**UNIVERSIDADE ALTO VALE DO RIO DO PEIXE – UNIARP**
**PROGRAMA DE MESTRADO ACADÊMICO EM DESENVOLVIMENTO E SOCIEDADE – PPGDS**

**IRINÉIA DA SILVA**

# A INTELIGÊNCIA DE SEGURANÇA PÚBLICA NO CONTEXTO DAS SMART CITIES

**CAÇADOR**
2023

**UNIVERSIDADE ALTO VALE DO RIO DO PEIXE – UNIARP**
**PROGRAMA DE MESTRADO ACADÊMICO EM DESENVOLVIMENTO E SOCIEDADE – PPGDS**

**IRINÉIA DA SILVA**

# A INTELIGÊNCIA DE SEGURANÇA PÚBLICA NO CONTEXTO DAS *SMART CITIES*

**CAÇADOR**
**2023**

## FICHA CATALOGRÁFICA

Silva, Irinéia da

A inteligência de segurança pública no contexto das smart cities/ Irinéia da Silva - Caçador, 2023.

100 f

Orientador: José Luiz Gonçalves da Silveira

Dissertação (Mestrado) – Programa de Pós-Graduação em Desenvolvimento e Sociedade - Universidade Alto Vale do Rio do Peixe (UNIARP)

1. Segurança Pública. 2. Cidades Inteligentes. 3. Atividade de Inteligência.

**IRINÉIA DA SILVA**

**A INTELIGÊNCIA DE SEGURANÇA PÚBLICA**
**NO CONTEXTO DAS SMART CITIES**

**A Comissão Examinadora, abaixo assinada, aprova a Dissertação** apresentada no Programa de Mestrado Acadêmico em Desenvolvimento e Sociedade – PPGDS, Linha de Pesquisa Sociedade, Cidadania e Segurança, da Universidade Alto Vale do Rio do Peixe - UNIARP, como requisito parcial para obtenção do título de **Mestre em Desenvolvimento e Sociedade.**

**BANCA EXAMINADORA**

---

**Profº Dr. José Luiz Gonçalves da Silveira** - UNIARP
Presidente da Banca/ Orientador

---

**Profº Dr. Levi Hülse** - UNIARP
Membro

---

**Profº Dr. André Moraes dos Santos** - UNIVALI
Membro

Caçador - SC, junho de 2023.

Aos meus filhos Isabelle (14 anos) e Lucas (7 anos).

## AGRADECIMENTOS

Este trabalho é conjugação de esforços de um elenco de ilustres mestres, cada um contribuindo para a minha caminhada, a quem agradeço: Dr. Adélcio Machado dos Santos, Dr. Anderson Antônio Mattos Martins; Dr. Cesar Augustus Winck, Dra. Claudriana Locatelli, Dra. Eliana Rezende Adami, Dra. Ivanete Schneider Hahn, Dr. Joel Cezar Bonin, Dr. Joel Haroldo Baade, Dr. Lincon Bordignon Somensi, Dr. Maurício Andrade de Lima, Dr. Ricelli Endrigo Ruppel da Rocha, Dra. Rosana Cláudio Silva Ogoshi, Dr. Giovani de Paula (professor colaborador na disciplina);

Um agradecimento especial ao professor coordenador do curso e membro da banca Profº Dr. Levi Hülse e ao Profº Dr. André Moraes dos Santos – UNIVALI - Membro Externo da minha Banca.

Um agradecimento muito especial ao Profº Dr. José Luiz Gonçalves da Silveira (Coronel Gonçalves) meu professor, orientador, amigo e inenarrável ser humano, ao qual não tenho palavras para expressar toda a minha gratidão e admiração.

A todos os colegas do mestrado, em especial, os da linha de pesquisa "Sociedade, Legislação e Segurança".

Ao meu companheiro de vida Alessandro José Maia agradeço pela compreensão e apoio. Também agradeço aos profissionais médicos que me trataram durante o percurso, em especial ao Dr. Rui Arsego. Por fim, minha gratidão a Dra. Tiani Regina de Borba, a minha irmã Profª. Francieli da Silva e ao Dr. Paulo Lima.

A todos aqueles que de forma presencial ou à distância participaram ou contribuíram para a elaboração deste estudo.

## RESUMO

O presente estudo evidenciou que a segurança pública, assim como a própria atividade de inteligência pode ser potencializada utilizando-se da tecnologia que compõe o ecossistema das chamadas *Smart Cities* ou cidades inteligentes, visando além das ações de segurança (prevenção, mitigação e repressão), a produção de conhecimento para fundamentação e proposição de políticas públicas para a melhoria da qualidade de vida. As cidades inteligentes se transformaram em tema de grande importância nas discussões sobre o desenvolvimento urbano sustentável, no mundo e no Brasil e o estudo, portanto, está em consonância com a linha 03 (três) do mestrado em Desenvolvimento e Sociedade: "Sociedade, Legislação e Segurança", com abordagem interdisciplinar com interfaces do campo do direito, a administração pública, da segurança pública, ciências policiais e tecnologia da informação e comunicação. No âmbito metodológico, o estudo se caracterizou como bibliográfico de caráter exploratório-descritivo, através de livros, artigos e revistas especializadas. A pesquisa foi documental, utilizando-se da doutrina e publicações sobre o tema. Para fundamentação teórica, se buscou evidências científicas nas bases teóricas da atividade de inteligência de segurança pública e seus instrumentos normativos no Brasil, abordando os conceitos e dinâmicas operacionais da atividade de inteligência, os conceitos aplicáveis ao tema das cidades inteligentes e as experiências da literatura sobre as cidades inteligentes. E, por fim, se buscou levantar exemplos de sistemas e dispositivos que podem ser utilizados pela inteligência de segurança pública, a exemplo do cinturão digital, como parte da arquitetura de uma cidade inteligente, como uma possibilidade de aplicação pelas cidades que avançam para caracterizar-se como inteligentes, abordando os desafios e as perspectivas deste novo momento das cidades, cujo uso da inovação e das tecnologias de informação e comunicação vêm contribuir para um melhor desenvolvimento da sociedade contemporânea, com olhar voltado à sustentabilidade e à concretização dos Objetivos do Desenvolvimento Sustentável (ODS – Agenda 2030).



**Palavras-chave:** Inteligência. Segurança Pública. "Smart Cities". Sustentabilidade

## ABSTRACT

The present study showed that public safety, as well as the intelligence activity itself, can be enhanced using the technology that makes up the ecosystem of the so-called Smart Cities or smart cities, aiming beyond security actions (prevention, mitigation and repression), the production of knowledge to support and propose public policies to improve the quality of life. Smart cities have become a topic of great importance in discussions on sustainable urban development, in the world and in Brazil, and the study, therefore, is in line with line 3 of the master's degree in Development and Society: "Society, Legislation and Security" with an interdiciplinary approach with interfaces from the field of law, public administration, public security, police sciences and information and communication technology. In the methodological scope, the study was characterized as bibliographical with an exploratory-descriptive character, through books, articles and specialized magazines. The research was documentary, using the doctrine and publications on the subject. For the theoretical foundation, scientific evidence was sought in the theoretical bases of public security intelligence activity and its normative instruments in Brazil, addressing the concepts and operational dynamics of intelligence activity, the concepts applicable to the theme of smart cities and the experiences of the literature on the smart cities. And finally, we sought to raise examples of systems and devices that can be used by public security intelligence, such as the digital belt, as part of the architecture of a smart city, as a possibility of application by cities that advance to characterize it as intelligent, addressing the challenges and perspectives of this new moment for cities, whose use of innovation and information and communication technologies contribute to a better development of contemporary society with a focus on sustainability and the achievement of the Sustainable Development Goals (SDG - Agenda 2030).



**Keywords**: Intelligence; Public security; “Smart Cities”. Sustainability.

## LISTA DE FIGURAS

## LISTA QUADROS

## LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| ABIN | Agência Brasileira de Inteligência |
| ABNT | Associação Brasileira de Normas Técnicas |
| ADPF | Arguição de Descumprimento de Preceito Fundamental |
| AGM Brasil | Associação dos Guardas Municipais do Brasil |
| CDN | Conselho de Defesa Nacional |
| CDN | Seções de Defesa Nacional |
| CIA | Agência Central de Inteligência |
| DI | Departamento de Inteligência |
| DIE | Divisão de Infantaria Expedicionária |
| DINI | Diretoria de Informação e Inteligência |
| DNISP | Doutrina Nacional de Inteligência de Segurança Pública |
| ENISP | Estratégia Nacional de Inteligência de Segurança Pública |
| ESG | Escola Superior de Guerra |
| EsNI | Escola Nacional de Informações |
| FEB | Força Expedicionária Brasileira |
| GSI/PR | Gabinete de Segurança Institucional da Presidência da República |
| ISO | International Organization for Standardization |
| NAU | Nova Agenda Urbana |
| OCRs | *Optical Characteres Recognized* |
| ODS | Objetivos de Desenvolvimento Sustentável |
| ONU | Organização das Nações Unidas |
| PDTCI | Plano Diretor de Cidade Inteligente |
| PNI | Política Nacional de Inteligência |
| PNI | Plano Nacional de Informações |
| PNISP | Política Nacional de Inteligência de Segurança Pública |
| PNSPDS | Política Nacional de Segurança Pública e Defesa Social |
| Pronasci | Programa Nacional de Segurança Pública com Cidadania |
| RFA | República Federal Alemã |
| SAE | Secretaria de Assuntos Estratégicos |
| SBI | Sistema Brasileiro de Inteligência. |
| SENASP | Secretaria Nacional de Segurança Pública |
| SEPROT | Secretaria de Defesa Civil e Segurança Pública |

| | |
|---|---|
| SFICI | Serviço Federal de Informações e Contrainformações |
| SIC | Serviço de Informações e Contrainformações |
| SisNi | Sistema Nacional de Informações |
| SISP | Subsistema de Inteligência de Segurança Pública |
| SNI | Serviço Nacional de Informações |
| SSI/SAE | Subsecretaria de Inteligência da Secretaria de Assuntos Estratégicos |
| SUSP | Sistema Único de Segurança Pública |
| TD | Transformação Digital |
| TIC | Tecnologia da informação e da Comunicação |

## SUMÁRIO

# 1 INTRODUÇÃO

O presente estudo tem como tema a atividade de inteligência de segurança pública e os sistemas que fazem parte das *Smart Cities* ou cidades inteligentes, que podem ser utilizados pelos serviços de inteligência, visando além das ações de segurança (prevenção, mitigação e repressão) a fundamentação de proposição de políticas públicas para a melhoria da qualidade de vida. A pesquisa, portanto, buscou responder ao seguinte questionamento: a implantação de sistemas de tecnologia voltados à coleta de dados e produção de conhecimento pela atividade de inteligência de segurança pública favorece a gestão da segurança pública no âmbito do município?

Para tanto, o objetivo geral da pesquisa foi analisar a atividade de inteligência de segurança pública e os aspectos do ecossistema que compõe a chamada *smart city*, identificando uma arquitetura de sistemas que seja aplicável ao contexto. E como objetivos específicos: referenciar bases teóricas da atividade de inteligência de segurança pública, trazendo um breve histórico da atividade no Brasil e a sua regulamentação, apresentar os conceitos aplicáveis ao tema das cidades inteligentes e experiências da literatura e os respectivos critérios utilizados para a caracterização de uma cidade inteligente e, ainda, levantar possíveis sistemas e dispositivos que podem ser utilizados pela inteligência de segurança pública, como parte da arquitetura de uma cidade inteligente, destacando os seus desafios e potencialidades.

O primeiro capítulo deste trabalho se propõe a tratar da atividade de inteligência de segurança pública e para tanto abordará os conceitos e dinâmicas operacionais da atividade de inteligência, e, na sequência um breve histórico da institucionalização dos serviços de inteligência no Brasil, sua trajetória, com destaques para os seus marcos normativos. No segundo capítulo, a proposta é o estudo da chamada cidade inteligente ou Smart *City*, que ultimamente se transformou em tema de grande importância nas discussões sobre o desenvolvimento urbano sustentável, no mundo e no Brasil. Sob o tema das cidades inteligentes, são trazidos conceitos aplicáveis e experiências da literatura que apontam os critérios para se caracterizar uma cidade denominada inteligente. No último capítulo, o presente trabalho buscará apresentar exemplos de ferramentas que fazem parte do ecossistema da cidade denominada inteligente, os quais podem

ser utilizados pela inteligência de segurança pública, reforçando os desafios e perspectivas deste novo momento das cidades e a importância da atividade de inteligência de segurança pública, ou seja, de que forma ela poderá contribuir para um melhor desenvolvimento das cidades.

A segurança pública é dever do Estado, direito e responsabilidade de todos. Nesta perspectiva, percebemos o impacto sobre a qualidade de vida das pessoas, bem como do aspecto da sustentabilidade, impulsionada pela atividade de inteligência associada no contexto das cidades inteligentes (*smart cities*), onde o emprego de novas tecnologias, processos e inovação são incorporados a todo instante e compõem o novo cenário das cidades, a exemplo dos sistemas de videovigilância, de leitura de placas veiculares, de câmeras com reconhecimento facial, gerando um enorme volume de dados coletados que precisam ser analisados e interpretados pela atividade de inteligência.

A busca pelo aprimoramento da qualidade de vida das pessoas, por meio da implementação e consolidação de cidades inteligentes, representa a convergência dos interesses coletivos, conectados pelo uso da inovação e das tecnologias de informação e comunicação.

As cidades estão vivendo verdadeiras transformações por conta do mundo digital cada vez mais conectado, inteligente, demandando por parte do poder público, uma mudança na forma de governar (governança). Um dos desafios é acompanhar a atualização tecnológica onde tradicionalmente a burocracia se faz presente, equipar-se de forma suficientemente adequada de informações, qualificações e tecnologias capazes e fazer frente aos cenários adversos e responder de forma satisfatória as demandas antigas e novas, com vistas ao seu desenvolvimento.

Assim, uma cidade inteligente também requer ação assertiva, eficiente e rápida dos gestores tanto no uso da inteligência quanto da contrainteligência de segurança pública.

## 1.1 ASPECTOS METODOLÓGICOS

A despeito de uma disponibilidade considerável de bibliografia sobre os aspectos transversais do presente estudo, detectamos certa escassez de literatura sobre o tema quando o associamos a inovação, tecnologia e políticas públicas,

vinculadas ao processo de produção de conhecimento da atividade de inteligência, deduzindo pela aplicação dos sistemas e aproveitamento pela atividade de inteligência de segurança pública e mediante o estudo que se caracteriza como descritivo e explicativo.

Busca-se o embasamento teórico na revisão da literatura, coletando dados e informações em fontes primárias e secundárias, destacando-se livros, artigos científicos, legislações em âmbito nacional e organizacional e na Doutrina Nacional de Inteligência de Segurança Pública (DNISP).

A análise e interpretação dos resultados se darão através da identificação de alguns sistemas que estão sendo implantados nas cidades, os quais possuem aplicação de inteligência artificial que visam otimizar as rotinas, proporcionando ao gestor um *overwiew* da cidade, bem como o monitoramento detalhado de pontos estratégicos, numa espécie de raio-x da cidade, tornando-a mais visível para a segurança pública e possibilitando o compartilhamento dos dados com as diversas agências de segurança pública.

Quanto ao método utilizado para a coleta de dados, este é qualitativo e documental.

A classificação desta pesquisa é do tipo descritiva-exploratória tendo em vista a necessidade e possiblidade de intervenção ao final de uma proposta de implantação de uma arquitetura de sistemas de vigilância nas cidades, a exemplo, do cercamento eletrônico. Serão apresentados, portanto, alguns exemplos de sistemas que podem ser implantados nas cidades como parte da arquitetura de uma cidade inteligente e que podem ser utilizados pela atividade de inteligência de segurança pública.

# 2 ESTADO, SOCIEDADE E ATIVIDADE DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA

Neste capítulo, iremos descrever e articular a base conceitual, a evolução e reflexão sobre os temas que envolvem o título em comento.

## 2.1 ATIVIDADE DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA

A atividade de inteligência compreende a obtenção e o processamento de um conjunto de ativos informacionais que são de interesse de uma organização ou entidade visando a produção de determinados conhecimentos que possam vir a gerar influências em determinados juízos, ações e comportamentos, em especial, quanto às influências nos processos decisórios, voltados para as pessoas, à sociedade e ao Estado (PAULA, 2013, p. 35).

Assim, se desde os tempos mais remotos se buscou obter conhecimentos capazes de favorecer vantagens nos mais diversos campos: territorial, diplomático, econômico, geopolítico, com posições de prevalência, bem como atuações decisivas em campos de batalha, atualmente, no cenário das grandes transformações tecnológicas, com uso da tecnologia da informação em alta implementação, as atividades de inteligência e de contrainteligência vêm se fortalecer com os novos recursos e abrangência também proporcionadas pela Tecnologia da Informação e Comunicação, seguindo acompanhando, portanto, o desenvolvimento da sociedade (PAULA, 2013, p. 35).

Este capítulo, portanto, se propõe a tratar da atividade de inteligência de segurança pública e para tanto abordará os conceitos e dinâmicas operacionais da atividade de inteligência, e apresentará um breve histórico da institucionalização dos serviços de inteligência no Brasil, sua trajetória, com destaques para os seus marcos normativos.

### 2.1.1 Síntese Histórica da Atividade de Inteligência

No que tange às bases históricas, faremos um breve apanhado sobre a atividade de inteligência.

A necessidade de conhecer confunde-se com a própria história da humanidade. No livro do Gênesis, por exemplo, observam-se passagens que reportam sobre a busca de informações. Noé, a partir de sua Arca, remete uma

pomba ao prazer dos ventos em busca de terra firme. Moisés, assim como seu sucessor Josué, envia agentes à Terra Prometida, para obter informações sobre os hábitos e os costumes do povo que lá vivia (RÊGO, 2012, p. 30).

A Bíblia cristã é citada como uma das fontes mais antigas sobre a atividade. No Antigo Testamento há, por exemplo, a passagem em que Moisés teria enviado espiões à Terra de Canaã, no que pode ter sido uma das primeiras "ordens de busca" que se tem registro (SILVA; ROLIM, 2017, p. 150).

Desde os primórdios da civilização humana, a atividade de inteligência norteou a tomada de decisões buscando sempre uma avaliação precisa, quer no campo militar, quer no campo político, para um planejamento estratégico eficaz. Alguns personagens, no transcorrer da história, tornaram-se líderes destacados, tais como: Moisés (Livro do Êxodo), SunTzu (A Arte da Guerra), Maquiavel (O Príncipe), Mao Tse-Tung – estrategista de guerra e guerrilha e Napoleão Bonaparte – que deu ênfase às informações de combate, bem como foi o precursor do Estado-Maior. (RODRIGUES *apud* SILVA; ROLIM, 2017, p. 150)

O general chinês Sun Tzu, século IV a.C, dedica um capítulo de seu livro A Arte da Guerra para falar sobre a importância da Atividade de Inteligência para se alcançar vitórias, destacando que "se um soberano iluminado e seu comandante obtém a vitória sempre que entram em ação e alcançam feitos extraordinários, é porque eles detêm o conhecimento prévio e podem antever o desenrolar de uma guerra. [...] Este conhecimento deve ser obtido das pessoas que, claramente, conhecem as situações do inimigo. (TZU, 2007, p. 128 *apud* SILVA; ROLIM, 2017, p. 151).

