaboração entre agências de segurança é vital, assim como a formação contínua de profissionais para o uso adequado dessas ferramentas. Autores como Mendes, Correia e Serra (2021) sublinham que a aplicação colaborativa e descentralizada de tecnologias em cidades inteligentes promove eficiência e sustentabilidade, mas deve ser feita de maneira responsável. Dessa forma, a Inteligência Corrente se torna um elemento-chave na construção de cidades mais seguras e resilientes, desde que gerida com cuidado e respeito aos direitos dos cidadãos.

A análise apresentada evidencia que, embora as Cidades 4.0 ofereçam avanços significativos na gestão urbana, também demandam políticas públicas ágeis e flexíveis. As experiências globais com cidades como Barcelona e Masdar fornecem lições valiosas sobre os benefícios e limitações dessa transformação tecnológica. Com políticas adequadas, investimentos em capacitação e um compromisso ético, a Inteligência Corrente pode ser um poderoso aliado na segurança pública, garantindo que as cidades do futuro sejam não apenas mais conectadas, mas também mais seguras e humanas.

Além dos aspectos já discutidos, a presente dissertação destaca que o avanço das Cidades 4.0 não se limita apenas à incorporação de tecnologias emergentes, mas representa uma mudança paradigmática na maneira como interagimos com o ambiente urbano e na forma como a segurança pública é estruturada e gerida. A gestão da segurança pública, baseada em princípios de Inteligência Corrente, exige uma abordagem que combine inovação tecnológica com estratégias operacionais integradas.

As experiências internacionais supramencionadas, como as de Barcelona e Masdar, oferecem modelos que podem ser adaptados ao contexto brasileiro. Barcelona, reconhecida por suas iniciativas de inovação urbana, ilustra como a integração de tecnologias de vigilância e monitoramento pode melhorar a segurança e o bem-estar da população, enquanto Masdar destaca os desafios financeiros e de sustentabilidade envolvidos em projetos urbanos de alta tecnologia.

Essas experiências reforçam a importância de políticas que sejam tanto tecnológicas quanto socialmente conscientes, equilibrando a inovação com a inclusão e a acessibilidade.

Autores como Schuurman, Baccarne, De Marez e Mechant (2012) argumentam que as cidades modernas refletem uma evolução histórica na qual as exigências por segurança e infraestrutura se tornaram cada vez mais complexas. Com a revolução digital, os desafios se multiplicam, incluindo a necessidade de lidar com novas formas de criminalidade, como ataques cibernéticos, e a gestão de dados sensíveis em tempo real. Nesse contexto, o papel da Inteligência Corrente é fundamental para responder proativamente a ameaças, utilizando dados de múltiplas fontes para informar decisões rápidas e eficazes.

Por outro lado, o uso extensivo de tecnologias, como a IoT e *big data*, requer um gerenciamento ético e transparente. Rizzon, Bertelli, Matte, Graebin e Macke (2017) alertam para os riscos associados a uma inovação irresponsável, que pode comprometer a segurança dos dados pessoais e criar desigualdades sociais. Assim, as políticas públicas precisam ser formuladas com um olhar crítico e uma compreensão abrangente dos impactos sociais e éticos das novas tecnologias.

O desenvolvimento de Cidades 4.0 destaca a importância de estratégias de Policiamento Orientado por Inteligência (ILP) para maximizar a eficiência das operações policiais. O ILP, sustentado por dados analíticos, permite uma gestão mais eficiente dos recursos e uma melhor coordenação interinstitucional. Isso é crucial para enfrentar as ameaças urbanas contemporâneas, que muitas vezes ultrapassam as fronteiras de jurisdição e exigem uma resposta integrada de múltiplas agências.

Isso reforça o outro ponto importante abordado na dissertação que é a regulamentação do uso de RPAs (drones) e outras tecnologias de vigilância. Enquanto esses dispositivos proporcionam vantagens operacionais significativas, como o monitoramento aéreo em tempo real e a capacidade de intervir rapidamente em situações críticas, seu uso deve ser equilibrado com considerações éticas e legais. A ANAC, por exemplo, estabelece normas rigorosas para garantir a segurança do espaço aéreo e a proteção da privacidade dos cidadãos, demonstrando como a regulamentação pode acompanhar o ritmo da inovação tecnológica.