Na Europa moderna, a partir do século XVI, surgiram as primeiras organizações permanentes e profissionais de Inteligência e de segurança para atender à necessidade que reis e governantes têm de demonstrar seu poder, diante de sua população e perante outros Estados, por intermédio da obtenção constante de informações, que com o tempo as tecnologias foram permitindo obter informações mais seguras. E face a demanda de novas necessidades, criou-se *staffs* permanente nas forças armadas, responsáveis pelo planejamento e pelo suporte de informações que pudessem auxiliar os seus comandantes na tomada de decisão (SILVA; ROLIM, 2017, p. 151).

Conforme Gonçalves (*apud* SILVA; ROLIM, 2017, p. 152): "O século XX foi denominado o "Século dos espiões" devido à intensidade, abrangência, profissionalização e popularidade da atividade".

Silva e Rolim (2017, p. 152) explanam que:

> No Século XX, assim como o mundo alcançou um grau sem precedentes no desenvolvimento das relações internacionais, também houve o surgimento e o fortalecimento dos serviços secretos, das técnicas de reunião de dados e do conhecimento produzido como inteligência.

Nas últimas duas décadas, porém, o número de informações cresceu mais do que nos últimos 5 (cinco) mil anos e o homem sempre está a pesquisar dados e informações, procurando por segurança no seu dia-a-dia (MEDEIROS, ([2009], p. 1).

Os Serviços de Inteligência, portanto, produzem conhecimentos sobre conflitos desde que foram criados e institucionalizados. A natureza dessas disputas, entretanto, sofreu transformações ao longo do tempo, principalmente após as guerras mundiais do século XX e, mais recentemente, com o fim da Guerra Fria. A análise de conflitos se desenvolveu nesse contexto, reunindo estudos sobre guerra e paz, diplomacia, negociação, prevenção e gerenciamento de conflitos.

### 2.1.2 A Atividade de Inteligência no Brasil

A atividade de inteligência no Brasil teve início no governo democrático do Presidente Washington Luís (1926-1930), que instituiu em 1927 o Conselho de Defesa Nacional (CDN), mediante o Decreto nº 17.999, de 29 de novembro de 1927. O Conselho de Defesa Nacional era um órgão de caráter consultivo, reunia-se ordinariamente duas vezes por ano, e tinha a função de estudar e coordenar as informações sobre todas as questões de ordem econômica, bélica e moral relativas à defesa da Pátria. (SILVA; ROLIM, 2017, p. 153)

De acordo com Buzanelli (2004, p. 1): "em 1934, foram criadas as Seções de Defesa Nacional (SDN) nos Ministérios Civis, vinculadas ao Conselho de Defesa Nacional (CDN), sendo o mais antigo ancestral do que é atualmente o SISBIN".

E, conforme Buzanelli (2004, p. 1):

> apesar de ser criada por um governo civil e democrático, a atividade de inteligência, como em outros países, também no Brasil nasceu sob forte influência militar, de vez que associada ao processo de tomada de decisões e de assessoramento típico de estruturas do estado-maior.

A implantação da atividade de inteligência no Brasil, foi consequência direta da influência exercida pelos sucessivos movimentos modernizadores que tonificaram, a partir da segunda década do Século XX, as instituições militares brasileiras, em especial o Exército Brasileiro. Entre os movimentos, têm destaque os chamados *Movimento dos Jovens Turcos*, a *Missão Indígena* e a *Missão Francesa*. (BUZANELLI, 2004, p. 1)

De acordo com Buzanelli (2004, p.1):

> O Movimento dos Jovens Turcos, composto por oficiais que haviam estagiado no Exército Imperial alemão, nos anos anteriores a I Guerra Mundial, e que, no seu retorno, tiveram papel central na criação da revista "A defesa nacional", em 1911, de papel decisivo na evolução do pensamento estratégico brasileiro. A Missão Indígena, constituída por jovens oficiais brasileiros que lograram introduzir importantes modificações na instrução e organizações militares. A Missão Francesa, composta por prestigiosos oficiais do Exército Francês, que, no período entre guerras, durantes vinte anos (de 1920 a 1940), contribuiu de maneira fundamental para a consolidação dos processos de formação e aperfeiçoamento de oficiais e graduados - sobretudo com o fortalecimento da Escola Militar do Realengo e da Escola de Aperfeiçoamento de Oficiais-; organização de grandes unidades – as chamadas brigadas estratégicas-; das divisões militares regionais; do funcionamento de estruturas de comando e controle e do trabalho de estado-maior; da consolidação da aviação militar; e da atividade de inteligência militar, então com o foco voltado para as chamadas informações de combate.

Ainda, segundo Buzanelli (2004, p.1):

> mais tarde com a participação brasileira na campanha da Itália, no período de 1943 a 1945, as informações militares ganharam posição de realce, com a criação em 1944 do Serviço de Informações e Contrainformações (SIC) da Força Expedicionária Brasileira (FEB), subordinado à 2ª seção do estado-maior da1ª Divisão de Infantaria Expedicionária (DIE).

Somente em 1946, no período da Guerra Fria, é que se criou um órgão específico para tratar das atividades de Informações no Brasil, o Serviço Federal de Informações e Contrainformações (SFICI), que, contudo, somente foi efetivado 12 anos depois, marcando o desinteresse pela temática numa época da política marcada pelo populismo (GONÇALVES *apud* SILVA; ROLIM, 2017, p. 154).

Conforme Freire, Furlan e Silveira (2018, p. 68):

> em 1946, o presidente Dutra, defendendo a ideia de um órgão de apoio presidencial, criou por Decreto o Serviço Federal de Informações e Contrainformações (Sfici), vinculado ao Conselho de Segurança Nacional (CSN). Desde então vários órgãos se sucederam, acompanhando a conjuntura nacional e internacional.

De acordo com Medeiros ([2009], p. 1), no final da década de 1950, o Serviço Federal de Informações e Contrainformações (SFICI) consolidou-se como principal instrumento de informação do Estado brasileiro. Seria sucedido pelo Serviço Nacional de Informações (SNI). Hoje a atividade de inteligência é exercida pela Agência Brasileira de Inteligência (ABIN).

Para Buzanelli (2004, p. 3), significativos avanços setoriais foram alcançados no período dos governos militares, sobremaneira no que se refere à organização, técnicas e doutrina, cabendo mencionar a notável influência doutrinária exercida pela Escola Superior de Guerra (ESG), no que concerne à formulação do pensamento estratégico nacional aplicado à inteligência.

De acordo, ainda, com Buzanelli (2004, p. 3):

> igualmente importante a influência metodológica recolhida de modelos proporcionados por órgãos de inteligência estrangeiros, em especial a Agência Central de Inteligência (CIA), particularmente no que concerne à obtenção e produção de inteligência estratégica e à formulação de uma doutrina brasileira de inteligência.

Destaca-se neste período o Sistema Nacional de Informações (SisNi), precursor do atual SISBIN.

O Serviço Nacional de Informações passou, a partir da criação do SisNI da Escola Nacional de Informações (EsNI) e com a elaboração do Plano Nacional de Informações (PNI), a exercer papel de crescente relevância na condução dos assuntos de governo e na defesa do modelo implantado pelo Movimento de março de 1964. (BUZANELLI, 2004, p. 5)

Com o Governo Geisel, a partir de 1974, seguiu-se a adoção de importantes medidas em política externa (o Brasil ficou mais independente em relação aos blocos de poder – como o reconhecimento da independência de Angola e Moçambique em 1975, a denúncia do Acordo Militar Brasil-Estados Unidos da América, em 1976; e o Acordo de Cooperação Nuclear com a República Federal Alemã (RFA), também em 1976), o SNI passou a ocupar-se também de temas internacionais, de modo a assessorar as decisões governamentais em assuntos não tratados pelos canais de relações exteriores convencionais. (BUZANELLI, 2004, p. 5)

Em 1971, foi criada a Escola Nacional de Informações (ESNI) que seguia a doutrina utilizada pela CIA e FBI. Após 1984, com a abertura política, o SNI

permaneceu funcionando até 1990, sendo extinto com o fim do mandato do Governo Sarney. (FREIRE; FURLAN; SILVEIRA, 2018, p. 64)

Conforme Buzanelli (2004, p. 4):

> A EsNI, criada em 31 de março de 1971 pelo Decreto 68.488/71 notabilizou pelos padrões de excelência atingidos, conduzindo o SNI e o SisNI à autossuficiência em matéria de pesquisa, formação e aperfeiçoamento de recursos humanos para a atividade de inteligência, alcançando patamares comparáveis aos serviços congêneres dos EUA e União Soviética. "Laboratórios químicos, fotográficos, eletrônicos, balísticos e um centro de pesquisa para a segurança das comunicações – este que resultou de grande importância para o desenvolvimento da indústria eletrônica no país, inclusive no que concerne ao sistema de televisão a cores (Palm-m), implantado em nosso país no início da década de setenta, foram ali estabelecidos.

Quanto à Escola Nacional de Informações (ESNI), Buzanelli (2004, p.4) afirma que: "em sua profícua existência, no período de abril de 1971 a março de 1990, promoveu inúmeros cursos de formação, especialização e aperfeiçoamento não só para componentes do SisNi, mas também para oficiais de inteligência de nações amigas".

De acordo com Buzanelli (2004, p. 4):

> inúmeros manuais técnicos, de instrução e de procedimentos foram editados, tendo adotado estudos de cunho doutrinário produzido no exterior como os contidos nas obras "Informações estratégicas", de Sherman Kent e "A produção de informações estratégicas", do Almirante Washington Platt.

Em março de 1985, com a posse de José Sarney, primeiro Presidente da República civil, após vinte e um ano de governo exercido por militares e na prática um governo de transição, persistiu o Serviço Nacional de Informações (SNI) em situação de proeminência e grande prestígio, dando suporte ao governo. (BUZANELLI, 2004, p. 5)

Conforme Buzanelli (2004, p. 5):

> Com o modelo em franca mudança, as prioridades da atuação da inteligência voltaram-se para temas relacionados à corrupção, e a partir de 1989, ao terrorismo internacional, ao narcotráfico, proliferação de armas e a outras formas de crimes transnacionais já pressagiando temas que hoje são prioritários a todos os serviços congêneres.

Iniciando uma fase de transição pós-SNI, em 15 de março de 1990, o então Presidente Fernando Collor, ao ser empossado e cumprindo promessa de campanha extinguiu o Serviço Nacional de Informações (SNI) e, por extensão, o SISNI. Em seu lugar foi criada a Secretaria de Assuntos Estratégicos (SAE) e, na

estrutura desta, o Departamento de Inteligência (DI/SAE), com uma estrutura bastante diluída e com outras atividades de natureza estratégica (BUZANELLI, 2004, p. 5)

Embora o serviço de inteligência não tenha conseguido recuperar seu antigo prestígio, mostrou-se bem-sucedido em assuntos importantes e de relevância para o governo como, entre estes, as previsões de derrocada da União Soviética, resultante dos processos de "*glasnost*" e da "*perestroika*"; e o acompanhamento do Conflito no golfo Pérsico, no período de agosto de 1990 a março de 1991, promovido por uma central de monitoramento de acontecimentos e previsão de cenários em tempo real. A partir da extinção do SisNI, verificou-se um verdadeiro "apartheid institucional" entre os vários órgãos, especialmente os militares e a DI/SAE, com grave prejuízo para a atividade de inteligência como um todo. (BUZANELLI, 2004, p. 6)

De acordo com Silva e Rolim (2017, p. 152):

> no Brasil, durante muito tempo, empregou-se o vocábulo Informações para reportar ao meio para orientar e assessorar o governo em questões de defesa nacional, no entanto, após a extinção do Serviço Nacional de Informações (SNI) e a Criação da Secretaria de Assuntos Estratégicos (SAE), em 1990, o país passou a adotar o termo Inteligência.

Durante a primeira metade da década de 1990, a atividade de inteligência no Brasil permaneceu desprestigiada e o fantasma do SNI e do autoritarismo continuavam a assombrar o debate sobre o papel da inteligência no regime democrático. No entanto, a comunidade de inteligência militar e criminal continuaram atuando, fortalecendo suas respectivas áreas.

Em 19 de novembro de 1992, no Governo Itamar Franco, editou-se a Lei 9.490/92, extinguindo-se o DI/SAE e criando a Subsecretaria de Inteligência da Secretaria de Assuntos Estratégicos (SSI/SAE), não mudando a estrutura na prática. (BUZANELLI, 2004, p. 6)

Em 1992, surge a Subsecretaria de Inteligência, que funcionou até 1999, com a criação da Agência Brasileira de Inteligência (ABIN). (PAULA, 2013, p. 49)

Fruto de um grupo de trabalho constituído em 1997, a Lei nº 9.883, de 07 de dezembro de 1999, criou a Agência Brasileira de Inteligência (ABIN) e o instituiu o Sistema Brasileiro de Inteligência (SISBIN) (BRASIL, 1999, p. [1]). A ABIN foi criada com o intuito de ser um órgão de inteligência adequado aos padrões do regime democrático, com estrita obediência às leis, aos princípios constitucionais, aos direitos e às garantias individuais (SILVA; ROLIM, 2017, p. 156).

De acordo com Buzanelli (2004, p. 7):

> mais tarde, em 1999, a Subsecretaria de Inteligência teve seu status elevado para Secretaria de Inteligência (SI) seguindo desde 1996, subordinada à Casa Militar da Presidência da República, transformada em setembro de 1999 em Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

### 2.1.3 O Sistema e os Subsistemas de Inteligência no Brasil

A lei 9.883/99 define a atividade de inteligência como:

> a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado (BRASIL, 1999, 1º, § 2º).

A Contrainteligência, por sua vez, é definida como "a atividade que busca neutralizar a inteligência adversa", conforme a Lei 9.883/99 (BRASIL, 1999, art. 1, § 3º).

Quanto a constituição do Sistema Brasileiro de Inteligência, traz o art. 2º, da referida lei (Lei nº 9.883/1999) que:

> são 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, na forma de ato do Presidente da República (BRASIL, 1999, p. [1]).

A atividade de inteligência na área de segurança é regulamentada pelo Decreto nº 3.695, de 21 de dezembro de 2000, que criou o Subsistema de Inteligência de Segurança Pública (SISP), no âmbito do SISBIN, com o objetivo de coordenar e integrar a atividade de Inteligência de Segurança Pública no Brasil (BRASIL, 2000, p. [1]).

O Decreto nº 4.376, de 13 de setembro de 2002, por sua vez, dispõe sobre a organização e o funcionamento do SBI (Sistema Brasileiro de Inteligência), definindo os órgãos que compõem o sistema, o qual tem a Agência Brasileira de Inteligência (ABIN) como órgão central, sendo atualizado periodicamente, com a última atualização dada pelo Decreto nº 10.759, de 2021 (BRASIL, 2002, 2021).

O Sistema Brasileiro de Inteligência, de acordo com o Parágrafo 1º, do art. 2º, da Lei nº 9.883, de 07 de dezembro de 1999 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 (BRASIL, 1999, art. 2).

Conforme Freire, Furlan e Silveira (2018, p. 66) a Secretaria Nacional de Segurança Pública SENASP integra o SISP como órgão central, sendo o SISP um aglomerado de Subsistemas e Agências de Inteligência no âmbito da União e tendo, ambos, um padrão doutrinário, metódico e sistemático em comum.

Importante destacar a Doutrina Nacional de Inteligência de Segurança Pública (DNISP), documento normativo, criado pela Portaria nº 22, de 23 de julho de 2009), da SENASP/Ministério da Justiça (BRASIL, 2009, p. [1]), em conformidade com o art. 3º do Decreto nº 3.695, de 21 de dezembro de 2000 (BRASIL, 2000, p. [1]),), que trata da criação do SISP, sendo este subordinado à Agência Brasileira de Inteligência (ABIN).

A DNISP, teve sua primeira edição no Rio de Janeiro, no ano de 2009. Sendo que sua versão mais atual, foi revisada pelo Comitê Nacional de Revisão da DNISP, nos anos de 2013 e 2014.

O SISP organiza a atividade de Inteligência de Segurança Pública de forma integrada, com ações técnicas, metódicas e sistêmicas, a fim de produzir e proteger o conhecimento e fornecer subsídios no apoio decisório, facilitando o arranjo, o planejamento, a realização, a gestão e o monitoramento de Políticas de Segurança Pública. (FREIRE; FURLAN; SILVEIRA, 2018, p. 68)

Na sequência cronológica, tratando da regulamentação do sistema de inteligência, temos o Decreto 8.793, de 29 de junho de 2016, que fixa a Política Nacional de Inteligência (PNI), tendo o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) como coordenador das atividades de inteligência no âmbito da administração pública federal (BRASIL, 2016, p. [1]). Atualmente, a coordenação das atividades de inteligência de segurança pública está sob a responsabilidade da Agência Brasileira de Inteligência (ABIN) (Decreto nº. 11.426, de 1º de março de 2023). (BRASIL, 2023 p. [1]))

A Política Nacional de Inteligência (PNI), de acordo com o texto anexo do Decreto 8.793, de 29 de junho de 2016 é:

> é documento de mais alto nível de orientação da atividade de Inteligência no País, foi concebida em função dos valores e princípios fundamentais consagrados pela Constituição Federal, das obrigações decorrentes dos tratados, acordos e demais instrumentos internacionais de que o Brasil é parte, das condições de inserção internacional do País e de sua organização social, política e econômica (BRASIL, 2016, p. [1]).

A PNI define os parâmetros e limites de atuação da atividade de Inteligência e de seus executores e estabelece seus pressupostos, objetivos, instrumentos e diretrizes, no âmbito do Sistema Brasileiro de Inteligência (SISBIN).

De acordo com o texto do Decreto 8.793, de 29 de junho de 2016, para a implementação da Política Nacional de Inteligência (PNI), adotam-se os seguintes conceitos:

> Atividade de Inteligência: exercício permanente de ações especializadas, voltadas para a produção e difusão de conhecimentos, com vistas ao assessoramento das autoridades governamentais nos respectivos níveis e áreas de atribuição, para o planejamento, a execução, o acompanhamento e a avaliação das políticas de Estado. A atividade de Inteligência divide-se, fundamentalmente, em dois grandes ramos:
>
> I – Inteligência: atividade que objetiva produzir e difundir conhecimentos às autoridades competentes, relativos a fatos e situações que ocorram dentro e fora do território nacional, de imediata ou potencial influência sobre o processo decisório, a ação governamental e a salvaguarda da sociedade e do Estado;
>
> II – Contrainteligência: atividade que objetiva prevenir, detectar, obstruir e neutralizar a Inteligência adversa e as ações que constituam ameaça à salvaguarda de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado (BRASIL,2016, p. [1]).

A Lei nº 13.675, de 11 de junho de 2018 institui o Sistema Único de Segurança Pública (SUSP) cria Política Nacional de Segurança Pública e Defesa Social (PNSPDS), com a seguinte finalidade:

> Art. 1º [..] preservação da ordem pública e da incolumidade das pessoas e do patrimônio, por meio de atuação conjunta, coordenada, sistêmica e integrada dos órgãos de segurança pública e defesa social da União, dos Estados, do Distrito Federal e dos Municípios, em articulação com a sociedade (BRASIL, 2018, art. 1).

O Plano Nacional de Segurança Pública, por sua vez, é regulamentado pelo Decreto 9.630, de 26 de novembro de 2018.

Em 2021, temos a edição do Decreto 10.759, de 30 de julho de 2021 que "Altera o Decreto nº 4.376, de 13 de setembro de 2002, que dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência", trazendo a atualização dos membros que compõem o Sistema Brasileiro de Inteligência (SBI). (BRASIL, 2021, p. [1]).

O Decreto nº 10.777, de 24 de agosto de 2021, por sua vez, institui a Política Nacional de Inteligência de Segurança Pública (PNISP), com o objetivo de

estabelecer os parâmetros e os limites de atuação da atividade de inteligência de segurança pública no âmbito do Subsistema de Inteligência de Segurança Pública ( SISP), competindo à Diretoria de Inteligência da Secretaria de Operações Integradas do Ministério da Justiça e Segurança Pública a coordenação das atividades de inteligência de segurança pública no âmbito do SISP, que exercerá em cooperação com os órgãos e as entidades que integram o Sistema Brasileiro de Inteligência (BRASIL, 2021, p. [1]).

A Política Nacional de Inteligência de Segurança Pública (PNISP) (Decreto nº 10.777/2021), traz como pressupostos da atividade de inteligência em segurança pública, quais sejam: a) obediência à Constituição e as Leis; b) atividade de Estado de caráter permanente; c) atividade de assessoramento oportuno; d) atividade especializada; e) conduta ética; f) abrangência; g) gestão estratégica; h) interação entre as agências de inteligência; i) coordenação e controle; e j) sigilo (BRASIL, 2021, p. [1]).

O Decreto nº 10.777/2021, destaca os desafios do Estado no âmbito da aplicação da política nacional de inteligência de segurança pública:

> 3.5. O desenvolvimento das tecnologias da informação e das comunicações impõe a implementação e a utilização de instrumentos e técnicas avançadas de apoio que sejam capazes de analisar, com tecnologia de ponta e profissionais qualificados, as ações nocivas realizadas no espaço cibernético, considerada a migração massiva de práticas ilícitas e criminosas para esse espaço, o que tem tornado a sociedade mais vulnerável (BRASIL, 2021, p. [1]).

O Decreto 10.777, de 24 de agosto de 2021, reforça a necessidade da busca de soluções integradas e articuladas do SUSP na inteligência de segurança pública considerando as realidades regionais heterogêneas dos Estados, associada à extensão continental do Brasil (BRASIL, 2021, p. [1]).

Quanto as principais ameaças, assevera o Decreto nº 10.777/2021 como prioridades do Estado:

> o combate aos crimes violentos, ao crime organizado, a corrupção, a lavagem de dinheiro e evasão de divisas, as ações contrárias à segurança pública no espaço cibernético, as ações contrárias ao Estado Democrático de Direito e as ações contrárias à segurança de infraestruturas críticas com impacto na segurança pública (BRASIL, 2021, p. [1]).

No que tange as suas diretrizes (Decreto nº 10.777/2021), a Política Nacional de Inteligência de Segurança Pública estabelece que estas são: a) produzir conhecimento para o enfrentamento da criminalidade organizada e violenta; b)

aperfeiçoar as inteligências cibernética, financeira e de sinais; c) fomentar a integração da atividade de inteligência de Segurança Pública; d) subsidiar ações de preservação da ordem pública, da incolumidade das pessoas e do patrimônio e do meio ambiente; e) promover o respeito aos direitos humanos; f) garantir a proteção aos profissionais de inteligência; g) fortalecer a atividade de inteligência de segurança pública; h) fomentar o compartilhamento de informações com o Sistema Brasileiro de Inteligência; i) fomentar o compartilhamento de informações com as agências de inteligência do sistema prisional; j) estimular a produção de conhecimento destinada à prevenção e resposta a situações de emergência e a desastres (BRASIL, 2021, p. [1]).

Ainda, necessário destacar o Decreto nº 10.778, de 24 de agosto de 2021, que aprova a Estratégia Nacional de Inteligência de Segurança Pública, que tem o seguinte objetivo: “estabelecer os parâmetros e os limites de atuação da atividade de inteligência de segurança pública e de seus executores, no âmbito do Subsistema de Inteligência de Segurança Pública (SISP)” (BRASIL, 2021, p. [1]).

O recente Decreto nº 11.426, de 1º de março de 2023 (BRASIL, 2023 p. [1])), por sua vez, altera a regulamentação para determinar como órgão central do Sistema Brasileiro de Inteligência, passando a integrar a Casa Civil da Presidência da República.

> Art. 1º A Agência Brasileira de Inteligência - Abin, órgão integrante da Casa Civil da Presidência da República, criada pela Lei nº 9.883, de 7 de dezembro de 1999, é órgão central do Sistema Brasileiro de Inteligência e tem por competência planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País, obedecidas a política e as diretrizes estabelecidas em legislação específica (BRASIL, 1999, art. 1).

Aos órgãos e entidades responsáveis pela atividade de inteligência de segurança pública compete acompanhar e avaliar as conjunturas interna e externa, com visitas a identificar fatos ou situações que possam resultar em ameaças e oportunidades no âmbito da segurança pública, por meio de uma leitura de cenários, que possibilitem ao tomador de decisão adotar as medidas adequadas, voltadas à preservação da ordem pública, da incolumidade das pessoas e do patrimônio e do meio ambiente.

Em Santa Catarina, a Diretoria de Informação e Inteligência (DINI) é a Agência Central integrada à Secretaria de Segurança Pública, sendo a responsável pela atividade de coletar, analisar, produzir e difundir a informação, assim como

realizar análise criminal, estatística, geoprocessamento e operações de inteligência e contrainteligência. A DINI trabalha integrada com as instituições estaduais, sendo composta por integrantes da Polícia Civil, Polícia Militar e profissionais especialistas de outras instituições do Estado (FREIRE; FURLAN; SILVEIRA, 2018, p. 67).

A Diretoria de Informação e Inteligência (DINI) realiza atividades de coleta de informações, bem como de análise criminal, estatística, geoprocessamento e operações de inteligência e contrainteligência de segurança pública.

### 2.1.4 Reflexão sobre a Inteligência de Segurança Pública no Âmbito Municipal

A Lei nº 13.675, de 11 de junho de 2018 institui o Sistema Único de Segurança Pública (SUSP) e cria Política Nacional de Segurança Pública e Defesa Social (PNSPDS), traz que: “a segurança pública é dever do Estado e responsabilidade de todos, compreendendo a União, os Estados, o Distrito Federal e os Municípios, no âmbito das competências e atribuições legais de cada um” (BRASIL, 2018, art. 2).

No âmbito do município, a legislação vem atribuindo aos órgãos municipais a incumbência de execução das ações de segurança, com a criação, por exemplo das Secretarias Municipais de Segurança Pública, bem como, com as guardas municipais, cuja criação é facultativa, que além da segurança do patrimônio público do município, atuam em articulação com os demais órgãos e entidades, também na prevenção e repressão à criminalidade.

A Lei Federal 13.675, de 11 de junho de 2018, em seu artigo 3º que compete aos Estados, ao Distrito Federal e aos Municípios:

> estabelecer suas respectivas políticas, observadas as diretrizes da política nacional, especialmente para análise e enfrentamento de riscos à harmonia da convivência social, com destaque às situações de emergência e aos crimes interestaduais e transnacionais (BRASIL, 2018, p. [1]).

Assim, o município, necessita articular-se com os demais órgãos de segurança estaduais e federais e desenvolver, de acordo com a Declaração dos Direitos Humanos, projetos, programas e políticas públicas no âmbito de sua competência, com o objetivo de cumprir com suas finalidades estabelecidas em lei municipal.

De acordo com o Decreto nº 10.778, de 24 de agosto de 2021, que aprova a Estratégia Nacional de Inteligência de Segurança Pública (ENISP) (ANEXO):

> A atividade de inteligência de segurança pública figura como uma importante ferramenta e deve cuidar do desenvolvimento de técnicas e processos capazes de analisar grande volume de dados, por meio de profissionais qualificados e soluções tecnológicas e contribuir para atender ao anseio social por um País mais seguro. (BRASIL, 2021, p. 2)

Neste contexto, a tecnologia utilizada pelas cidades inteligentes, ou seja, os sistemas e dispositivos que conectam as relações da sociedade (pessoa/IoT, etc.) vêm otimizar, coletar, compilar, filtrar e analisar dados, favorecendo a atividade.

Conforme o Decreto 10.778, de 24 de agosto de 2021 (BRASIL, 2021, p. 4) ao tempo que temos uma evolução crescente das formas de se comunicar, oportunizando a consolidação da atividade de inteligência e o fortalecimento dos níveis de integração e intercâmbio e dados, por outro lado, o desenvolvimento das formas e comunicação também apresentam desafios à segurança e à atuação objetiva das instituições de inteligência de segurança pública, sobretudo pelo aumento do volume de dados produzidos, compartilhados e expostos. Destacando-se, assim, a importância de uma inteligência de segurança pública voltada para a ciência de dados, preparada para lidar com a coleta, busca, estruturação e análise de grandes volumes de dados.

É essencial, para além do senso comum, a compreensão de que a evolução da ciência, inovação e tecnologia, traz benefícios à qualidade de vida das pessoas, contudo, as organizações criminosas também usufruem desses benefícios, aliando a vantagem de agirem em conflito com a lei. Assim, a prevenção e o desenvolvimento de novas estratégias são igualmente essenciais ao enfrentamento de novas ameaças.

Para finalizar este capítulo, vamos apresentar um quadro contendo a síntese da evolução da atividade de inteligência no Brasil, com as normas que se considerou mais relevantes para o presente estudo:

**Quadro 1** - Síntese das normas sobre a atividade de inteligência no Brasil

| Ano | Marco Legal | Objeto | Observações |
|---|---|---|---|
| 1927 | Decreto nº 17.999, de 29.11.1927 | Criação do Conselho de Defesa Nacional (CDN) | * A inteligência no Brasil surgiu essencialmente por influência militar, com o objetivo de assessorar o apoio decisório após o ano de 1920. |
| 1934 | | Criação das Seções de Defesa Nacional (SDN) nos Ministérios Civis | |

| | | | |
|---|---|---|---|
| 1944 | | Criação do Serviço de Informações e Contrainformações (SIC), da Força Expedicionária Brasileira (FEB) | * Antes de 1940, excetuando-se a inteligência militar, a atividade de inteligência era realizada pela Polícia Política.<br>* Com o fim da 2ª Guerra Mundial, após o Governo Vargas, ficou evidenciada a importância da atividade de inteligência.<br>* Em 1946, o Presidente Dutra criou por Decreto o SFICI, vinculado ao CSN, e em 1964 o SFICI foi absorvido pelo SNI.<br>* A atividade de inteligência no regime militar passou a focar na reunião de dados sobre movimentos sociais no Brasil, objetivando a repressão.<br>* Após o golpe militar em 1964, as ações foram reforçadas sendo criado o Ato Institucional nº 5 – AI5.<br>*Houve uma sequência de Decretos criados pelo regime militar objetivando a censura à imprensa e o controle da liberdade de expressão, supostamente em defesa do Estado.<br>(FREIRE; FURLAN; SILVEIRA, 2018, p.63-68) |
| 1946 | | Criação do Serviço Federal de Informações e Contrainformações (SFICI). | |
| 1958 | | Efetivação do Serviço Federal de Informações e Contrainformações (SFICI). | |
| 1964 | Lei nº 4341, de 13.06.1964 | Criação do Serviço Nacional de Informações (SNI) | |
| 1967 | Decreto nº 60.182, de 03.02.1967 | Regulamenta o Serviço Nacional de Informações (SNI) | |
| | | I Plano Nacional de Desenvolvimento e (PND) I Plano Nacional de Segurança (PNS) | |
| 1970 | | I Plano Nacional de Informações (PNI) | |
| 1971 | | Criação da Escola Nacional de Informações (ESN)I | |
| 1972 | | Criação Plano Nacional de Informações (PNI) e do Sistema Nacional de Informação (SISNI) | |
| 1974 | | II – Plano Nacional de Informações | |
| 1981 | | III – Plano Nacional de Informações | |
| 1983 | Lei nº 7.102, de 20.06.1983 | Dispõe sobre segurança para estabelecimentos financeiros, estabelece normas para constituição e funcionamento das empresas particulares que exploram serviços de vigilância e de transporte de valores, e dá outras providências. | |
| 1990 | | Criação do Departamento de Inteligência (DI) e da Secretaria de Assuntos Estratégicos (SAE) | * Fim do SNI junto com o fim do mandato do Governo Sarney. |
| 1992 | Lei nº 9490/2992 | Criação da Subsecretaria de Inteligência (SSI) da Secretaria de | |

| | | | |
|---|---|---|---|
| | | Assuntos Estratégicos (SAE) | |
| 1999 | Lei nº 9.883, de 7.12.1990 | Criação do Sistema Brasileiro de Inteligência (SISBIN) e da Agência Brasileira de Inteligência (ABIN) | * A ABIN tem o objetivo de planejar e executar a atividade de inteligência no País, bem como assessorar o Presidente da República. |
| 2000 | Decreto nº 3,695, de 21.12.2000 | Regulamenta a atividade na área de Segurança Pública. Criou o Subsistema de Inteligência de Segurança Pública (SISP), no âmbito do SISBIN. | * O SISP – tem o objetivo de coordenar e integrar a atividade de inteligência de Segurança Pública no Brasil. |
| | | A Secretaria Nacional de Segurança Pública (SENASP) | A SENASP Integra o SISP, como órgão central, seno o SISP um aglomerado de Subsistemas e Agências de Inteligência no âmbito da União. |
| 2002 | Decreto nº 4.376, de 13.09.2002 | Dispõe sobre o Sistema Brasileiro de Inteligência (SBI) | |
| 2009 | Portaria nº 22, de 23.07.2009 | Cria a Doutrina Nacional de Inteligência e Segurança Pública (DNISP) | Foram editadas atualizações da DNISP, sendo a 4ª Edição de 2014 |
| 2012 | Lei nº 12.681, de 04.07.2012 | Institui o Sistema Nacional de Informações de Segurança Pública, Prisionais e sobre Drogas (SINESP) | |
| 2016 | Decreto nº 8.973, de 29.06.2016 | Fixa a Política Nacional de Inteligência (PNI) | O GSI/PR – Gabinete de Segurança Institucional da Presidência da República – coordena as atividades de inteligência |
| 2018 | Lei nº 13.675, de Jun. 2018 | Institui o Sistema Único de Segurança Público (SUSP) e cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS) | |
| 2018 | Decreto nº 9.489, de 30.08.2018 | Regulamenta a Lei 13.675/2018 – que trata da Política Nacional de Segurança Pública e Defesa Social (PNSPDS) | |
| 2018 | Decreto nº 9.491, de | Altera o Decreto nº 4.376, de 13 de setembro de 2002, que dispõe sobre a | |

| | | | |
|---|---|---|---|
| | 04.09.2018 | organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei nº 9.883, de 7 de dezembro de 1999. | |
| 2018 | Lei nº 13,756, de 12.12.2018 | Dispõe sobre o Fundo Nacional de Segurança Pública (FNSP) e sobre a destinação do produto da arrecadação das loterias. | |
| 2018 | Decreto nº 9.630, de 26.12.2018 | Institui o Sistema Nacional de Informações de Segurança Pública, Prisionais e sobre Drogas (SINESP) | |
| 2021 | Lei nº 14.155, de 27.05.2021 | Altera o Decreto-Lei nº 2.848, de 6 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos na forma eletrônica ou pela internet [...] | |
| 2021 | Decreto nº 10.759, de 30.07.2021 | Altera o Decreto nº 4.376, de 13 e setembro de 2002, que dispõe sobre a organização e o funcionamento o Sistema Brasileiro de Inteligência | |
| 2021 | Decreto nº 10.777, de 24.08.2021 | Institui a Política Nacional de Inteligência de Segurança Pública (PNISP) | Secretaria de Operações Integradas – Ministério da Justiça e Segurança Pública – Coordenação GSI - PR |
| 2021 | Decreto nº 10.778, de 24.08.2021 | Aprova a Estratégia Nacional de Inteligência de Segurança Pública (ENISP)- | A ENISP orientará a execução entre 2021 e 2025. |
| 2023 | Decreto nº 11.426, de 1º.03.2023 | Altera o Decreto nº 11.327, de 1º de janeiro de 2023, o Decreto nº 11.329, de 1º de janeiro de 2023, o Decreto nº 9.435, de 2 de julho de 2018, e o Decreto nº 4.376, de 13 de setembro de 2002, para integrar a Agência Brasileira de Inteligência à Casa Civil da Presidência da República. | A Agência Brasileira de Inteligência - Abin, órgão integrante da Casa Civil da Presidência da República, é órgão central do Sistema Brasileiro de Inteligência e tem por competência planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País. |
| 2023 | Decreto nº 11.491, de 12.04.2023 | Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, | |

| | | | |
|---|---|---|---|
| | | em 23 de novembro de 2001 | |

**Fonte**: A autora (2023).

# 3 ARTICULAÇÃO ENTRE INTELIGÊNCIA E SEGURANÇA PÚBLICA

O desenvolvimento da sociedade, impulsionado pelo uso de novas tecnologias, é acompanhado pelo aumento da mobilidade entre as diversas regiões do planeta. Esse cenário aponta para uma crescente preocupação com os crimes interestaduais e transnacionais. A cooperação entre as agências de inteligência de segurança pública se reveste, portanto, de uma característica imperativa de intercâmbio de dados, conhecimentos e boas práticas na realização de suas atividades.

Uso do Sistema de Inteligência de Segurança Pública, com acesso aos dados das diversas secretarias, monitoramento dos sistemas de um município até outro, vão ao encontro da tão desejada interoperabilidade sistêmica. A análise detalhada da criminalidade violenta, tanto a eventual quanto aquela associada a grupos criminosos organizados, representa uma questão cada vez mais premente de enfrentamento. Ações de inteligência podem contribuir tanto para o mapeamento e estudo das formas de transgressão realizadas sob violência, quanto para a identificação de pessoas, e análise de grupos organizados e a busca de elementos que permitam a repressão das práticas delitivas mais destacadas e cujo impacto social é mais patente. (Decreto nº 10.778/2021) (BRASIL, 2021, p. 4).

## 3.1 A INTELIGÊNCIA COMO ESTRATÉGIA DE ESTADO À SEGURANÇA

Conforme apresentado no sitio eletrônico Fórum Brasileiro de Segurança Pública ([2023], p. [1]):

> a Segurança Pública é um serviço público, baseado na prevenção e na repressão qualificada, com respeito à equidade, à dignidade humana e guiado pelo respeito aos Direitos Humanos e ao Estado democrático de Direito". A partir destes princípios, políticas de segurança pública ganham diversidade nos diferentes territórios e contextos.

A Segurança Pública é a atividade desenvolvida pelo Estado, por meio de várias instituições públicas, que visa garantir a normalidade, paz e harmonia social, assegurando os direitos e deveres individuais. A era da informação e do conhecimento exige que a sociedade e suas organizações ampliem suas estratégias e ações visando a construção de um ambiente social equilibrado e com o mínimo de conflitos, logo, as atividades de inteligência são fundamentais nesse processo (PAULA, 2013, p. 22).