A discussão também aborda a necessidade de políticas de segurança pública que sejam flexíveis e adaptáveis para enfrentar a evolução constante das tecnologias. O conceito de governança inteligente, como enfatizado por autores como Carlos T. Calafate *et al*. (2020), sugere que as cidades podem se tornar mais eficientes e sustentáveis se adotarem uma abordagem colaborativa, que integre diferentes setores da sociedade, como saúde, transporte, e meio ambiente, na busca por soluções de segurança abrangentes.

A dissertação enfatiza que a transformação urbana trazida pelas Cidades 4.0 exige uma reavaliação constante das práticas e políticas de segurança pública. A IA, por exemplo, pode ajudar a prever crimes com base em padrões de dados históricos, mas também precisa ser gerida com transparência para evitar preconceitos e discriminação algorítmica. O uso ético de *big data* e IA na segurança pública deve ser monitorado por estruturas reguladoras, garantindo que as ferramentas sejam usadas de maneira justa e equitativa.

Os resultados desta dissertação evidenciam a importância da integração tecnológica no contexto da segurança pública nas Cidades 4.0. A necessidade do alinhamento da inteligência, RPAs e *big data* tem o potencial de transformar as operações policiais, permitindo uma resposta mais ágil e eficaz aos desafios contemporâneos. No entanto, o estudo também revelou desafios significativos, como a falta de integração tecnológica, a regulamentação insuficiente e a dificuldade de treinamento adequado das forças de segurança para lidar com essas inovações. Esses desafios precisam ser superados para que as tecnologias emergentes possam ser plenamente aproveitadas nas operações de segurança pública.

Portanto, a dissertação sugere que, para a Inteligência Corrente ser plenamente eficaz, é necessário um investimento contínuo em capacitação e treinamento dos agentes de segurança. O sucesso na implementação das tecnologias emergentes depende da competência dos profissionais em interpretá-las e aplicá-las de forma estratégica. Assim, a formação adequada e a atualização constante devem ser prioridades das políticas públicas para garantir que as cidades do futuro sejam resilientes, seguras e humanizadas.

Dessa forma, este trabalho não apenas contribui teoricamente para o campo da segurança pública, mas também oferece *insights* práticos para a aplicação da Inteligência Corrente em um mundo

urbano em constante transformação. Destarte, com a integração responsável da tecnologia e o compromisso ético com a proteção dos direitos dos cidadãos, podemos construir ambientes urbanos mais seguros e eficazes, capazes de responder aos desafios e oportunidades trazidos pela era digital.

A partir dessas constatações, este trabalho aduz que a Inteligência Corrente é uma peça importante para a transformação das Cidades 4.0 em espaços mais seguros. No entanto, seu uso deve ser acompanhado por políticas públicas robustas que garantam a proteção de dados, a privacidade dos cidadãos e a eficácia operacional das tecnologias utilizadas.

Os resultados desta dissertação reforçam que as tecnologias emergentes, como Aeronaves Remotamente Pilotadas (RPAs), *big data* e sensores inteligentes, desempenham papéis estratégicos na modernização da segurança pública em Cidades 4.0. No contexto brasileiro, os estudos de caso destacaram avanços significativos, como o aumento da precisão e eficiência nas intervenções, a redução de custos operacionais e a melhoria da segurança das equipes em campo, especialmente no Distrito Federal e em Minas Gerais.

O uso de *big data* consolidou-se como uma ferramenta essencial para análises preditivas, permitindo a identificação de padrões e a previsão de incidentes em ambientes urbanos complexos. Já os sensores inteligentes, embora amplamente adotados em cidades internacionais, ainda enfrentam desafios de implementação no Brasil. Sua integração com plataformas de inteligência corrente mostrou-se crucial para monitoramento urbano eficiente e intervenções rápidas. Esses achados evidenciam a importância de investimentos contínuos em infraestrutura tecnológica, capacitação de agentes e políticas públicas que garantam a regulamentação ética e eficaz dessas ferramentas. Assim, a Inteligência Corrente e as tecnologias emergentes não apenas fortalecem a segurança pública, mas também contribuem para a construção de cidades mais seguras, conectadas e resilientes, alinhadas aos princípios das Cidades 4.0.