A violência e a criminalidade são questões endêmicas arraigadas na sociedade desde o seu processo de formação e atinge a todos indistintamente.

A segurança sempre foi objeto de preocupação dos povos, desde a antiguidade mais remota. A necessidade de segurança pelos povos, surgiu com a própria humanidade "consubstanciada na proteção do grupo contra o ataque de animais ou de outros agrupamentos humanos" (MACHADO, 2000, p. 19).

As teorias políticas que explicam a origem e justificam a existência do Estado apontam que o fim principal deste é a garantia da coexistência pacífica entre indivíduos, com a prevenção e arbitramento de conflitos, e punição dos faltosos, atividades estas de que o Estado deve se fazer representar por órgãos devidamente instituídos.

Nesse sentido é possível falar na existência de "direitos de proteção" (Alexy), ou seja, de direitos que tem frente ao Estado o titular de um direito fundamental, para que aquele o proteja da intervenção de terceiros. Com efeito, ao passar de uma situação pré-estatal à situação estatal, o indivíduo renuncia à autotutela em troca da proteção estatal.

Desse modo, a ordem constitucional, para além de enunciar os direitos fundamentais, deve prover também os mecanismos institucionais que garantam a proteção desses direitos. Essa ampla gama de tarefas estatais destinadas a garantir o respeito aos direitos individuais básicos é referida na Constituição Federal brasileira, no que diz respeito ao rol de atribuições do Poder Executivo, como atividades atinentes à "segurança pública". (VAZ-FERREIRA; RODRIGUES, 2021, p. 34-44)

A Constituição Federal, no art. 144, traz que é "dever do Estado, direito e responsabilidade de todos. Cabe ao Poder Público, em cada esfera de governo – União, Estados, Municípios, com a participação da sociedade civil atuar conjuntamente em prol de uma segurança pública de qualidade, participativa e inclusiva (BRASIL, 1988, art. 144).

De acordo com Silva (2012, p. 111), pode se afirmar que:

> a segurança pública consiste numa situação de preservação ou restabelecimento dessa convivência social que permite que todos gozem de seus direitos e exerçam suas atividades sem perturbação de outrem, salvo nos limites de gozo e reivindicações de seus próprios direitos e defesa de seus legítimos interesses".

É neste contexto, onde é dever do Estado a preservação da Ordem Pública e permeado por um cenário de constantes mudanças, que a atividade de inteligência vem acompanhando o crescimento e o desenvolvimento da humanidade, ao longo de sua evolução histórica. A inteligência possui inúmeras aplicações e, cada vez mais, é utilizada como uma ferramenta para potencializar as vantagens estratégicas e competitivas, frente aos novos desafios que, paralelamente, também acompanham as mudanças nos diversos campos do conhecimento.

A temática da “Segurança Pública” que, até então, contara tão somente com menções indiretas nas Constituições brasileiras, na Constituição Federal (BRASIL, 1988, art.144), passa a ter previsão normativa expressa no art. 144.

De acordo com Cepik (2003, p. 28 *apud* MOTA *et al.* 2018, p. 137), a atividade de inteligência, por sua vez, não está expressa na Constituição Federal e os governantes ao se depararem com temas afetos à segurança nacional, tendem a justificar institucionalmente e a delimitar as funções das forças armadas, das polícias e dos serviços de Inteligência, com lastro na clássica concepção de que estes três ramos de atividades estatais caminham conjunta e complementarmente.

De acordo com a Lei nº 9.883, de 7 de dezembro de 1999, que institui o SISBIN e cria a ABIN, art. 1º, § 1º:

> O Sistema Brasileiro de Inteligência tem como fundamentos a preservação da soberania nacional, a defesa do Estado Democrático de Direito e a dignidade da pessoa humana, devendo ainda cumprir e preservar os direitos e garantias individuais e demais dispositivos da Constituição Federal, os tratados, convenções, acordos e ajustes internacionais em que a República Federativa do Brasil seja parte ou signatário, e a legislação ordinária (BRASIL, 1999, art.1, § 1).

A atividade de inteligência foi empregada ao longo da história e teve um grande impulso, nas áreas militares, especialmente durante as duas grandes guerras, no entanto ainda é pouco compreendida e fica mais adstrita as Instituições militares e intimamente ligada aos chefes de estado.

Já, de acordo com Woloszyn (a*pud* FREIRE, FURLAN E SILVEIRA, 2018, p. 59):

> a atividade de inteligência ao longo da história humana foi utilizada como ferramenta para se obter poder e domínio sobre os povos, porém, com a diferença que na era contemporânea a informação é disseminada em larga escala. Ao longo do tempo, a atividade de inteligência tem sido constante e contínua. Historicamente, ela sempre esteve intimamente ligada às guerras, tendo seu ápice de utilização ocorrido na segunda Guerra Mundial.

Destacando que há pouca literatura nacional sobre o serviço de inteligência no Brasil e menos ainda normas específicas de regulamentação e controle, inclusive no âmbito internacional que trate sobre o Brasil, os autores Mota *et al.* (2018, p. 137), posicionam-se trazendo que essa frágil regulamentação reflete nos mecanismos de controle dos órgãos responsáveis pela atividade, concluindo pela

> necessidade de refazer um arcabouço jurídico que permita tanto uma atuação efetiva dos serviços de inteligência quanto ao seu efetivo controle, na medida em que a legalidade e a legitimação, poder e controle andam e devem realmente andar juntos em qualquer Estado democrático, que por outro lado, não deve prescindir de fortes estruturas para assessoramento das decisões estratégicas e para a elaboração das políticas públicas vetoriais (MOTA *et al*. 2018, p. 1370.

No entanto, podemos afirmar que a Atividade de Inteligência de Segurança Pública, vem se estruturando em termos normativos, com recente Decretos que instituem a Política Nacional de Inteligência de Segurança Pública, ampliam e definem a composição do Sistema Nacional de Inteligência, onde está inserido o subsistema da Inteligência de Segurança Pública.

Em decorrência das necessidades e peculiaridades da segurança pública, foi criado o SISP, por meio do Decreto nº 3.695, de 21 de dezembro de 2000, com o objetivo de coordenar e integrar a atividade de inteligência desenvolvida pelas forças de segurança pública e de subsidiá-las no processo decisório. Desde então, a atividade de inteligência de segurança pública tem se destacado e, atualmente, tem fundamental importância para a implementação da PNSPDS e do Susp, instituídos pela Lei nº 13.675, de 11 de junho de 2018 (BRASIL, 2000, 2018).

Os autores Freire, Furlan e Silveira (2018, p. 69), trazem à luz que as principais finalidades da Inteligência em Segurança Pública (ISP) são auxiliar o gestor na tomada de decisão, de modo a fornecer ao gestor descrição minuciosa e suposição sobre os fatos da área de segurança pública; colaborar na relação e comunicação entre usuário e profissionais de ISP; apoiar o planejamento estratégico regional; fornecer informações importantes na prevenção e repressão e proteger o conhecimento.

Freire, Furlan e Silveira (2018, p. 70) citam o objetivo da Inteligência de Segurança Pública:

> A ISP busca auxiliar o processo decisório com base na produção de conhecimento, em nível político, estratégico, tático e operacional. O nível político refere-se ao desenvolvimento de políticas de segurança pública, o nível estratégico é relativo à implementação de políticas de segurança

> pública; o nível tático visa à execução de ações táticas para a implementação de políticas de segurança pública, e o nível operacional busca observar e apoiar o planejamento e a execução de ações operacionais.

As novas tecnologias disponíveis e as possibilidades de construção de redes de conhecimento favorecem a atividade de inteligência e permitem uma maior efetividade nas estratégias e nas ações, tanto no que diz respeito a prevenção e ao enfrentamento da violência e criminalidade quanto nos processos de defesa e promoção da cidadania (PAULA, 2013, p. 22-23)

No que se refere à atividade de Inteligência de Segurança Pública, como dito acima, esta não se encontra expressa na Constituição Federal, no entanto, a legislação nacional incumbiu-se de dar o caráter constitucional à atividade e ela é desenvolvida por diversos órgãos que atuam no campo da segurança, tais como exército, marinha, aeronáutica, as polícias estaduais e federal, inclusive no âmbito das secretarias municipais de segurança pública. Ou seja, é uma atividade que permeia atividades afetas à segurança do país.

## 3.2 CIDADES INTELIGENTES – *SMART CITIES*

Segundo a União Européia (*apud* FGV PROJETOS, [2019], p. [1]), Smart Cities são sistemas de pessoas interagindo e usando energia, materiais, serviços e financiamento para catalisar o desenvolvimento econômico e a melhoria da qualidade de vida.

### 3.2.1 Cidades Inteligentes (Smart Cities): Conceitos e Objetivos

De acordo com Santos Filho e Coêlho (2021, p. 69):

> o termo ‘Cidades inteligentes’, refere-se aos esforços e iniciativas que buscam melhorar os aspectos do funcionamento dos equipamentos, serviços, relações humanas e economia das cidades, com o uso da Tecnologia da Informação e Comunicação, buscando melhorar a eficiência ou diminuir o desperdício de recursos na cidade.

A discussão em torno deste assunto - *smart cities* ou “cidades inteligentes” - apresenta-se em âmbito global, destacando-se a grande preocupação e necessidade de se avançar no tema de como a tecnologia é usada em locais públicos e promoverá os princípios fundamentais, incluindo segurança e privacidade.

Nesse sentido, cita-se a título de exemplo, a Aliança Global de Cidades Inteligentes (FÓRUM ECONÔMICO MUNDIAL, 2019, p. [1]) como o seu próprio nome traz, é uma aliança que estabelece e promove normas de política global para ajudar a acelerar as melhores práticas, mitigar riscos potenciais e promover maior abertura e confiança pública.

A Aliança Global de Cidades Inteligentes tem a Organização Internacional para Cooperação Público-Privada, do Fórum Econômico Mundial, como seu secretariado e o Brasil participa como membro fundador da Aliança Regional para a América latina, podendo se reunir regularmente para analisar as políticas de cidades inteligentes e receber suporte técnico da rede de especialistas globais do Fórum (FÓRUM ECONÔMICO MUNDIAL, 2021b).

De acordo com o Globalsmartcitiesalliance.org, o G20 Global Smart Cities Alliance – G20GSCA foi estabelecido em junho de 2019, buscando reunir entes governamentais e o setor privado em torno de um conjunto compartilhado de princípios para o uso responsável e ético das tecnologias voltadas para as cidades inteligentes. (FÓRUM ECONÔMICO MUNDIAL, 2019, p. [1]).

Verifica-se que há um esforço global de discussão sobre a evolução das *smart cities*, no entanto, atualmente, não há uma estrutura global ou conjunto de regras em vigor sobre como os dados são coletados em espaços públicos, como por câmeras de tráfego, por exemplo, assim, o esforço da Aliança, visa promover maior abertura e confiança, bem como, criar padrões sobre como esses dados são coletados e usados. O tema da tecnologia de cidades inteligentes e governança de tecnologia global, portanto, é parte da agenda principal do Fórum Econômico Mundial ([2021a], p. [1]).

No bojo da realidade dos sistemas de informação, temos um aumento no volume de dados coletados e a necessidade de uso de sistemas para a adequada gestão destes. A tecnologia da informação e da Comunicação (TIC) apresenta ferramentas de gestão, inclusive na área da segurança pública e da mobilidade urbana, permitindo uma maior efetividade na gestão dos espaços e no combate à criminalidade.

Para Carnevali e Alcântara (2020, p. 94) “a cidade inteligente se utiliza dos mais variados recursos da Tecnologia da Informação e Comunicação (TIC), como exemplo: Big Data, *Internet of Things* (IoT), Geração de Comunicação Móvel (4G ou 5G), entre outros”.

Assim, importante trazer alguns dos conceitos tecnológicos e científicos que se associam às Cidades Inteligentes. Os conceitos citados a seguir são apontados como usuais da ciência da informação associado ao termo “cidades inteligentes”.

Internet das Coisas (*Internet of Things* – IoT) é o uso de tecnologia de conectividade e processamento para que objetos de uso cotidiano possam enviar, receber e processar informações, formando uma rede entre si, de forma análoga ao que é a Internet para os computadores. De modo geral, usa-se IoT para se definir sensores e atuadores, que captam dados e implementam ações. Alguns exemplos como a coleta de lixo inteligente, em que o trajeto considera as condições de ocupação em que estão as lixeiras, semáforos inteligentes, postes de iluminação com sensores de luz, estacionamentos que indicam aos motoristas onde há vagas já é uma realidade em muitas cidades (SANTOS FILHO; COÊLHO, 2018, p. 71).

A IoT tem sido utilizada para um maior controle dos serviços públicos e melhor comunicação com os usuários nas cidades, melhorando, assim a transparência e desta forma possibilitar a comunicação em tempo real. “A internet das coisas é uma tecnologia que interliga os equipamentos conectados à internet criando uma interação máquina a máquina e máquina a pessoas, visando trazer mais conforto, segurança e otimização dentro dos lares, já a indústria 4.0 é utilizada para maior agilidade e otimização em seus processos (CARNEVALI; ALCÂNTARA, 2020, p. 94).

Os sistemas utilizados geram uma enorme quantidade de dados, sendo uma importante fonte para fazer a gestão da segurança pública das cidades. Para a gestão desse grande volume dados, precisa de tecnologia para extrair a informação otimizada para além da pronta resposta ao crime, buscando uma gestão eficiente na área da segurança pública.

A área de pesquisa denominada Big Data tem sido utilizada na busca de soluções para o gerenciamento desse expressivo volume de dados de maneira mais eficiente e customizada às necessidades do gestor público, inclusive na área de segurança pública.

De acordo com Santos Filho e Coêlho (2018, p. 70): “Big *Data* é o estudo sobre o processamento de quantidades muito grandes de dados, que podem estar sendo produzidas em alta velocidade e em formatos variáveis: texto, tabelas, imagens, etc.”

A definição de internet das coisas é trazida por Carnevali e Alcântara (2020, p. 94):

> Internet das Coisas (Internet of Things – IoT) é o uso de tecnologia de conectividade e processamento para que objetos de uso cotidiano possam enviar, receber e processar informações, formando uma rede entre si, de forma análoga ao que é a Internet para os computadores.

### 3.2.2 O Big Data e a Gestão Eficiente dos Dados

No contexto da gestão urbana, o uso do Big Data pode aumentar significativamente a capacidade de compreensão acerca dos problemas enfrentados pelas cidades e, consequentemente, auxiliar na tomada de decisão para construção de cidades inteligentes, citando que poucas cidades que conseguiram apresentar resultados benéficos advindo do Big Data na gestão pública, vincularam o uso de dados a outras mudanças de estratégia governamental, como é o caso da integração das atividades de segurança pública, gestão de resíduos e água, administração pública, educação, segurança, mobilidade, energia e habitação, entre outros, estando a gestão desses eixos interligada por meio de ferramentas tecnológicas como a internet, aplicativos de celulares, sensores, etc. concluindo-se que o simples armazenamento e disposição dos dados, por si sós, não resolvem entraves no processo administrativo e decisório. (COSTA. 2014, p. 71)

A tecnologia do *big data* é fundamental para o funcionamento das cidades inteligentes (ALDAIRI; TAWALBETH, 2017, p. 1090) e de acordo com Remédio (2017, p. 673), o big data “possibilita o acompanhamento dos comportamentos humanos em tempo real e de maneira massificada, proporcionando inteligência às cidades, quando devidamente processados e analisados os dados que o integram” (VAZ-FERREIRA; RODRIGUES, 2021, p. 36).

Além do armazenamento dos dados gerados pelos sensores e pelos dispositivos tradicionais de governança, esses dados que serão utilizados na produção de conhecimento útil que ajude no processo de administração pública, particularmente à tomada de decisão (papel da atividade de inteligência de segurança pública), precisam ser manipulados com auxílio de técnicas específicas de armazenamento e processamento. Para isso, muitas técnicas de análise de dados já são estudadas e aplicadas, com sistemas de mineração atuando sobre os dados gerados. Essas técnicas específicas impõe o uso de armazenamento e acesso desses dados por diferentes equipamentos e aplicações com diferentes

finalidades, onde a computação em nuvem (*Cloud Computing*) aparece como uma solução viável e largamente empregada para este fim. O aprendizado de máquina (*Machine Learning*), por sua vez, é conceituado como técnicas conhecidas como “aprendizado de máquina”. (COSTA, C., 2014, p. 71)

Com a ampliação do uso dos sistemas de vigilância pela administração pública, vão surgindo novos tipos de violências, como o caso de “roubo” de dados, assim, o Estado precisa se preocupar com investimento em pesquisa e aplicação em segurança cibernética.

Ainda, de acordo com a autora acima citada, as novas tecnologias fomentaram os anseios de uma sociedade onde tudo é ao mesmo tempo e agora. Tudo nos remete à troca de dados e informações em tempo real: smartphones, redes sociais, internet das coisas, geolocalização. As informações geo-espacializadas tornam-se protagonistas, quando a localização é fator comum de integração e interoperabilidade.

Para Carvalho (2019, p. 15):

> não existe um conceito único sobre o que são cidades inteligentes, mas existe um consenso de que uma cidade inteligente deve ter como foco a melhoria da qualidade de vida da sua população. Passa por compreender como as temáticas de mobilidade, infraestrutura, saneamento, educação, saúde, segurança, meio ambiente, cultura, novas tecnologias e marco legal, por exemplo, interagem e impactam a dinâmica econômica, social e ambiental do município, em como impactam diretamente a população.

Ser uma cidade inteligente também requer ação assertiva, eficiente e rápida dos gestores. Uma vez compreendendo o cenário atual, é preciso identificar as ações necessárias para minimizar ou mesmo anular algumas falhas na gestão. E para alcançar este objetivo, os gestores devem investir em cinco pilares que sustentarão, a longo prazo, no tempo e no espaço, o projeto de cidades inteligentes: plano de metas, tecnologias, participação cidadã, desenvolvimento de pessoas, processos e procedimentos (CARVALHO, 2019, p. 15).

### 3.2.3 Cidade Inteligente (*Smart City*): Experiências Práticas

A importância da colaboração global é destacada pelo prefeito de Nova Iorque Bill de Blasio que no mundo interconectado de hoje, a colaboração global não é mais apenas uma opção, mas uma necessidade, orgulhando-se de ter defendido um modelo de cidade inteligente que coloca os seus residentes mais vulneráveis em

primeiro lugar, e enquanto gestor assumiu “a responsabilidade única de liderar pelo exemplo e demonstrar um caminho sustentável em direção a um futuro mais inclusivo e igualitário” (FÓRUM ECONÔMICO MUNDIAL, 2019, p. [1]).

Como caso de sucesso, Santos Filho e Coêlho (2018, p. 73-75), destacam a cidade de Santander, na Espanha, “onde há uma infraestrutura de sensores que disponibilizam uma série de dados sobre os mais diversos temas, como por exemplo, sensores de ruídos, pontos de acesso à Internet, vagas de estacionamento, lixeiras, dados coletados em ônibus, táxi (e Uber), caminhões de coleta de lixo, além de pontos turísticos, equipamentos urbanos (transportes, prédios públicos, etc.).” Outras cidades como Barcelona (Espanha), Songdo (Coréia do Sul), Masdar (Emirados Árabes Unidos) também se destacam nesta área.

No Brasil, os autores citam o município de Búzios, com oito áreas de atuação definidas, destacando-se a substituição dos medidores de energia elétrica eletromecânicos por medidores eletrônicos inteligentes. Além de Búzios, os autores também citam Rio de Janeiro, com câmeras e sensores instalados em diversos pontos da cidade, cujos dados ficam integrados numa sala de controle e Porto Alegre com destaque para dezenas de câmeras que monitoram 24 horas por dia, praças, monumentos, prédios públicos e a grande maioria das vias da cidade, ainda dispõe de um grande número de semáforos inteligentes, com Sistema de Controle de Trânsito em Tempo Real, os quais captam o fluxo de tráfego alternando o estado do semáforo de forma automática, acelerando o tempo de circulação em até 30% (trinta por cento) e reduzindo a taxa de emissão de gases em até 7% (sete por cento). Ainda, Curitiba, PR e Smart City Laguna, São Gonçalo do Amarante – CE (SANTOS FILHO; COÊLHO, 2018, p. 69-76).

Num estudo realizado sobre as primeiras iniciativas de cidades inteligentes que trazem benefícios à sustentabilidade urbana, tratando da experiência mundial no uso de sistemas digitais inteligentes, foram levantados dados de 10 cidades: Anyang (Coreia do Sul), Medellín (Colômbia), Namyangju (Coreia do Sul), Orlando (Estados Unidos), Pangyo (Coreia do Sul), Rio de Janeiro (Brasil), Santander (Espanha), Singapura (República de Singapura), Songdo (Coreia do Sul) e Tel Aviv (Israel), concluindo os autores que quando se procura garantir sustentabilidade e que geralmente já possui algum monitoramento com TIC, o item mobilidade (transportes públicos) é uma das primeiras preocupações dos gestores e a segurança é um foco importante em uma cidade inteligente, sendo que este dado não está

necessariamente associado ao número de habitantes. (CARNEVALI; ALCÂNTARA, 2020, p. 96)

Brasília faz parte da Aliança Global de Cidades Inteligentes (G20 Global Smart Cities Alliance) e tem seu plano baseado nos princípios de equidade, inclusão e impacto social; abertura e interoperabilidade; segurança e resiliência; privacidade e transparência; e operacionalização e sustentabilidade financeira, sendo exemplo a ser citado de organização de "*smart cities*", que possui planejamento e regulamentação para desenvolver o projeto Brasília Inteligente.

O Plano Diretor de Cidade Inteligente (PDTCI) do Projeto Brasília Inteligente visa atender as determinações da Lei Distrital nº 6.620 de 15 de junho de 2020, bem como, a capital do país tem regulamentado o assunto, consoante os Decretos Distritais que criam os órgãos e disciplinam as ações para implementar o Projeto.

A Carta Brasileira para Cidades Inteligentes orienta que as cidades avaliem e promovam ações levando em conta o potencial que elas têm de responder aos desafios locais, adequando-as ao estágio tecnológico do município. A referida carta traz como almejo "cidade que queremos": cidades seguras, resilientes e autorregenerativas, que necessita de planejamento e preparação para que possa responder prontamente a desafios climáticos, demográficos, sanitários, políticos e econômicos. Isso feito, busca-se garantir a segurança social, ambiental e urbana e o acesso aos serviços essenciais em todas as circunstâncias (BRASIL, [2020], p. [1]).

A Carta Brasileira para Cidades Inteligentes (BRASIL, [2020], p. 61), apresenta o seguinte conceito de *smart city*:

> São cidades comprometidas com o desenvolvimento urbano e a transformação digital sustentáveis, em seus aspectos econômico, ambiental e sociocultural, que atuam de forma planejada, inovadora, inclusiva e em rede, promovem o letramento digital, a governança e a gestão colaborativas e utilizam tecnologias para solucionar problemas concretos, criar oportunidades, oferecer serviços com eficiência, reduzir desigualdades, aumentar a resiliência e melhorar a qualidade de vida de todas as pessoas, garantindo o uso seguro e responsável de dados e das tecnologias da informação e comunicação.

### 3.2.4 Cidades Inteligentes e os Objetivos de Desenvolvimento Sustentável

A AGENDA 2030, aprovada em 2015, pela Assembleia Geral da Organização das Nações Unidas (ONU) estrutura-se em 17 Objetivos de Desenvolvimento Sustentável (ODS). Entre eles, está o Objetivo 11 – "Tornar as cidades e os assentamentos humanos inclusivos, seguros, resilientes e sustentáveis", sendo que

o item 11.7 estabelece como meta: “até 2030, proporcionar o acesso universal a espaços públicos seguros, inclusivos, acessíveis e verdes, em particular para as mulheres e crianças, pessoas idosas e pessoas com deficiência”(INSTITUTO DE PESQUISA ECONÔMICA APLICADA, 2019, p.[1]).

Nesse sentido, o Brasil assinou a Nova Agenda Urbana (NAU) – Declaração de Quito sobre Cidades e Assentamentos Urbanos para Todos, aprovada em 2016 na Conferência das Nações Unidas para Habitação e Desenvolvimento Urbano Sustentável (Habitat III). Os países que assinam acordos se comprometem a implementar as decisões, respeitando as realidades nacionais. Quando o Brasil assinou a NAU, prometeu que adotaria uma abordagem de cidade inteligente. Portanto a Carta Brasileira para Cidades Inteligentes é uma ação concreta nesse sentido.

Conforme a Carta Brasileira para Cidades Inteligentes (BRASIL, [2020], p. [1]), recomenda-se fortalecer a articulação entre governos para consolidar a governança urbana multinível (que atua em vários níveis - nacional, regional, estadual e local), interfederativa (com cooperação entre diferentes entes da federação - União, Estados, Municípios e Distrito Federal) e intersetorial (com cooperação entre as diferentes áreas de política pública). Firmar o papel dos governos estaduais e federal no apoio à adaptação de recomendações e políticas para os contextos locais em conjunto com os municípios.

Hoje, de acordo com a publicação Cadernos FGV – Smart Cities, cidade inteligente significa cidade resiliente e sustentável, isto é, com flexibilidade e capacidade de adaptação, capaz de dar respostas rápidas e eficientes às ameaças externas, como, por exemplo, mudanças climáticas, desastres, chuvas intensas, furacões, ou, simplesmente, atender aos princípios básicos de segurança alimentar ou de qualquer outra natureza (COSTA, 2014, p. 108-122).

A ideia de sustentabilidade, na qualidade de princípio jurídico, encontra-se em diversos dispositivos da Constituição Federal brasileira, a começar pelo preâmbulo e trazendo no art. 225, *caput*, da Constituição de 1988, que:

> todos têm direito ao meio ambiente ecologicamente equilibrado, bem de uso comum do povo e essencial à sadia qualidade de vida, impondo-se ao Poder Público e à coletividade o dever de defendê-lo e preservá-lo para as presentes e futuras gerações (BRASIL, 1988, art. 225).

De acordo com Cordeiro *et al.* (2021, p. 18) o cumprimento das três dimensões da sustentabilidade, quais sejam “ambiental econômica e social – ocorrerá com a participação da sociedade em geral, desde pequenos gestos rotineiros até que se atinja como todo o seu entorno para o bem comum [...]” concluindo os autores que:

> a sustentabilidade vem para que hábitos adquiridos ao longo dos anos sejam renovados, ou seja, para (re) educarmos nosso relacionamento com a natureza, (re)educarmos com o ser consumista instaurado em nossa estrutura e (re)educarmos socialmente desobstruídos de paradigmas obsoletos (CORDEIRO *et al.*, 2021, p. 18).

Uma cidade inteligente, portanto, requer o pensamento voltado à sustentabilidade, ou seja, é preciso maximizar os benefícios e diminuir os riscos da tecnologia para que toda a sociedade possa se beneficiar e viver com qualidade.

De acordo com Lee (2022, 1:51:00): “Smart city aim to enhance the quality of life, increase competitiveness and sustainability that encompass social, economic and environmental aspects”. Ou seja, o objetivo de uma smart city (cidade digital) é aumentar a competitividade e a sustentabilidade, englobando os aspectos sociais, econômicos e ambientais.

### 3.2.5 A Certificação de Cidades Inteligentes no Brasil

A Associação Brasileira de Normas Técnicas (ABNT) é uma associação civil sem fins lucrativos fundada em 1940, considerada de utilidade pública, é membro fundadora da International Organization for Standardization (ISO), gerando a criação e fomento de normas técnicas para diversos setores da sociedade e a certificação baseada nos mais diversos padrões normativos. (ABNT)

A ABNT desenvolveu um processo e certificação de indicadores baseado nas normas ABNT NBR ISO 37120, ABNT NBR ISO 37122 e ABNT NBR ISO 37123, cujo objetivo principal é ajudar as cidades a atrair investimentos e impulsionar o desenvolvimento econômico com dados comparativos globais.

De acordo com a Associação Brasileira de Normas Técnica, 2020b, p. [1]:

> Esse processo permite medir o desenvolvimento urbano sustentável, informar os investimentos em infraestrutura com resultados mensuráveis, medir a gestão de desempenho de serviços urbanos e qualidade de vida ao longo do tempo. Além disso, facilita a troca de informações e projetos através do compartilhamento de informação, permitindo comparações por meio de uma vasta gama de medidas de desempenho

A ABNT disponibiliza o acesso à plataforma onde são inseridos indicadores e evidências, é feita a auditoria de certificação, a análise dos resultados e a emissão do certiicado, se for o caso.

O questionário faz parte do programa “Certificação e indicadores para cidades e comunidades sustentáveis”, o qual é baseado nas seguintes normas: ABNT NBR ISO 37.120 – indicadores para serviços urbanos e qualidade de vida, ABNT NBR ISO 37.122 – indicadores para cidades inteligentes e ABNT NBR ISO 37.123 – indicadores para cidades resilientes.

Conforme informação da ABNT o primeiro certificado de conformidade deste programa de certificação ABNT foi emitido para o Município de São José dos Campos no dia 16/03/2022, tornando São José dos Campos a primeira cidade brasileira a receber este tipo de certificação. O município atingiu a certificação nos seguintes níveis: Platina na norma ABNT NBR ISO 37120; Ouro na norma ABNT NBR ISO 37122 e Ouro na norma ABNT NBR ISO 37123.

Já o município de Pindamonhangaba recebeu o seguinte certificado, emitido em 25/01/2023: Platina na norma ABNT NBR ISO 37120.

Os certificados têm prazo de validade, que pode ser prorrogado anualmente caso seja cumprido satisfatoriamente o processo de avaliação anual chamado manutenção da certificação.

Empresas de consultoria têm disponibilizado serviços visando obter certificações, já indicando um rol de outras empresas que fornecem os mais variados produtos e serviços.

Temos como exemplo a *Bright Cities*, que presta consultoria e oferece soluções (cardápio de opções) para diversas áreas, inclusive premiando cidades em eventos nacionais, como o *Smart City* Curitiba.

As soluções e boas práticas envolvem as diversas áreas, tais como: educação, meio ambiente, energia, governança, saúde, empreendedorismo, tecnologia e inovação, mobilidade e segurança.

Destacamos no quadro 2, as áreas da inovação e da segurança pública.

**Quadro 2** - áreas da inovação e da segurança pública

| Área | |
|---|---|
| Tecnologia e inovação | Ex. Plataforma de energia inteligente *Omniled - Smart* - agrega vários níveis de serviço para serem usados em muitas aplicações como Iluminação Inteligente com a integração de 5G/LTE/WIFI, soluções de mobilidade, segurança com análise inteligente e compatibilidade de borda. Com nossa solução, as cidades podem transformar um simples poste de luz em um objeto neutro em carbono que pode ser usado para várias finalidades de IoT em uma única infraestrutura. Todas as unidades *Omniflow* possuem conectividade IoT para gerenciamento e controle dos aplicativos integrados. O design premiado oferece todas as funcionalidades em uma solução totalmente integrada pronta para funcionar com um tempo de instalação inferior a 30min. |
| Segurança | Ex. Núcleo da Íris – em situações de emergência, as informações são críticas para os comandantes de incidentes. Novas tecnologias como drones, câmeras corporais, Sistema de Informação Geográfica (GIS) estão fornecendo informação em tempo real que trazem um novo desafio: as informações são fragmentadas e não filtradas, saturando, assim, os tomadores de decisão no momento dos incidentes. A solução é uma plataforma Softwares como Serviço (SaaS) modular projetada especificamente para os comandantes de incidentes, que permite integrar múltiplas fontes de dados sob um hub central, processar e exibir informações relevantes; coordenar as equipes e outras agências para agir. É uma nova oportunidade para os socorristas realmente adotarem novas tecnologias em sua missão: salvar vidas e proteger propriedade. |

**Fonte:** adaptado de Bright Cities ([2023].

As empresas de consultoria quanto ao tema das cidades inteligentes têm como base normas da International Organization for Standadization (ISO), que lança os documentos de avaliação que define estabelece metodologias para uma série de indicadores relacionados às cidades inteligentes, buscando medir o desempenho das cidades cujas questões são alinhadas aos Objetivos do Desenvolvimento Sustentável da Organização das Nações Unidas (ONU), estabelecidos em 2015, para guiar o desenvolvimento dos países de maneira sustentável e inclusiva.

Importante trazer que a ABNT NBR ISO 37122 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2020a, p. xvi), é um documento que vem complementar a norma técnica ISO 37120, adotada pela ABNT em 2017 (ABNT NBR ISO 37120:2017, Desenvolvimento sustentável de comunidades – indicadores para serviços urbanos e qualidade de vida), considerando a necessidade de indicadores adicionais para cidades inteligentes. Assim dispondo:

> Este documento, quando usado em conjunto com a NBR ISO 37120, auxilia as cidades a identificarem indicadores para a aplicação de sistemas de gestão urbana, como a ABNT NBR ISO 37101, e a implementarem políticas, programas e projetos de cidades inteligentes que:
>
> - respondam a desafios como as mudanças climáticas, o rápido crescimento populacional e a instabilidade política e econômica, melhorando fundamentalmente a forma como envolvem a sociedade;
>
> - apliquem métodos de liderança colaborativa e trabalhem entre disciplinas e sistemas urbanos;
>
> - usem informações de dados e tecnologias modernas para oferecerem melhores serviços e qualidade de vida para aqueles que estão nas cidades (moradores, empresas, visitantes);
>
> - proporcionem um melhor ambiente de vida, em que políticas, práticas e tecnologias inteligentes sejam colocadas a serviço os cidadãos;
>
> - alcancem os seus objetivos ambientais e de sustentabilidade de forma mais inovadora;
>
> - identifiquem a necessidade e os benefícios das infraestruturas inteligentes;
>
> - facilitem a inovação e o crescimento; e
>
> - construam uma economia dinâmica e inovadora, pronta para os desafios do futuro (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2020a, p. [1]).

## 3.3 INOVAÇÃO TECNOLÓGICA

A história da evolução mostra que o ser humano, de forma contínua e repetitiva, busca inovar visando à melhoria da qualidade de vida, por meio do conhecimento recebido, da observação e da pesquisa científica. A palavra “inovar” tem origem no latim e significa “renovar”, “tornar novo”, mas são muitos os conceitos de inovação tanto no meio científico quanto em âmbito social, havendo inclusive contradições entre eles (FREIRE; FURLAN; SILVEIRA, 2018, p. 43).

Para os autores citados acima, o conceito de inovação transcende a simples ideia de mudança tecnológica, pois tem relação com a comunicação e sofre influência de vários meios, incluindo a associação entre organizações, agências de pesquisa e governo. A inovação eficiente depende de todas as relações criadas de forma eficaz, não se limitando apenas a produtos, mas também a serviços, tanto no setor público quanto no privado.

A chamada Lei de Inovação, Lei 10.973, de 2 de dezembro de 2004, traz a definição do termo inovação: “inovação é todo e qualquer mecanismo de introdução ou aperfeiçoamento no ambiente produtivo ou social que resulte em novos produtos, processos ou serviços […]”

Importante salientar que inovação não se confunde com invenção, cuja Lei 10.973/2004 também regula e define.

De acordo com Freire, Furlan e Silveira (2018, p. 7), a Lei nº 10.973/2004 de incentivo à inovação, à pesquisa científica e tecnológica no ambiente produtivo, busca nortear e incentivar a pesquisa científica e tecnológica. Ela objetiva quebrar o paradigma cultural que somente as universidades são responsáveis pelo desenvolvimento científico e tecnológico, já que, em outros países, essa responsabilidade cabe às universidades, às empresas e à sociedade.

A Constituição da República Federativa do Brasil (BRASIL, 1988, art. 23), dispõe que é competência comum da União, dos Estados, do Distrito Federal e dos Municípios proporcionar os meios de acesso à cultura, à educação, à ciência, à tecnologia, à pesquisa e à inovação, e em seus arts. 218 e 219, 219 A e B, trata da promoção e do incentivo do estado para o desenvolvimento científico, apoio à pesquisa e preparação tecnológica.

A inovação de processo no serviço público procura aumentar a eficiência dos processos internos para propiciar a fabricação de produtos e prestação de serviços a população. O estudo sobre inovação no setor público tem conflito micro/macro aumentado, o que se justifica em razão das dimensões e complexidades das estruturas organizacionais, bem como da incorporação da legislação existente e de políticas públicas, sendo que estas devem primar por igualdade social e eficiência (FREIRE; FURLAN; SILVEIRA, 2018, p. 54-55).

As tecnologias são um dos pilares que fazem a cidade inteligente, no entanto, a tecnologia é o meio e não o fim. É preciso saber antes que tipo de tecnologia deve ser aplicada (CARVALHO, 2019, p. 16).

Diferentes tecnologias são requisitadas para que as iniciativas na implantação de cidades inteligentes sejam viabilizadas, estas são tanto para manter as iniciativas em operação quanto para integrá-las com outras que porventura existam ou venham a existir (SANTOS FILHO; COÊLHO, 2018, p. 71).

Nesse cenário, se apresentam desafios para o gestor público, especialmente da área de segurança, devendo este agir com base nos princípios constitucionais,

mediante uma gestão ética e responsável, face à escassa regulamentação do assunto e dos interesses que podem estar por trás do uso desta tecnologia.

Os desafios que podem ser apontados à implantação da cidade inteligente são muitos, visto que pode o tema ser tratado como uma mudança de paradigmas, onde toda a dinâmica da cidade tem um novo direcionamento.

Percebe-se a necessidade de planejamento do município, podendo iniciar pela construção de um plano específico para o que se denomina cidade inteligente, visando planejar e adotar tecnologias para tornar as regiões mais inteligentes, humanas, sustentáveis e seguras.

Projetos distintos (direcionados para as diversas áreas de atuação do município), como os propostos neste trabalho, articulados com um plano principal, iniciando com o planejamento pela identificação da cidade que temos e que queremos, buscando levantar onde e como fazer, bem como, qual é a melhor tecnologia a aplicar, analisando os custos em relação aos benefícios e de onde serão provenientes os recursos que contribuirão para o desenvolvimento de uma cidade mais inteligente, com vistas a qualidade de vida de seus habitantes.