Em conclusão, este estudo oferece contribuições teóricas e práticas para o campo da segurança pública, destacando a importância de uma abordagem integrada e tecnológica no policiamento urbano. A dissertação propõe que, com políticas públicas adequadas e investimentos em capacitação, a Inteligência Corrente pode ser um

aliado poderoso na criação de cidades mais seguras e resilientes. Assim, a segurança pública nas Cidades 4.0 pode ser significativamente aprimorada, desde que haja um compromisso coletivo para enfrentar os desafios e aproveitar as oportunidades trazidas pela era digital.

Destarte, esta dissertação contribui significativamente para a discussão sobre o uso de tecnologias emergentes na segurança pública, oferecendo uma análise aprofundada de como essas ferramentas podem ser integradas para melhorar a eficácia das operações policiais nas Cidades 4.0. Ao destacar os principais desafios e benefícios da aplicação de RPAs, *big data* e sensores inteligentes, o trabalho abre caminho para novas investigações acadêmicas e propostas de políticas públicas mais eficientes.

Estudos futuros podem explorar as seguintes áreas: modelos de governança tecnológica para garantir a integração eficaz das tecnologias emergentes; capacitação das forças de segurança pública para lidar com a complexidade das Cidades 4.0; regulamentação mais clara e eficiente sobre o uso de drones e *big data* na segurança pública, garantindo a proteção dos direitos fundamentais dos cidadãos.

Esse estudo demonstra que embora existam desafios a serem superados, o potencial das tecnologias emergentes para transformar a segurança pública é vasto. A partir dessa base, espera-se que futuros estudos possam explorar ainda mais profundamente o papel da inteligência corrente e sua interação com tecnologias de ponta nas Cidades 4.0.

REFERÊNCIAS

REFERÊNCIAS

REFERÊNCIAS

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL (ANAC). *Regras para Operação de RPAs*. Disponível em: https://www.anac.gov.br.

AHVENNIEMI, Hannele, *et al. What are the differences between sustainable and smart cities?* Cities, v. 60, 2017. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0264275116302578?via%3Dihub.

ANTUNES, Priscila Carlos Brandão *SNI & ABIN: entre a teoria e a prática*. Rio de Janeiro: FGV, 2001

ALVES, Paulo Henrique Ferreira. *Valores humanos, metas de compaixão e autoimagem e comprometimento organizacional na polícia militar do Distrito Federal*. Dissertação (Mestrado). Universidade de Brasília, 2018. Disponível em: http://dx.doi.org/10.26512/2018.02.D.32016.

_____. *"Ser policial é, sobretudo, uma razão de ser; é enfrentar a morte, mostrar-se forte no que acontecer": O papel dos valores, das metas e do suporte social no bem-estar na PMDF. 2023*. Tese (Doutorado em Psicologia Social, do Trabalho e das Organizações) — Universidade de Brasília, Brasília, 2023.

ASSOCIAÇÃO NACIONAL DE DIRIGENTES DE INSTITUIÇÕES FEDERAIS DE ENSINO SUPERIOR (ANDIFES). Carta Brasileira para Cidades Inteligentes. Disponível em: https://cartacidadesinteligentes.org.br/#:~:text=A%20Carta%20%C3%A9%20um%20pacto%20com%20conceitos,%20estrat%C3%A9gias.

BRASIL. Agência Brasileira de Inteligência. *Doutrina da Atividade de Inteligência*. Brasília: ABIN, 2023.

_____. *Constituição da República Federativa do Brasil de 1988*. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm.

_____. Decreto nº 8.793, de 29 de junho de 2016. Institui a Política Nacional de Inteligência e dispõe sobre o Sistema Brasileiro de Inteligência. Diário Oficial da União: seção 1, Brasília, DF, 30 jun. 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm.

_____. Decreto nº 3.695, de 21 de dezembro de 2000. *Cria o Subsistema de Inteligência de Segurança Pública, no âmbito do Sistema Brasileiro de Inteligência, e dá outras providências*. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d3695.htm.