Assim, como no setor privado, a Transformação Digital (TD) mobiliza recursos ágeis relativos à flexibilidade operacional e capacidades tecnológicas e informacional, impulsionando as inovações em serviços digitais, visto o contexto de ambientes intensivos digitais, proporcionando o desenvolvimento das cidades como um todo. Ou seja, o setor econômico é mola propulsora do desenvolvimento das cidades e a gestão pública se utiliza dos seus produtos, serviços e valores (inclusive intangíveis, como ativos digitais) em benefício de toda a coletividade. E, como bem lecionam Andrade, Gonçalo e Santos (2022, p. 1):

> A diversidade de combinações de recursos tecnológicos e processos permite às empresas criarem novas configurações e modelos de negócios, produzindo ativos digitais intangíveis em ambientes de serviços. as organizações que desenvolvem a capacidade dinâmica da TD com agilidade têm maiores possibilidades de obter valor sustentável por meio da exploração de plataformas e integração em ecossistemas digitais.

Assim, este trabalho buscará apresentar, a seguir, exemplos de ferramentas que fazem parte do ecossistema da cidade denominada inteligente, os quais podem ser utilizados pela inteligência de segurança pública, reforçando os desafios e perspectivas deste novo momento das cidades e a importância da atividade de

inteligência de segurança pública, ou seja, de que forma ela poderá contribuir para um melhor desenvolvimento das cidades.

## 3.4 REFLEXÕES PARA UMA ARQUITETURA DE INTELIGÊNCIA MUNICIPAL

Contemporaneamente, a Segurança Pública é definida pela Constituição Federal, no art. 144, como dever do Estado, direito e responsabilidade de todos. Cabe ao Poder Público, em cada esfera de governo – União, Estados, Municípios, com a participação da sociedade civil atuar conjuntamente em prol de uma segurança pública de qualidade, participativa e inclusiva. Efetivada de fato por meio de políticas públicas de segurança, que visem o interesse público, o interesse coletivo e ao exercício da cidadania e do controle social (ALVES, 2016, p. 1384).

Nesse sentido, o art. 144, da Constituição estabelece que "A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio".

As atividades atinentes à segurança pública, estão principalmente afetas às polícias estaduais civis e militares, uma vez que a polícia federal tem um âmbito restrito de atribuições (BRASIL, 1988, art. 144, § 1º e incisos).

O art. 144, da CF/88, assim dispõe:

> Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos:
>
> I - polícia federal;
>
> II - polícia rodoviária federal;
>
> III - polícia ferroviária federal;
>
> IV - polícias civis;
>
> V - polícias militares e corpos de bombeiros militares.
>
> VI - polícias penais federal, estaduais e distrital.
>
> [...]
>
> § 8º Os Municípios poderão constituir guardas municipais destinadas à proteção de seus bens, serviços e instalações, conforme dispuser a lei. (BRASIL, 1988, art. 144)

No âmbito municipal, portanto, podem ser instituídas as guardas municipais, cujo Estatuto Geral é regido pela Lei Federal 13.022, de 08 de agosto de 2014.

No que tange à competência municipal para as atividades de polícia ostensiva para a preservação da ordem pública, pelos guardas municipais, a discussão ainda segue no Supremo Tribunal Federal, na Arguição de Descumprimento de Preceito Fundamental (ADPF 995). A ação, de autoria da Associação dos Guardas Municipais o Brasil (AGM Brasil), pede o reconhecimento das guardas municipais como órgão de segurança pública. Conforme a notícia veiculada no site “Diarinho” o julgamento da ação começou em 17 de fevereiro de 2023 e no voto do ministro Alexandre de Moraes, este julgou procedente a ação.

> O recurso contesta decisão do Superior Tribunal de Justiça (STJ), que em 2022 reforçou entendimento de que a GM, por não estar entre os órgãos de segurança previstos na Constituição, não pode exercer atividades das polícias Civil e Militar, devendo se restringir à proteção patrimonial dos municípios. Pela decisão, a atuação da GM na realização de abordagens e revista pessoal só poderia ocorrer em casos excepcionais, e não ser tarefa rotina das guardas no país (DIARINHO, 2023, p. [1]).

Portanto, o voto do ministro Moraes abre caminho para o entendimento consolidado da questão.

De acordo com a Lei nº 11.150/07 que instituiu o Programa Nacional de Segurança Pública com Cidadania (Pronasci), reforçou o papel insubstituível das municipalidades na execução das suas ações, de forma integrada, além de focar na promoção da cidadania. Neste norte, os municípios possuem um importante papel, dentro das suas competências constitucionais. (CORRALO; KEMMERICH, 2021, p. 126-140).

O último capítulo buscará, portanto, apresentar exemplos de ferramentas que fazem parte do ecossistema da cidade denominada inteligente, os quais podem ser utilizados pela inteligência de segurança pública, reforçando os desafios e perspectivas deste novo momento das cidades e a importância da atividade de inteligência de segurança pública, ou seja, de que forma ela poderá contribuir para um melhor desenvolvimento das cidades.

## 3.5 A INTELIGÊNCIA DE SEGURANÇA PÚBLICA NO CONTEXTO DAS SMART CITIES

Neste ponto trataremos da atividade de inteligência pública tratando da importância da atividade para a prevenção da criminalidade apresentando alguns exemplos de sistemas ou ferramentas que podem ser implantados nas cidades e que a atividade de inteligência pública utilizará potencializando a sua atuação.

### 3.5.1 A Atividade de Inteligência para a Prevenção da Criminalidade

Considerando que as cidades reconhecidas como seguras, têm implementado sistemas de monitoramento, pautados no binômio “inovação e tecnologia”, continuamente têm buscado empregar ferramentas que viabilizem a interoperabilidade sistêmica e ofereça acesso a informações, em tempo real, que racionalizem os meios e potencializem os resultados, focados na antecipação, prevenção e pronta resposta nas ações de enfrentamento do crime e da violência. Lembrando que existem uma série de fatores intervenientes, que permeiam a ocorrência de um crime:

> O triângulo do crime oferece uma visão dos elementos necessários para a ocorrência de um crime, cuja interação pode ser assim sintetizada: para que um crime ocorra deve haver convergência de tempo e espaço em, pelo menos, três elementos – um provável agressor, uma vítima/alvo adequado, na ausência de um guardião capaz de impedir o crime. [...] A teoria das atividades rotineiras exige mais do que a existência de um agressor (infrator), requer um alvo (vítima) vulnerável e um ambiente propício, ou seja, um ambiente que forneça as condições exatas para que o crime ocorra. (HIPÓLITO; TASCA, 2012, p. 199- 201).

Como exemplos trazemos o projeto de desenvolvimento de uma arquitetura tecnológica, de conectividade inteligente, coletando dados, identificando veículos e pessoas, nos pontos de entrada e saída do município de Joinville, Santa Catarina, transmitindo estes dados em tempo real ao Observatório de Políticas Públicas, onde funciona o Núcleo de Inteligência da Secretaria de Defesa Civil e Segurança Pública (SEPROT), para análise e produção do conhecimento e apoio a ações de prontas respostas operacionais e implementação de estratégias e ações do conceito de cidades inteligentes.

De acordo com Silva e Rolim (2003, p. 156), a sociedade espera que o Estado seja eficiente no planejamento e na articulação de ações que evitem situações de riscos e promovam intervenção qualificada. Para atendê-la, há

necessidade de produzir conhecimento para que as ações estejam pactuadas em subsídios amplos, efetivos e eficazes. Portanto, evidencia-se a importância do emprego da atividade de inteligência de Segurança de Pública na otimização da prevenção criminal.

Para Barbosa (2008 *apud* SILVA; ROLIM, 2017, p. 156) as atividades delituosas manifestam-se de dois tipos:

> a microcriminalidade - quando os crimes são praticados de maneira desorganizada, como nos casos dos crimes de furtos, roubos, estupros, crimes esses praticados no contexto da violência urbana; a macrocriminalidade – no qual há uma organização para a prática do crime, onde os delinquentes organizam e estruturam suas atividades criminosas de modo profissional, como nos crimes de roubo a bancos, tráfico de drogas, de sequestro, de infiltração em altos escalões da República para crimes de corrupção ativa e tráfico de influência.

E diante do cenário de criminalidade, Cruz (2013 *apud* SILVA; ROLIM, 2017, p. 157), traz que a atividade de inteligência é o instrumento estatal capaz de subsidiar, por intermédio da produção de conhecimento, a prevenção da violência e da criminalidade. Esse conhecimento, elaborado em tempo adequado e com a devida confiabilidade, é capaz de reduzir as incertezas e apresentar soluções adequadas para a tomada de decisão.

O trabalho de coleta e de busca de dados, carece às vezes, de pesquisas que podem ser confundidas com investigação. A busca de dados negados é chamada de “Operações de Inteligência”. (SILVA; ROLIM, 2017, p. 157)

Segundo Cepik (*apud* SILVA; ROLIM, 2017, p. 157) a atividade de Inteligência Interna – segurança pública – é o conjunto de atividades de análise e de operações de natureza compartimentada que têm por escopo dar suporte aos atos de prevenção e repressão criminais para fins de neutralização das ações criminosas cotidianas, bem como das ações criminosas organizadas.

A atividade de inteligência pode ser entendida sob dois aspectos: o primeiro, de natureza tática, ligado diretamente à prevenção imediata de práticas criminosas e repressão criminal; o outro, de caráter estratégico, vinculado à análise de cenários e prospecção. (SILVA; ROLIM, 2017, p. 158)

A prevenção criminal depende do poder do Estado de implementar políticas públicas que assegurem a todos os brasileiros o exercício dos seus direitos. Por isso a importância da Atividade de Inteligência de Segurança Pública e sua relação com o fortalecimento das ações de prevenção criminal, pois quanto maior o nível

hierárquico funcional do tomador de decisão, mais relevante será o conhecimento produzido no processo decisório e para o planejamento de políticas públicas de segurança pública e de defesa do cidadão. (SILVA; ROLIM, 2017, p. 158)

> A atividade de inteligência de segurança pública não é a parte mais importante da atividade de prevenção criminal, mas constitui um elemento indispensável à abordagem estratégica e tática da prevenção criminal. [...] O tema Segurança Pública não pode ser encarado apenas como responsabilidade do Estado, mas sim de toda a sociedade – necessita da participação de vários atores e espaços de socialização. Por intermédio do conhecimento elaborado pela Atividade de inteligência, pode-se viabilizar a formulação de diagnósticos que apresentarão novas formas de enfrentamento ao fenômeno da violência e ao da criminalidade. (SILVA; ROLIM, 2017, p. 157-159).

A inteligência de segurança pública, pode de forma tangível e efetiva contribuir para o combate à impunidade no Brasil. Se por um lado temos uma atividade de inteligência bem sistematizada e uma gama de atuações oportunas dentro do cenário da segurança pública brasileira, por outro lado, ainda temos uma grande sensação de impunidade, como se vê diariamente nos noticiários dos diversos meios de comunicação.

Outro campo da segurança, que atualmente ganha destaque, é a segurança cibernética. Esta é definida como a proteção de sistemas interconectados via *internet*, incluindo hardware, *software* e dados, contra-ataques cibernéticos de agentes maliciosos. Segurança cibernética requer coordenação de esforços ao longo de todo um sistema de informação: segurança de aplicações; segurança da informação; segurança de rede; recuperação de desastres; segurança operacional e educação do usuário final.

De acordo com Carvalho (2019, p. vi) a segurança pública se utiliza de ferramentas com localização geoespacial, inserindo-se no novo paradigma na gestão urbana, “onde a cidade cria laços digitais que unem cidadãos, empresas, poder público com o objetivo de propiciar melhor qualidade de vida e maior desenvolvimento”.

De acordo com a Carvalho (2019, p. vi), o urbano apresenta inúmeras características dos sistemas complexos, dentre eles:

> por ser um sistema dinâmico, onde as cidades mudam a todo o momento e em um ritmo acelerado. Seja na implantação de infraestruturas, na configuração de sua paisagem, na dinâmica da ocupação territorial, ou nos manifestos sociais e culturais. Além disso, mudam-se seus gestores, e com eles as prioridades de investimentos, o que a torna dinâmica em ambos os sentidos: físico e sociopolíticos.

Segundo Bruno (2019, p. 48), considerando que o urbano é um sistema dinâmico, os meios aplicados pelo Estado para fornecer a sensação de segurança também precisam estar em constante inovação e ajustar-se às novas necessidades, de forma a melhor atender ao interesse público e as necessidades da sociedade.

A tecnologia para cidades inteligentes, portanto, pode ser desenvolvida e utilizada para todos os aspectos da vida, podendo gerenciar as coisas que conectam tudo onde vivemos: sensores de inteligência artificial para a observação do tempo, segurança pública, coleta de lixo, estacionamento inteligente, trânsito inteligente, qualidade da água, do solo, do ar, iluminação pública, saúde pública, safras, gestão do uso e da reciclagem de energia, planejamento, gestão e design de edifícios, prevenção de desastres, restauração devido a eventos climáticos, entre outros.

Cada instalação gera dados individuais e públicos, e necessita de um gerenciamento técnico, cujo objetivo é integrar as bases e gerenciar de forma adequada e útil os dados. Ou seja, a capacidade e usar e operar os dados é muito importante, devendo o governo estabelecer em conjunto com os residentes o que deve ser priorizado, visando aumentar o desenvolvimento sustentável da região, sob a perspectiva do que irá proporcionar maior conforto, segurança e felicidade, melhorando, portanto, a qualidade de vida.

### 3.5.2 O Cercamento Eletrônico das Cidades

Um modelo de arquitetura de segurança pública utilizado pela atividade de inteligência é o chamado cinturão digital ou cercamento eletrônico da cidade.

Neste sentido, este sistema visa para proteger e fortalecer a população de eventuais ameaças do crime organizado, que utilizam o sistema viário local, como rotas de entrada e de fuga para a perturbação da paz.

O projeto tem a finalidade de empreender o monitoramento preventivo, detectar e rastrear infratores, nas ocorrências e ações de enfrentamento ao crime organizado, de quadrilhas especializadas de roubo de cargas, roubo a estabelecimentos bancários, tráfico de drogas e outras modalidades criminosas que atentem contra a segurança pública. O Cinturão abrange todas as entradas e saídas da cidade, com acesso às rodovias, inclusive às vias secundárias. A finalidade é conter o aumento do crime e transformar a cidade mais segura.

A implantação de um Cinturão Digital de Segurança, atuando de forma integrada com as Forças de Segurança, no âmbito do Município, compartilhando essas informações com outros órgãos e instituições de segurança no Município, observadas ainda, sua finalidade como ferramenta nas ações de articulação territorial, nas ações de prevenção à violência e criminalidade.

O objetivo deste tipo de projeto é criar um cinturão de segurança na cidade para gerenciar e controlar os fluxos de tráfego dotando as entradas e saídas do município de câmeras de vigilância com identificador de placas de automóveis, através de um sistema que capta a imagem e placa de todos os veículos que entram e saem, de maneira a ter mais controle do fluxo de veículos através de barreira eletrônica.

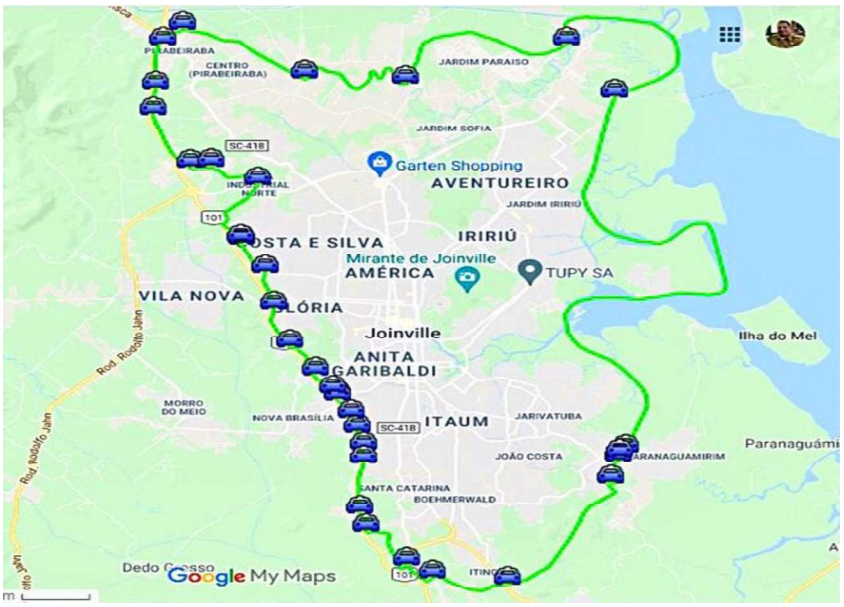
Como objetivos específicos temos: a) Implantar o sistema de segurança por monitoramento eletrônico, com aumento e expansão da rede de locais monitorados, com avanço tecnológico de equipamentos considerados estado da arte ou de ponta (em inglês, cutting-edge), isto é, que trabalha com as mais recentes inovações tecnológicas, ou na sua investigação, b) instalar sistemas de reconhecimento automático de placas de identificação veicular, com câmeras *Optical Characteres Recognized* (OCRs) – Leitores Ópticos de caracteres, que reconhecem placas de veículos com registros em ferramenta computacional de controle de trafego viário; c) identificar fatores decisivos para a obtenção dos melhores resultados com o uso desses sistemas automáticos de placas de identificação veicular; e d) utilizar radares em associação às câmeras de registro fotográfico, softwares de OCRs e ferramentas computacionais que permitirão a consulta em uma base de dados consistente.

#### 3.5.2.1 Descrição do funcionamento

As câmeras de OCRs permitem monitorar e analisar imagens de câmeras específicas ou integradas com as câmeras de trânsito, instantaneamente, e verificar em tempo real, ilegalidades diversas, tais como carros roubados, documentação irregular e placas clonadas. O sistema também permite fazer buscas por placa, marca e modelo dos veículos, e também com base em características obtidas pelos operadores, como adesivos que tenham caracteres passíveis de leitura. Ao detectar algo suspeito, as informações são reunidas no Observatório de Políticas

Pública/Centro Integrado de Comando e Controle, que após análise, repassa às forças de segurança.

**Figura 1** - Cercamento eletrônico.- exemplo de Joinville - SC




**Fonte**: Secretaria de Proteção Civil e Segurança Pública de Joinville (apud SILVEIRA, 2021, p. [1])

Neste sentido, a proposta do cercamento eletrônico das cidades, com câmeras inteligentes de vigilância, vem colaborar para a construção de redes, possibilitando a troca de informações de um município para outro e de um estado para outro, como é o caso de estados vizinhos, sendo um dos itens que podem ser considerados parte de uma cidade inteligente.

### 3.5.3 O emprego da Videovigilância na Gestão Pública

O emprego da videovigilância na atividade de inteligência de segurança pública é um tema que traz preocupação ao gestor público quanto aos limites de sua atuação, tendo em vista a necessidade da observância dos princípios que regem a atividade da administração pública, a própria atividade de inteligência de segurança pública e os direitos da pessoa de inviolabilidade da intimidade, da vida privada, da honra e da sua imagem.

Uma preocupação não menos importante a ser destacada, é quanto a eficiência dos serviços, considerando-se o custo-benefício trazido pelas novas tecnologias, especialmente no tocante ao uso das câmeras de vídeo-monitoramento.

A justificativa utilizada para o emprego da vídeo-vigilância é apresentada por alguns dos autores pesquisados. Para Lemos *et al.* (2011), há cultura do medo, da insegurança, onde ser vigiado e monitorado é uma necessidade.