_____. Decreto-Lei nº 3.689, de 3 de outubro de 1941. *Código de Processo Penal (CPP)*. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm.

_____. Decreto nº 10.531, de 26 de outubro de 2020. *Institui a Estratégia Federal de Desenvolvimento para o Brasil no período de 2020 a 2031*. Disponível em: http://www.in.gov.br/en/web/dou/-/decreto-n-10.531-de-26-de-outubro-de-2020-285019495.

_____. Doutrina Nacional de Inteligência de Segurança Pública (DNISP). Coordenação-Geral de Inteligência. Secretaria Nacional de Segurança Pública - Ministério da Justiça, 2016.

_____. Estratégia Nacional de Inteligência (ENINT). Brasília: ABIN, 2017.

_____. Lei nº 9.883, de 7 de dezembro de 1999. *Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências*. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/L9883.htm.

_____. Lei n.º 13.709, de 14 de agosto de 2018. *Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet)*. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

_____. Ministério da Ciência, Tecnologia e Inovação. *Cidades Inteligentes*. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/camara-cidades.

_____. Ministério da Defesa. *Política de Inteligência de Defesa*. 1. ed. Brasília: Ministério da Defesa, 2023. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD60P01PolticadeIntelignciadeDefesaPID1Ed.2023.pdf.

_____. Projeto de Lei nº 1.864, de 2019. *Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 3.689, de 3 de*

outubro de 1941 - Código de Processo Penal, e outras leis para estabelecer medidas contra a corrupção, o crime organizado e os crimes praticados com grave violência à pessoa. Disponível em: https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-1864-2019.

_____. Projeto de Lei nº 2.310, de 2022. *Dispõe sobre as ações de inteligência exercidas pelas instituições previstas no art. 144 da Constituição Federal, destinada à busca, produção e tratamento de informações necessárias à prevenção da criminalidade e violência*. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/136646.

_____. Projeto de Lei do Senado nº 2.719/2019. *Estabelece o marco regulatório da Atividade de Inteligência Brasileira*. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/136646.

_____. Resolução SENASP nº 1, de 15 de julho de 2009. *Regulamenta o Subsistema de Inteligência de Segurança Pública - SISP, e dá outras providências*. Disponível em: https://www.normasbrasil.com.br/norma/?id=111521.

CALAFATE, Carlos Tavares. *et al*. *The transition from smart cities to smart cities 4.0. Journal of Urban Technology,* 2020.

CAPDEVILA, Ignasi; ZARLENGA, Matias. I. *Smart City or Smart Citizens?* The Barcelona Case. 2015.

CARAGLIU, Andrea, *et al*. *Smart cities in Europe. Proceedings of the 3rd Central European Conference on Regional Science*, 2009.

CARNEIRO, Juvenildo dos Santos; MOREIRA, Waldicharbel Gomes. *Ciberritório do crime: desafios da inteligência de segurança pública no combate ao crime organizado*. In: LEIMGRUBER, Mónica Pinto; SOUZA, Hêndrio Inandy José de; LOPES, Yuri Fonseca (Orgs.). Inteligência, segurança pública e organização criminosa. Brasília, DF: Gráfica Movimento, 2023. p. 291.

CASTELLS, Manuel. *The rise of the network society*. 2. ed. Malden: Wiley-Blackwell, 2010.

CENTRO DE GESTÃO E ESTUDOS ESTRATÉGICOS (Brasil). *Segmentos ou nichos com maior potencial para o desenvolvimento tecnológico nacional*. Brasília, DF: Centro de Gestão e Estudos Estratégicos, 2022.

(Série Documentos Técnicos, 31), 112 p. ISBN 978-65-5775-029-2. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivo-camara-industria/iniciativas/ci_nt_nicho_tec_nac.pdf.

CEPIK, Marco. *Espionagem e democracia: agilidade e transparência como dilemas na institucionalização de serviços de inteligência*. Rio de Janeiro: FGV, 2003.

_____. *Inteligência como Processamento de Informação*. In: _____. Inteligência, Processos e Política. Brasília: UnB, 2003.