De acordo com Evangelista *et al*. (2016, p. 322), "na sociedade contemporânea, as câmeras de vigilância são tecnologias de uso rápido e crescente. As razões dadas para essa proliferação estão principalmente relacionadas a preocupações com segurança. Nos países pobres, a ênfase está no controle da criminalidade urbana. Nos países ricos, elas estão justificadas também pela ameaça ao terrorismo.

Tratando do uso das câmeras de vigilância com novas tecnologias, na área de inteligência de segurança pública, citamos Paula (2013, p. 22), que aduz: "as novas tecnologias disponíveis e as possibilidades de construção de redes de conhecimento favorecem a atividade de inteligência e permitem uma maior efetividade nas estratégias e nas ações".

Registra-se que no Brasil a adoção desses aparelhos tem sido crescente e o discurso da segurança pela vigilância está presente em todos os setores (polícia, academia, mídia). O crescimento da adoção de câmeras de segurança é gigantesco (LEMOS *et al*., 2011, p. 144).

Para Firmino *et al*. (2013), são apontados três fatores para o aumento do uso de câmeras de segurança no Brasil, quais sejam: a ausência de legislação específica que regule a forma como esses sistemas são utilizados; o escopo limitado do debate sobre a implantação da tecnologia de vigilância e as implicações de seu uso generalizado; e uma crescente atmosfera de medo urbano que afeta o caminho onde as pessoas vivem e se deslocam em cidades grandes e médias.

Em países como o Brasil, sede de recentes eventos internacionais como a Copa do Mundo de 2014 e as Olimpíadas de 2016, a intensificação no uso de sistemas de monitoramento por câmeras partindo do poder público está, no discurso, associada à prevenção de ataques terroristas (EVANGELISTA *et al*., 2016, p. 322).

Conforme os autores acima, em se tratando de câmeras que alvejam espaços públicos como praças, ruas e calçadas, podemos dizer que a maioria se divide no cumprimento de dois propósitos: o combate à violência e à criminalidade, sendo instaladas e controladas por particulares ou por órgãos públicos; e a administração e disciplinamento do trânsito, mas podendo ser administradas e instaladas por

empresas privadas terceirizadas. Há situações específicas em que uma acaba fazendo a função da outra, como quando câmeras de controle de tráfego capturam “por acidente” algum evento significativo acontecendo.

Segundo Bruno (apud LEMOS *et al*., 2011, p. 145), a instalação de câmeras em espaços públicos no Brasil começou há 27 anos e tem se consolidado ao longo dos anos. Reconhecendo que a vigilância no Brasil teve início nos anos 1980, enquanto Bruno (2009, apud LEMOS *et al*., 2011, p. 145), defende sua intensificação nos anos 1990 e sua configuração como sinônimo de segurança a partir de 2003, passando a existir não mais apenas em setores privados ou semipúblicos, como também nos espaços públicos.

Lemos *et al*. (2011, p.143), tratando do tema da vigilância e sociedade contemporânea, traz que:

> a sociedade contemporânea pós 11 de setembro alia, ao mesmo tempo, formas de vigilância disciplinar, panóptica (Foucault) e formas de controle, digitais, em movimento, típico das sociedades de controle (Deleuze). Câmeras de vigilância, rastreamento de dados na internet, formação de perfis digitais com mineração de dados em redes sociais como Facebook, Orkut, rastros com uso de cartões de crédito ou com as novas ferramentas sociais de geolocalização *comoTwitter, Gowalla, Foursquare* estão em expansão. As formas de controle, monitoramento e vigilância estão por toda a parte e passam a integrar o *modo operandis* da sociedade da informação neste começo de século XXI. O singelo “sorria você está sendo filmado” deve ser levado a sério. A sociedade contemporânea expandiu, como nenhuma outra, as formas de controle, monitoramento e vigilância, tanto de maneira forçada (como as câmeras de vigilância) como de forma espontânea (como os perfis e informações construídos e fornecidos pelos internautas nas mais diversas redes sociais).

As câmeras de vigilância controladas pelo Estado, no entender de Mosetic, Barbiero e Barbiero (2022, p. 229-230), “por alcançar entradas de residência e até suas janelas, causam mudança de comportamento. Há assim, uma redução das liberdades civis daqueles que circulam sob seu alcance podendo inclusive prejudicar relações sociais, que tendem a ficar mais discretas – cerceadas – sob os olhos atentos do Estado”.

Ainda, segundo os autores acima, a tecnologia da informação está inserida na vida das pessoas cujos efeitos acompanham também o tema da vigilância, que além de proporcionar a sensação de segurança (direito à segurança), também influencia em aspectos da vida privada, porque reflete no receio da publicação de imagens individuais em situações que podem gerar danos à intimidade. Contudo, o princípio da privacidade não deve ser considerado isoladamente, mas relacionado com o

princípio da segurança pública, a qual é dever e responsabilidade também do Estado, que, para tanto, utiliza-se das prerrogativas proporcionadas por essa ferramenta tecnológica e resguardado na legislação vigente.

Sobre as *smart cameras*, citamos Bruno (2012, p. 50) que dispõe:

> um dos argumentos recorrentes nas pesquisas e indústrias que projetam tais artefatos é de que eles superariam as limitações perceptivas e atencionais presentes no monitoramento dos sistemas convencionais de vídeo-vigilância. A atenção humana seria limitada para lidar com o volume e a monotonia de tais imagens. Após apenas 20 minutos de atividade, a atenção da maioria dos indivíduos cairia a um nível abaixo do aceitável para um monitoramento eficiente.

Uma razão apontada para a ineficácia da vídeo-vigilância na promoção da segurança, sendo mais efetivas na produção de provas *post facto* do que na prevenção de incidentes ou crimes é o fato das limitações presentes no monitoramento pelos sistemas convencionais. Assim, a adição de uma camada "inteligente" às câmeras pretende automatizar a percepção e a atenção de modo a ressaltar nas imagens apenas os índices de ameaça, perigo ou qualquer situação que mereça destaque, conforme o propósito definido (BRUNO, 2012, p. 50).

O mercado tem apresentado uma evolução tecnológica e, neste sentido, ganha destaque a "videovigilância inteligente", chamada de terceira geração das tecnologias de videovigilância, cuja peculiaridade é o monitoramento automatizado de comportamentos. Na maioria dos casos, pretende-se que tais câmeras reconheçam e diferenciem padrões regulares de conduta e ocupação do espaço, tido como seguros, e padrões irregulares, categorizados como suspeitos, perigosos ou simplesmente não funcionais.

De acordo com Bruno (2012, p. 48), "costuma-se dividir os sistemas de videovigilância em três gerações: videovigilância controlada por operador, videovigilância de base automatizada e videovigilância inteligente".

Nesse sistema de câmeras inteligentes, além da captura, transmissão e arquivo de imagens, o sistema "interpreta" segundo categorias pré-definidas, o que é visto numa cena. Automaticamente, o sistema reconhece o que é significativo e o que é irrelevante, o que é regular e o que é irregular. Assim, por exemplo, o mesmo dispositivo pode ressaltar automaticamente na tela um objeto deixado na estação, indivíduos ou grupos de pessoas com comportamentos suspeitos, corpos se movimentando no contrafluxo ou qualquer outra situação previamente caracterizada

como devendo ser destacada no campo atencional da máquina e/ dos operadores de câmera. (BRUNO, 2012, p. 50).

De acordo com Kanashiro (2006 apud EVANGELISTA *et al.* (2016, p. 324):

> o barateamento da tecnologia e a consequente popularização do uso desses equipamentos tornaram quase impossível a circulação por espaços urbanos sem ser alvo das câmeras em algum momento. As novas tecnologias digitais de processamento de imagem potencializam práticas de identificação. O uso disseminado e descontrolado interfere na administração de espaços públicos pela intensificação do policiamento preventivo, permitindo abusos ligados ao chamado racial *profiling*[1] e à *gentrificação*[2]. Praças públicas, por exemplo, cuja seleção dos circulantes interessa ao setor imobiliário, são monitoradas para darem base à expulsão de populações indesejadas.

Na sociedade atual, onde temos as redes sociais e o Google, diz que não existe muralha que possa separar mundo interior do exterior, visto que o globo como um todo está se transformando em um mundo panóptico. Para o autor hoje a supervisão não se dá como se admite usualmente, como agressão à liberdade. Ao contrário, as pessoas se expõem livremente ao olho panótico. Elas colaboram intensamente na edificação do panótico digital na medida em que se desnudam e se expõem. O presidiário do panóptico digital é ao mesmo tempo o agressor e a vítima, e nisso é que reside a dialética da liberdade, que se apresenta como controle. (HAN, 2017, p. 115)

De acordo com Costa (2004, p. 161):

> Gilles Deleuze (1990) diferencia a sociedade disciplinar (Foucault, 1979) da sociedade de controle. Foucault chamava de sociedade disciplinar aquele período na história compreendido entre o século XVIII até a Segunda Guerra Mundial. Essa sociedade era caracterizada por uma repartição dos espaços em meios fechados; trabalhos, escolas, religiões, instituições, etc, em que o controle social era mais nítido, podendo ser aplicado às diversas formações sociais. No caso da sociedade do controle, a principal característica está na "interpenetração dos espaços, por suposta ausência de limites definidos (a rede)

A vigilância digital é uma espada afiada cuja eficácia ainda não sabemos como reduzir – e obviamente, uma espada com dois gumes, que ainda não conseguimos manejar com segurança. Os autores tratam da sociedade moderna,

---

1 Perfilamento racial (expressão do idioma inglês americano Racial profiling) é o ato de suspeitar ou visar uma pessoa de uma determinada raça, com base em características ou comportamentos observados ou assumidos de um grupo racial ou étnico, em vez de uma suspeita individual. In: https://pt.wikipedia.org/wiki/Perfilamento_racial.

2 Em sua definição primeira, o termo refere-se a processos de mudança das paisagens urbanas, aos usos e significados de zonas antigas e/ou populares das cidades que apresentam sinais de degradação física, passando a atrair moradores de rendas mais elevadas. In: https://ea.fflch.usp.br/conceito/gentrificacao.

que amplamente se expõe e que é demandada pelas mídias sociais (com a auto-exposição como uma necessidade de se exibir, tornar visível, se fazer existir), pelo marketing digital de consumo, que rastreia e monitora os seus clientes, cuja vigilância líquida se desenha e se opera atualmente. Reforçam sobre a dificuldade de se conjugar o poder que faz as coisas serem feitas e o poder capaz de garantir que sejam feitas coisas certas (costumávamos chamar esse segundo poder de "polítíca"), bem como a dificuldade das agências de governo de se adequar à grandiosidade desta tarefa (BAUMAN; LYON, 2013, p.134).

Ou seja, a vigilância cada vez mais se faz presente em suas diversas formas e pode ser usada tanto para o bem, quanto para o mal.

De acordo com a constatação da pesquisa de Firmino *et al.* (2013, p. 71):

> a criação e uso de sistemas CCTV não é considerada na perspectiva de uma interpretação sociotécnica, que é refletido diretamente na falta de preocupação em termos regulatórios sobre as possíveis implicações de seu "uso ou falta de uso".

A quanto ao modo como as câmeras de segurança são utilizadas, temos a advertência que não se deve descurar da utilidade das câmeras de vigilância em certas situações e mesmo de sua eficácia como aliada na manutenção da segurança, consideradas suas limitações e usos específicos, contudo, também não se pode negligenciar o modo como esse instrumento está sendo utilizado nos espaços públicos, por quem, com que treinamento, com quais critérios de suspeição sobre os indivíduos, com qual tecnologia, ofertando quais resultados favoráveis e, principalmente, com que preocupações em relação ao direito de privacidade das pessoas (MELLO, 2009, p.14).

Para Mello (2009, p. 15):

> O que há que se entender, enfim, é que o problema não se situa apenas no âmbito do controle da criminalidade. É indiscutivelmente mais amplo, abarcando considerações sobre políticas de segurança pública, crescimento da segurança privada, urbanismo, cidadania e observância de direitos fundamentais como a própria segurança, a privacidade e a dignidade da pessoa humana. Sem enfrentá-los de maneira clara, técnica e legítima, restará apenas o proselitismo.

Lemos *et al.* (2011, p. 143) argumentam que:

> Ao mesmo tempo em que temos um maior acesso à informação e podemos nos conectar a pessoas em quaisquer lugares do planeta, nunca fomos tão vigiados, filmados, catalogados e registrados como hoje. Câmeras de segurança, cartões de crédito, senhas, sensores, etiquetas de rádio frequência, serviços baseados em localização (LBS e LBT) são mecanismos

> presentes na vida das cidades contemporâneas e colaboram para a interpenetração dos espaços, para o controle e ameaça à privacidade e ao anonimato nas sociedades contemporâneas. Devemos reconhecer esta nova conjuntura.

Destacam os autores Lemos *et al.* (2011, p. 144) que há por um lado, o sujeito que quer reagir às câmeras na luta pelo direito à privacidade e à liberdade individual e, por outro, a segurança social e o controle visível do movimento do outro, sempre ameaçador.

No uso de câmeras com reconhecimento facial, maior é o risco em algum momento de nos depararmos com situações que podem beirar o conflito com a proteção dos direitos humanos dentro de um novo rol da considerada "5ª geração dos direitos humanos" (PINHEIRO, 2021, p. 182).

Seguindo o raciocínio da autora acima, vamos ao rumo maciço das soluções de inteligência artificial e ao debate sobre a transparência dos algoritmos, com a aplicação das novas regulamentações de proteção de dados que, em seus princípios trazem a necessidade de não discriminação, além da proteção da privacidade e da transparência. Mas também trazem uma série de exceções para, justamente, permitir o exercício da segurança pública.

Como visto, em muitas cidades são utilizadas câmeras de vigilância pelos gestores das áreas de segurança pública, sendo uma ferramenta para a elucidação de crimes possibilitando a geração de provas contundente de autoria e materialidade, estas podem ser utilizadas como parte de um conjunto de sistemas, a exemplo da integração com sistemas voltados a mobilidade, que fazem parte de uma cidade inteligente.

As câmeras dotadas de inteligência embarcada, apesar apresentarem um custo maior, inicialmente, para a implantação, podem trazer economia, além de serem apontadas como mais eficientes, pois além de diminuir a quantidade de equipamentos para determinada área de cobertura, também requer um número menor de pessoas para o monitoramento, bem como, podem trazer em destaque informações direcionadas como identificação de ameaças, otimizando a apresentação das informações, diante do grande volume de dados a serem geridos.

Assim, considerando que o urbano é um sistema dinâmico, os meios aplicados pelo Estado para fornecer a sensação de segurança também precisam estar em constante inovação e ajustar-se às novas necessidades, de forma a melhor

atender ao interesse público e as necessidades da sociedade. E, considerando a evolução das câmeras de vigilância, com camadas adicionais de inteligência, denominadas "*smart cameras*", esta ferramenta tem se apresentado, como uma alternativa para a gestão mais eficiente da segurança pelo Estado.

As *smart cameras* operam através de softwares (também chamados de video analytics) que filtram e analisam as imagens segundo algoritmos que ressaltam indivíduos, objetos, atitudes que devem ser o foco de atenção da 'cena", conforme as aplicações predefinidas no sistema. (BRUNO, 2012, p. 48.)

Nesse cenário, se apresentam desafios para o gestor público, especialmente da área de segurança, devendo agir com base nos princípios constitucionais, mediante uma gestão ética e responsável, face à escassa regulamentação do assunto e dos interesses que podem estar por trás do uso desta tecnologia.

A administração com base na ponderação de interesses tem a possibilidade de vigiar a sociedade sob a justificativa pela busca da efetividade do direito à segurança pública, sopesando os direitos em conflito, verificando o caso concreto, em contraponto ao direito à privacidade, resguardados os dados pessoais, é mais do que justificada a vigilância sob o argumento do interesse público. A Administração tem o dever de agir de acordo com a legalidade, com o regular processo de contratação e fiscalização, agindo a Administração com transparência, de acordo com os preceitos da moralidade, nos limites da competência do órgão (acessar mediante convênios específicos, com usuários legitimados ao acesso dos dados).

### 3.5.4 Sistema de Semáforos Inteligentes

Os Semáforos de Controle Inteligente de Tráfego estão sendo pensados com o propósito de otimizar a operação da rede de sinalização semafórica da cidade, melhorando o rendimento da capacidade viária instalada, diminuindo os congestionamentos e proporcionar segurança viária.

A implantação de semáforos inteligentes tem como objetivo organizar o tráfego de veículos, melhorar a circulação, diminuir o tempo de espera e reduzir o tempo gasto no percurso dos diferentes modais de transporte e desta forma, atenuar a emissão de gases produzidos pelos veículos e consequentemente melhorar a qualidade de vida do cidadão.

A estrutura dos equipamentos semafóricos, assim como os dados produzidos podem ser acessados pela inteligência de segurança pública para o exercício de suas atividades, numa ação integrada com outras áreas. A título de exemplo temos os acordos de cooperação firmados pela Polícia Rodoviária Federal com os municípios onde passam rodovias federais, permitindo o acesso aos dados das câmeras tanto de radares, quanto de controle de tráfego, as quais podem fazer leituras de placas de veículos e assim, fornecer dados para as agências de segurança pública.

### 3.5.5 O Uso do Reconhecimento Facial (Biometria) na Segurança Pública

No âmbito da segurança pública, o Brasil já conta com utilização da tecnologia de reconhecimento facial desde 2011 e a despeito da ampla utilização da biometria de face na segurança pública no Brasil, não existe, atualmente, uma norma de âmbito federal que regule os limites dos sistemas de vigilância e tampouco que regule a proteção de dados e da privacidade relacionadas ao reconhecimento facial na segurança pública (ARAÚJO; CARDOSO; PAULA, 2021, p. 4-9).

Além da necessidade de regulamentação no âmbito federal, visto que a LGPD exclui expressamente de seu âmbito de incidência o tratamento de dados na segurança pública, traz-se que é indispensável o controle das fontes primárias dos algoritmos. Conforme Araújo, Cardoso e Paula (2021, p. 11):

> É dizer, os sujeitos responsáveis por sua elaboração e programação, conquanto capazes de influir no funcionamento do sistema, merecem atenção dos responsáveis, a fim de que essa influência não acabe por perpetuar pré-conceitos.

Ainda, de acordo com Araújo, Cardoso e Paula, (2021, p. 9)

> cabe aos aplicadores da lei penal apreciar a validade da informação obtida através de algoritmos de reconhecimento facial, a fim de que a credibilidade do sistema não se sobreponha a garantia de igualdade e a presunção de inocência.

A identificação incorreta de um falso positivo, no entanto, é uma situação que pode ocorrer quando um algoritmo diz que duas fotos são da mesma pessoa, quando, na realidade, não são. Ou seja, diante de um falso reconhecimento, uma pessoa pode ser indevidamente detida pela acusação de um delito, ou, na fase investigativa pode gerar o comprometimento da memória do reconhecedor, que

poderá reproduzir o erro na fase judicial e contribuir para formação de uma condenação injusta. (ARAÚJO, CARDOSO; PAULA, 2021, p. 9).

Além dessas preocupações trazidas, ainda o Estado pode arcar com indenizações por danos materiais e morais, trazendo prejuízo aos cofres públicos.