CORDEIRO, Ivana Oliveira. *Accountability e seu impacto na qualidade da atividade policial na segurança pública*. 2014. 123 f. Dissertação (Mestrado em Segurança Pública, Justiça e Cidadania) – Universidade Federal da Bahia, Salvador, 2014.

CORREIO BRASILIENSE. *Entenda como agiu casal que sequestrou, dopou e estuprou criança na Asa Norte*. Correio Braziliense, Brasília, 30 jun. 2023. Disponível em: https://www.correiobraziliense.com.br/cidades-df/2023/06/5105593-homem-sequestrou-dopou-e-estuprou-uma-crianca-de-12-anos-na-asa-norte.html.

CORREIO BRASILIENSE. *Entenda como agiu casal que sequestrou, dopou e estuprou criança na Asa Norte*. Correio Braziliense, Brasília, 30 jun. 2023. Disponível em: https://www.correiobraziliense.com.br/webstories/2023/06/5105694-entenda-como-agiu-casal-que-sequestrou-dopou-e-estuprou-crianca-no-df.html.

CORREIO BRASILIENSE. *Com pouco efetivo da PM nas ruas do DF, a sensação de insegurança continua*. Correio Braziliense, Brasília, 11 jul. 2023. Disponível em: https://www.correiobraziliense.com.br/cidades-df/2023/07/5108631-com-pouco-efetivo-da-pm-nas-ruas-do-df-a-sensacao-de-inseguranca-continua.html .

COSTA, De Leon Petta Gomes da. *Cooperação entre Estado-Nação e crime organizado: uma geopolítica obscura. 2017*. Tese (Doutorado em Geografia Humana) - Faculdade de Filosofia, Letras e Ciências Humanas, Universidade de São Paulo, São Paulo, 2017. Disponível em: https://www.teses.usp.br/teses/disponiveis/8/8136/tde-19032018-115217/publico/2017_DeLeonPettaGomesDaCosta_VCorr.pdf.

COSTA, Rafaela Duarte. *Uso de drones na segurança pública: análise sobre a sua utilização pelas forças e serviços de segurança em Portugal*. 2019. Dissertação (Mestrado em Ciência Política e Segurança) – Faculdade de Ciências Sociais e Humanas, Universidade Nova de Lisboa, Lisboa, 2019. Disponível em: https://run.unl.pt/bitstream/10362/91298/1/Costa_2019.pdf. Acesso em: 06 out. 2024.

CNN BRASIL. *Brasil perdeu mais de 30 mil policiais militares em 10 anos, diz estudo*. CNN Brasil, 27 fev. 2024. Disponível em: https://www.cnnbrasil.com.br/nacional/pms-do-brasil-perderam-30-mil-policiais-em-uma-decada/ .

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO (DECEA). *Voos de RPAS (drones): entenda a nova legislação do DECEA*. 2015. Disponível em: https://www.decea.mil.br/?i=midia-e-informacao&p=pg_noticia&materia=voos-de-rpas-drones-entenda-a-nova-legislacao-do-decea.

EXATI. *Cidades digitais e cidades inteligentes: entenda as diferenças*. Disponível em: https://blog.exati.com.br/cidades-digitais-e-cidades-inteligentes/.

FAIAD, Cristiane; MELLO, Daniel Botelho de; TUPINAMBÁ, André Luis *et al*. *Saúde na segurança pública: indicadores e diretrizes para intervenções no âmbito do Programa Nacional de Qualidade de Vida para Profissionais de Segurança Pública – Pró-Vida*. Brasília: UnB, 2022.

FARIAS, José Lucio Dantas Júnior. *Monitoramento com veículos aéreos não tripulados em apoio às atividades da PMDF*. 2021. Trabalho de Conclusão de Curso (Bacharelado em Ciências Policiais) – Instituto Superior de Ciências Policiais, Brasília, 2021

FERREIRA, Luís Henrique Costa; FERREIRA, Nilton José Costa. *Investigação criminal: um estudo metodológico*. Salvador: OSPBA, 2011.

FOLHA DE SÃO PAULO. *Gestão Covas implanta programa contra crime adotado em Nova York*. Folha de S. Paulo, São Paulo, 22 fev. 2019. Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/02/gestao-covas-implanta-programa-contra-crime-adotado-em-nova-york.shtml.

FRANCO, Alberto Silva. *Leis Penais e sua interpretação jurisprudencial*. São Paulo: Revista dos Tribunais, 2002.

GARNETT, Kathryn, *et al*. *Towards an innovation principle: an industry trump or shortening the odds on environmental protection?* Law Innov. Technol., v. 10, n. 1, 2018.

GIBSON, David V., *et al*. *The Technopolis phenomenon: smart cities, fast systems, global networks. Lanham,* Md.: Rowman & Littlefield Publishers, 1992.

GIFFINGER, Rudolf, *et al*. *City-ranking of European medium-sized cities*. 2007. Disponível em: https://www.smart-cities.eu/index2.html.

GIL, Antonio Carlos. *Como elaborar projetos de pesquisa*. 4. ed. São Paulo: Editora Atlas, 2002.

GRIFFITHS, Steven; SOVACOOL, Benjamin K. *Rethinking the future low-carbon city: Carbon neutrality, green design, and sustainability tensions in the making of Masdar City*. Energy Research & Social Science, v. 62, 2020.

HARRISON, Colin, *et al*. *Foundations for Smarter Cities*. IBM Journal of Research and Development, v. 54, n. 4, 2010.

HOLLANDS, Robert G. *Will the Real Smart City Please Stand Up? Intelligent, Progressive or Entrepreneurial?* City, v. 12, n. 3, p. 303-320, 2008.

HULNICK, Arthur S. *What's wrong with the Intelligence Cycle*. *Intelligence and National Security*, v. 21, n. 6, p. 959-979, 2006.

INSTITUTO DE PESQUISA ECONÔMICA APLICADA (IPEA). *Atlas da Violência 2023*. Disponível em: https://www.ipea.gov.br/atlasviolencia/arquivos/artigos/9350-223443riatlasdaviolencia2023-final.pdf.

JOSS, Simon; MOLELLA, Arthur P. *The Eco-City as Urban Technology: Perspectives on Caofeidian International Eco-City (China)*. Journal of Urban Technology, v. 20, 2013.

KLAUSER, Francisco. *Police Drones and the Air: Towards a Volumetric Geopolitics of Security*. Swiss Political Science Review, 2021.

KENT, Sherman. *Informações Estratégicas*. Rio de Janeiro: Biblioteca do Exército, 1967.

KITCHIN, Rob. *The Real-Time City? Big Data and Smart Urbanism*. GeoJournal, v. 79, p. 1-14, 2014.

LAZZARINI, Álvaro *et al*. *Direito Administrativo da Ordem Pública*. 2. ed. Rio de Janeiro: Forense, 1987.

LAU, Arthur. Masdar City: *A model of urban environmental sustainability*. Stanford Undergraduate Research Journal, v. 11, 2012.

LEE, Jung Hoon, *et al*. *An integrated service-device-technology roadmap for smart city development. Technological Forecasting and Social Change*, v. 80, n. 2, 2013.

LENZA, Pedro. *Direito constitucional esquematizado***.** 26. ed. São Paulo: Saraiva, 2022.

MARRIN, Stephen. *Improving Intelligence Analysis*. 1. ed. Londres: Routledge, 2011. Disponível em: https://www.taylorfrancis.com/books/mono/10.4324/9780203810200/improving-intelligence-analysis-stephen-marrin.

MARTINS, Cláudia Garrido; FERREIRA, Miguel Luiz Ribeiro. *O Survey como tipo de pesquisa aplicado na descrição do conhecimento do processo de gerenciamento de riscos em projetos no segmento da construção.* Rio de Janeiro: VII Congresso Nacional de Excelência em Gestão, 12 e 13 de agosto de 2011. Disponível em:https://www.passeidireto.com/arquivo/90341578/o-survey-como-tipo-de-pesquisa-aplicado-na-descricao-do-conhecimento-do-processo.

MARTY, Otto Luiz. *Uso de aeronaves remotamente pilotadas pela inteligência policial militar no combate aos crimes violentos contra o patrimônio.* 2022. 130 f. Trabalho de Conclusão de Curso (Graduação em Inteligência Policial) – Academia de Polícia Militar, Curitiba, 2022.

MENDES, Ireneu de Oliveira Mendes, *et al*. *Smart Governance às Smart Cities*. Revista Estudo & Debate, v. 28, 2021.

MOUGENOT, Edilson. *Curso de Processo Penal*. 13. ed. São Paulo: Saraiva, 2019.

MUSTERD, Sako; OSTENDORF, Wim. *Creative Cultural Knowledge Cities: Perspectives and Planning Strategies.* Built Environment, v. 30, n. 3, 2003.

NAM, Taewoo; PARDO, Theresa A. *Conceptualizing smart city with dimensions of technology, people, and institutions.* 2011.

OLIVEIRA, Iramaria Pires de. *Infraestrutura 4.0: tecnologia das cidades inteligentes*. Disponível em: https://digital.intermodal.com.br/tecnologia/infraestrutura-40-tecnologia-das-cidades-inteligentes.

ORGANIZAÇÃO PARA A SEGURANÇA E COOPERAÇÃO NA EUROPA (OSCE**).** *Intelligence-Led Policing in Europa*, 2017.

PACHECO, Rafael. *Crime organizado: medidas de controle e infiltração policial.* Curitiba: Juruá, 2011.

PETERSON, Marilyn. *Intelligence-Led Policing: The New Intelligence Architecture*. Washington, D.C.: Bureau of Justice Assistance, 2005

PLANO ESTRATÉGICO: 2023 - 2034 - *Comando-Geral da Polícia Militar do Distrito Federal. Brasília: PMDF - Comissão do Plano Estratégico,* 2022. 1. ed. Disponível em: https://www.pmdf.df.gov.br.

PORTARIA PMDF Nº 1.212, DE 26 DE AGOSTO DE 2021. *Regulamenta o uso de RPAs no âmbito da Polícia Militar do Distrito Federal.* Disponível em: https://www.pmdf.df.gov.br.

PORTARIA SECRETARIA MUNICIPAL DE SEGURANÇA URBANA - *SMSU nº 1, de 4 de janeiro de 2019. Institui o Sistema Inteligente de Suporte à Tomada de Decisão em Segurança Urbana* - CompStat Paulistano. Disponível em: https://legislacao.prefeitura.sp.gov.br/leis/portaria-secretaria-municipal-de-seguranca-urbana-smsu-1-de-4-de-janeiro-de-2019.

PREFEITURA DE SÃO PAULO. *Prefeitura de São Paulo implanta o CompStat Paulistano*. Secretaria Municipal de Segurança Urbana, 27 fev. 2019. Disponível em: https://capital.sp.gov.br/web/seguranca_urbana/w/noticias/272128.

PREFEITURA DE SÃO PAULO. *CompStat Paulistano - sistema integrado para identificação de áreas sensíveis à desordem urbana*. Secretaria Municipal de Segurança Urbana, 14 set. 2023. Disponível em: https://capital.sp.gov.br/web/seguranca_urbana/w/noticias/314403.

PRUNCKUN, Hank. *Scientific methods of inquiry for intelligence analysis.* 2. ed. Lanham: Rowman & Littlefield, 2015.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL (PUCRS). *Cidades Inteligentes: o que são e quais suas vantagens?* Disponível em: https://online.pucrs.br/blog/cidades-inteligentes.

RATCLIFFE, Jerry. *Intelligence-Led Policing*. 2. ed. Londres: Routledge, 2016. Disponível em: https://www.taylorfrancis.com/books/mono/10.4324/9781315717579/intelligence-led-policing-jerry-ratcliffe.

REIS, Paulo. *Um panorama sobre a utilização de drones. 2019*. Trabalho de Conclusão de Curso (Graduação em Engenharia) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2019. Disponível em: https://inovacao.ufrj.br/images/vol_18_panorama_da_utilizacao_de_drones_2019.pdf.

RIZZON, Fernanda, *et al*. Smart City: *Um Conceito em Construção*. Revista Metropolitana de Sustentabilidade, v. 7, 2017.

SANTOS, Layla Maria de Sousa. *Inteligência e Segurança Pública*. Curitiba: IESDE, 2020.

SARTE, Átila Medeiros. *Proposta de padronização do serviço de aeronaves remotamente pilotadas no Corpo de Bombeiros Militar de Santa Catarina.* 2017. Monografia (Curso de Comando e Estado Maior em Gestão Pública com Ênfase na Atividade de Bombeiro Militar) – Corpo de Bombeiros Militar de Santa Catarina, Centro de Ensino Bombeiro Militar, Universidade do Estado de Santa Catarina, Florianópolis, 2017.

SCHUURMAN, Dimitri, *et al*. *Smart Ideas for Smart Cities: Investigating Crowdsourcing for Generating and Selecting Ideas for ICT Innovation in a City Context*. *Journal of theoretical and applied electronic commerce research,* v. 7, n. 3, 2012.

SELADA, Catarina; SILVA, Carla. *As Cidades Inteligentes na Agenda Europeia: Oportunidades para Portugal.* 2020. 200 f. Dissertação (Mestrado em Administração Pública) – Universidade de Lisboa, Lisboa, 2020.

SEVERINO, Antonio Joaquim. *Metodologia do trabalho científico***.** São Paulo: Cortez, 2016.

SILVA, João *et al*. *Intelligence-Led Policing: A strategy for modern law enforcement***.** Policing and Society, 2020.

SILVA, Jean Carlos Inácio. *Efeitos do Uso de Aeronaves Remotamente Pilotadas na Produção de Conhecimento no Campo da Inteligência de Segurança Pública*. Belo Horizonte: Academia de Polícia Militar de Minas Gerais, 2018.

SMITH, R. *Cybercrime, illicit markets, and the deep web: Trends in online criminality*. Global Crime Journal, v. 21, n. 1, p. 98-115, 2020. Disponível em: https://doi.org/10.1080/17440572.2020.1705189.

SOBRAL, Paulo Victor Nunes Costa; SANTOS, Ana Teresa. *A inserção dos drones (RPAs) na segurança pública brasileira: uma análise sob a ótica do princípio da eficiência.* Revista Em Tempo, v. 18, n. 01, p. 133-155, 2019. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3209.

STEPAN, Alfred C. *The Military in Politics: Changing Patterns in Brazil. Princeton: Princeton University* Press, 1971. Disponível em: https://www.degruyter.com/document/doi/10.1515/9781400868704/html.

STRECK, Lenio Luiz; MORAIS, José Luis Bolzan de. *Ciência Política e Teoria do Estado*. Porto Alegre: Editora Livraria do Advogado, 2014.

WENDT, Emerson; BARRETO, Alessandro Gonçalves. *Inteligência digital: foco nas fontes abertas como ferramentas para produção de provas e conhecimentos de inteligência policial*. Rio de Janeiro: Brasport, 2013.

TAVARES, Larissa. *A importância do planejamento de políticas públicas para cidades inteligentes*. Revista de Administração Pública, 2023.

TREVERTON, Gregory. *Reshaping National Intelligence for an Age of Information.* Cambridge University Press, 2001.

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). *Global Study on Homicide 2023.* Disponível em: https://www.unodc.org/documents/data-and-analysis/gsh/2023/Global_study_on_homicide_2023_web.pdf.

WASHBURN, Doug, *et al. Helping CIOs Understand "Smart City" Initiatives: Defining the Smart City, Its Drivers, and the Role of the CIO.* Forrester Research, Inc., 2010.

WERNECK, Marcus Aurelius Alkmim Pinho. *O uso de aeronaves remotamente pilotadas (drones) no policiamento ostensivo*. 2024. Trabalho de Conclusão de Curso (Especialista em Gestão Estratégica em Segurança Pública) – Instituto Superior de Ciências Policiais, Polícia Militar do Distrito Federal, Brasília, 2024.

YIGITCANLAR, Tan, *et al. The making of smart cities: Are Songdo, Masdar, Amsterdam, San Francisco and Brisbane the best we could build? Cities*, v. 88, 2019.

ZANELLA, Andrea, *et al. Internet of Things for Smart Cities*. IEEE Internet of Things Journal, v. 1, n. 1, 2014


idp
A ESCOLHA QUE
TRANSFORMA
O SEU CONHECIMENTO