Em que pese as preocupações, fato é que no Brasil, vem sendo utilizado pela segurança pública, com mais de vinte estados brasileiros já com processos de licitação instaurados para compra de tecnologia dessa natureza (NUNES, 2020), e segundo Araújo, Cardoso e Paula, (2021, p. 9): “um marco no reconhecimento facial na segurança pública ocorreu em 2019, quando, no estado da Bahia, mais de cem pessoas foram presas mediante uso da tecnologia”.

A Lei Geral de Proteção de Dados, excluiu do seu âmbito de aplicação a segurança pública, assim carece a matéria de regulamentação federal. O que se tem é a Portaria nº 793, de 2019, do Ministério da Segurança Pública, que prevê o fomento à implantação de sistemas de vídeo-monitoramento, com soluções de reconhecimento facial, mediante financiamento do Fundo Nacional de segurança Pública (BRASIL, 2019).

Os autores acima citados, citam o anteprojeto de lei que está em tramitação e visa regulamentar a matéria do tratamento de dados no âmbito da segurança pública, investigações penais e repressão de infrações penais (ARAÚJO, CARDOSO; PAULA, 2021, p. 10).

Outros exemplos de aplicações que podemos destacar: a) iluminação pública; b) energia solar c) videomonitoramento (totens) d) radares/fiscalização de velocidade com leitura de placa de veículos (*Optical Characteres Recognized* - OCRs); e) gestão dos resíduos sólidos; f) fiscalização da poluição; g) monitoramento de pontos de alagamento, entre outros.

**Figura 2** - Poste para eficientização da iluminação pública e infraestrutura de comunicações


**Fonte**: IPGC Instituto de Planejamento e Gestão de Cidades (apud EFICIENTIZAÇÃO [...], [2020?], p. 13)

No cenário das cidades inteligentes, não temos como tratar da segurança pública e mais específico da atividade de inteligência, sem pensar que todos os assuntos estão correlacionados. Um poste de iluminação, ao mesmo tempo que mede a qualidade do ar, pode dispor de câmera identificando pessoas, coletando informações mediante microfones, identificar a exata posição dos veículos, tudo servindo a atividade de inteligência que além das suas atividades voltadas à segurança, servirão para subsidiar decisões de gestão e planejamento, decidindo o futuro e o foco de interesse de determinada área.

## 3.6 INTELIGÊNCIA DE SEGURANÇA E CIDADES INTELIGENTES: DESAFIOS E PERSPECTIVAS

Conforme a Carta Brasileira para Cidades Inteligentes, recomenda-se fortalecer a articulação entre governos para consolidar a governança urbana multinível (que atua em vários níveis - nacional, regional, estadual e local), interfederativa (com cooperação entre diferentes entes da federação - União, Estados, Municípios e Distrito Federal) e intersetorial (com cooperação entre as diferentes áreas de política pública). Firmar o papel dos governos estaduais e

federal no apoio à adaptação de recomendações e políticas para os contextos locais em conjunto com os municípios (BRASIL, [2020], p. [1]).

Recentemente entrou em vigor a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) a qual incluiu o Brasil no rol de países que contam com uma legislação específica para a proteção de dados semelhante ao Regulamento Geral sobre a Proteção de Dados da União Europeia, de 2018.

No entanto, de acordo com Pinheiro (2021, p. 165) “existem desafios jurídicos ligados diretamente à segurança da informação, não podendo deixar de mencionar aqueles relacionados à proteção de dados pessoais: propriedade, tratamento, uso e segurança de dados gerados por IA (Inteligência Artificial) e dispositivos IoT; e, infraestrutura de cidades inteligentes”.

Quanto aos desafios que se apresentam para que as cidades tenham êxito, Santos Filho e Coêlho (2018, p. 69-76) destacam: a) qualidade de vida, b) integração de serviços e c) participação da população nas decisões. Quanto à qualidade de vida traz o problema da mobilidade urbana, uma dos grandes desafios enfrentados pelos gestores e pela população em geral, onde os congestionamentos urbanos são responsáveis por um grande desperdício de tempo, combustível e na geração de poluentes causadores de problemas de saúde, ainda o problema com o meio ambiente, onde o padrão de consumo de recursos naturais tem crescido mais do que a capacidade do próprio planeta em recuperá-los, o que implica em desafios logísticos, como os lixões (SANTOS FILHO; COÊLHO, 2018, p. 71).

Diferentes governos e setores da sociedade devem cooperar para os sistemas funcionarem de forma integrada, responsável e inovadora. Com segurança cibernética e garantia de privacidade pessoal. Devem cooperar para oferecer um ambiente de ética digital que assegure dados compartilhados e abertos, sempre que possível, e que garanta proteção jurídica às pessoas.

Em uma sociedade mais digital, temos uma nova geração de direitos – os “ciberdireitos”, assim, cuidando do direito à privacidade, nesta área, leva-se a outro do direito o de criptografia de dados. A preocupação, portanto, que merece ser destacada é a correta gestão dos dados, incluindo a propriedade, o tratamento, o uso e a segurança dos dados pessoais.

De acordo com Carnevali e Alcântara (2020, p. 106) “um fator importante para a implantação de uma cidade inteligente e o seu sucesso é a participação cidadã

tanto no estudo quanto no retorno para que tenha êxito na sustentabilidade da cidade”.

Um item que se destaca é o custo de implantação de tecnologias de comunicação e informação visando “construir” uma cidade inteligente. A TIC ainda é muito cara e são poucas cidades que investem em sistemas inteligentes, no entanto, com novos avanços produtivos os custos tendem a cair, refletindo, portanto, no aumento futuro de cidades inteligentes (CARNEVALI; ALCÂNTARA, 2020, p.106).

A questão do mercado de vigilância por câmeras, por sua vez, tem sido muito valorizada. O mercado se expande cada vez mais e se apresentam novas tecnologias que são empregadas para satisfazer a demanda associada.

No entanto, conforme observa Firmino *et al.* (2013, p. 81), há uma falta de preocupação do setor jurídico em compreender a lógica por detrás do uso dos sistemas de monitoramento por câmeras e suas possíveis implicações para a privacidade, as liberdades individuais e a organização dos espaços das cidades.

> On the one hand, security is highly valued, as, consequently, is all the technology related to private personal and property security, and a market exists to satisfy the associated demand. On the other, the legal environment is permeated by a lack of concern about understanding the logic behind the growing use of CCTV systems and their possible implications for privacy, individual liberties, and the organization of spaces in cities (FIRMINO *et al.,* 2013, p. 81).

Ou seja, esse cenário apresenta desafios para o gestor público, especialmente da área de segurança, assim, a atuação exige-se que as ações no âmbito do poder público sejam baseadas nos princípios constitucionais, mediante uma gestão ética e responsável, face à escassa regulamentação do assunto e dos interesses que podem estar por trás do uso desta tecnologia.

Para as atividades governamentais, a inteligência de segurança pública não é apenas um desafio – é um grande obstáculo para a transformação digital há muito aguardada. Além disso, hackear informações do setor público pode pôr em perigo a segurança nacional, bem como a confiança dos cidadãos.

Quando se trata de segurança de dados, tanto agências privadas quanto públicas podem dispor de dados altamente sensíveis que podem ser lucrativos nas mãos dos criminosos.

Os serviços de empresas privadas de segurança cibernética têm se apresentado como uma grande oportunidade para as Agências de Inteligência em obter informações estratégicas relevantes. Adverte, no entanto, a necessidade de os

Serviços de contrainteligência realizarem grandes investimentos, visando aperfeiçoar as medidas de defesa contra *spywares*, o que representa um desafio constante a ser superado. (XAVIER, 2022, p. [1]))

Para Xavier (2022, p. [1])):

> O governo, no entanto, armazena muito mais dados que o setor privado, e muitas vezes mantém sistemas mais velhos e vulneráveis. Assim aqueles com uma visão de transformação do governo digital estão encontrando a segurança cibernética como um grande desafio.

Conforme Pinheiro (2021, p. 158), nas contratações públicas é preciso adotar preferencialmente padrões abertos para evitar que a Administração se torne "refém" de fornecedores, ou seja, evitar uma compra futura forçada de peças de reposição e equipamentos complementares da mesma marca/fabricante primária, podendo também dificultar a expansão e interligação dos serviços.

A utilização de dados abertos, além de possibilitar uma ampliação da concorrência na contratação dos sistemas e sua manutenção, também possibilita que sejam disponibilizados de forma gratuita, atendendo também ao desejo de transparência na governança. Em se tratando de riscos da IoT, *smart cities* e inteligência artificial, conclui-se que a existência de riscos não deve eliminar os projetos ou ideias, e sim ajudar a moldar as práticas e soluções no caminho correto, lícito e seguro juridicamente (PINHEIRO, 2021, p. 159).

Importante alerta aos gestores no que diz respeito a segurança dos próprios sistemas. No caso de cidades inteligentes, a questão de segurança se torna cada vez mais séria, pois, com tantos pontos nevrálgicos sobre gestão digital, os responsáveis por tais serviços devem contratar pessoal técnico altamente especializado, realizar auditorias de segurança e verificar os códigos dos sistemas para prevenir o vazamento de dados, além de monitorar acessos e a utilização dos recursos, bem como, as técnicas de inteligência artificial, monitorar anomalia nos serviços e ter um plano rigoroso de respostas a incidentes e recuperação de desastres presente e revisado periodicamente (PINHEIRO, 2021, p. 159)

Estas ferramentas tecnológicas devem ser utilizadas com cautela, pois podem ser transformadas em "poderosas armas de controle social" (LYON, 1994, p. 6 *apud* VAZ-FERREIRA; RORIGUES, 2021, p. 34-44), na forma de vigilância (*surveillance*). O grande desafio para as cidades tecnológicas e para o governo eletrônico é

preservar a segurança e a privacidade dos dados, ou seja, é necessário aumentar as estratégias que preservem a *cibersegurança*.

Os crimes cibernéticos (digitais ou virtuais) são definidos por Marion e Twede (2020, p. 12 *apud* VAZ-FERREIRA; RORIGUES, 2021, p. 34-44) como sendo "qualquer crime que envolva um computador ou uma rede" incluindo como crimes cibernéticos ofensas e acesso, comprometimento de dados, uso indevido de dispositivos e interceptação de dados.

O ciberespaço é mais amplo que o conceito de internet ou rede mundial de computadores, ele constitui-se ainda em rede de telégrafo, de rádio amador, de telefonia fixa/móvel, de televisão via satélite, sistemas de tráfego aéreo e de navegação marítima, abrangendo também as intranets, tecnologias de telefonia celular e comunicações via satélite.

De acordo com Xavier (2022, p. [1]):

> tem se verificado no ciberespaço o uso cada vez mais frequente de empresas privadas de segurança cibernética, devido ao incremento das atividades cibernéticas ilícitas no mundo, bem como a Guerra Cibernética entre alguns Estados

Xavier (2022, p. [1]) destaca que as empresas têm desenvolvido programas (softwares) que possuem uma grande capacidade de realizar espionagem, justificando o seu desenvolvimento como ferramentas para o combate ao terrorismo e ao crime organizado.

A preocupação, no entanto, é que alguns Estados estão utilizando essas soluções computacionais para realizar espionagem contra opositores a seus governos e a alvos de interesse como jornalistas e autoridades de países e organismos internacionais. Xavier (2022, p. [1]) cita como exemplo os EUA que, por meio da sua agência de inteligência National Security Agency – NSA, que teve como referência o USA Patriot Act, utiliza do mesmo expediente para espionar alvos de interesse estadunidense, tanto no país como no exterior. Cita ainda, o software *Pegasus* da empresa israelense NSO Group que, conforme investigações internacionais, teria sido empregado, também, na espionagem de altos líderes governamentais.

Para o autor:

> Esse fenômeno tem sido motivo de preocupação por parte de várias organizações defensoras dos Direitos Humanos, como a Anistia Internacional, bem como pela Alta Comissária dos Direitos Humanos da

> ONU, pois uma boa parte dos governos que os utilizam possuem um viés antidemocrático e repressor, o que reforça a ideia de vários analistas de que essas empresas devem ter uma regulamentação internacional, com o intuito de não haver violações a direitos e liberdades, dentre elas a de expressão, privacidade e de manifestação. (XAVIER, 2022, p. [1])

A esfera pública é uma grande produtora e coletora de dados, possuindo um "gigantesco acervo, que é um recurso valioso que pode ser usado pelas partes interessadas para uma infinidade de propósitos" (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2020, p. 50). Neste contexto, é essencial que exista um arcabouço jurídico efetivo que proteja os dados pessoais. (VAZ-FERREIRA; RORIGUES, 2021, p. 40)

Como medidas preventivas técnicas, a esfera pública deve assegurar que a sua defesa eletrônica seja tão impenetrável quanto possível, por meio da utilização de antivírus, firewalls, *intrusion prevention systems* (IPS), filtragem de e-mail, entre outros recursos tecnológicos. Além de uma política e de processos robustos de cibersegurança, deve-de investir em um sistema de educação para que os utilizadores possam saber como se prevenir e lidar com os ataques (VAZ-FERREIRA; RODRIGUES, 2021, p. 40)

De acordo com o art. 52, §1º, da LGPD, o comportamento preventivo, como investimento em sistemas robustos de cibersegurança e realização de treinamentos poderá auxiliar na minimização das sanções decorrentes da LGPD.

A integração entre entes governamentais e a sociedade civil, no entanto, é de fundamental importância pois pode resultar em economia de recursos, atuando os diversos órgãos e entidades em colaboração mútua, resguardadas a supremacia da Administração em receber os dados. A área de inteligência pública, por sua vez, utilizará os dados em prol da segurança, devendo a Administração Pública tratar com o devido cuidado os dados em geral e os dados pessoais sensíveis, atuando com base nos princípios da legalidade, da moralidade e da proteção do direito à privacidade.

Assim, a questão que o tema instiga é como a atividade de inteligência em segurança pública pode se utilizar das tecnologias digitais, seja com recursos de vídeo-monitoramento dotado de camadas de inteligência, sistema de reconhecimento facial, sistemas de leitura de placas de veículos, entre outros, para melhorar a vida do cidadão e tornar a gestão pública mais eficiente, cumprindo o Estado o seu dever de garantir a segurança pública e a paz social, no contexto das chamadas cidades inteligentes.

O Sistema de reconhecimento facial é uma tecnologia de monitoramento de dados biométricos. Há um cenário de adoção progressiva e iminente de uma ferramenta que ainda apresenta muitos riscos. As preocupações são quanto ao potencial de vigilância em massa, as possíveis violações às liberdades individuais.

Questões éticas relacionadas ao uso da tecnologia (IA) também precisam ser considerados.

Percebe-se que um dos desafios é a gestão dos diversos sistemas, mas trata-se de uma oportunidade para a construção de cidades inteligentes, podendo fazer uso mais racional e eficiente dos recursos naturais, financeiros e humanos, objetivando a melhoria da qualidade de vida. Neste contexto de construção das “smart cities”, a promoção do desenvolvimento nacional sustentável é tema que cada vez mais ganha destaque pela doutrina, considerando a nova postura que deve a Administração Pública assumir perante a sociedade, inclusive como forma de primar pelos princípios fundamentais.

Os desafios que podem ser apontados à implantação da cidade inteligente são multifatoriais, visto que o tema pode ser tratado como uma mudança de paradigma, onde toda a dinâmica da cidade, tem um novo direcionamento. Entre os desafios, destacamos a necessidade de planejamento do município, que pode iniciar pela construção de um plano, onde busca identificar como a cidade consegue utilizar a tecnologia para desenvolver suas vocações, tornando as regiões mais inteligentes, humanas, inclusivas, seguras e sustentáveis.

Hoje, cidade inteligente significa cidade resiliente e sustentável, isto é, com flexibilidade e capacidade de adaptação; capaz de dar respostas rápidas e eficientes às ameaças externas, como, por exemplo, mudanças climáticas, desastres, chuvas intensas, furacões, ou, simplesmente, atender aos princípios básicos de segurança alimentar ou de qualquer outra natureza.

Uma cidade inteligente portanto, requer o pensamento voltado à sustentabilidade, ou seja, é essencial maximizar os benefícios e minimizar o risco da tecnologia de cidade inteligente, para que toda a sociedade possa se beneficiar e viver com qualidade.

Nesse contexto, a tecnologia utilizada pelas cidades inteligentes, ou seja, pelo sistemas e dispositivos que conectam as relações da sociedade (pessoa/IoT...) vem otimizar, proporcionar uma coleta, compilação, filtro e análise de dados, favorecendo a atividade, sendo uma oportunidade para as instituições encarregadas da atividade

de inteligência de segurança pública para consolidar sua atuação e fortalecer os níveis de integração e intercâmbio de dados e conhecimentos, favorecendo a gestão da segurança pública.

Por outro lado, o desenvolvimento das formas de comunicação também apresenta desafios à segurança e à atuação objetiva das instituições de inteligência de segurança pública, sobretudo pelo aumento do volume de dados produzidos, compartilhados e expostos (Decreto 10.778) (BRASIL, 2021, p. 4). Destacando-se a importância de uma inteligência de segurança pública voltada para a ciência de dados, preparada para lidar com a coleta, busca, estruturação e análise de grandes volumes de dados.

Este estudo se justifica pelo atual cenário do século XXI, onde a internet tem cada vez mais conectado pessoas e equipamentos, estabelecendo uma nova interação entre o gestor público e o cidadão. As cidades apresentam novas demandas, com novos desafios e a tecnologia se mostra uma importante ferramenta de gestão, possibilitando atuar com mais efetividade, de modo a melhorar a qualidade de vida.

Visando a construção do que se denomina uma cidade inteligente ou "*smart city*", muitos projetos têm sido propostos e já implementado, ganhando destaque a tecnologia baseada em geoprocessamento, a instalação de dispositivos eletrônicos de coleta de dados e sistemas informatizados, que traz novas experiências e interações entre o poder público e os seus moradores.

De acordo com Costa (2014, p. p. 108-122), como critério universal, a Cidade Inteligente deve incluir a sustentabilidade, com a finalidade de garantir que uma nova racionalidade será aplicada para tornar o aglomerado urbano compatível com um novo conceito de progresso e um novo estilo de vida.

# 4 CONSIDERAÇÕES FINAIS

O presente trabalho tratou da inteligência de segurança pública no contexto das cidades inteligentes (*smart cities*), considerando a relevância do tema na atualidade no que se refere ao desenvolvimento da sociedade.

Desde os primórdios da civilização quando se intensificaram as relações entre as pessoas com a trocas de produtos, o mercado e a vida em tribos, que a preocupação com a segurança é observada.

A vida moderna tem levado a grande concentração de pessoas em cidades requerendo, assim, a atuação permanente e em tempo integral dos órgãos de segurança.

Na sociedade da informação, com a tecnologia avançando numa velocidade sem igual, os dispositivos de segurança têm sido desenvolvidos de forma a propiciar a vigilância de modo cada vez mais minucioso e ao mesmo tempo com grande raio de abrangência e agilidade. Prova disto são os sistemas de informação e comunicação, com os dispositivos, máquinas e sistemas proporcionando o que se denomina uma cidade inteligente.

A internet, por sua vez, tem cada vez mais conectado pessoas e equipamentos, estabelecendo uma nova interação entre o gestor público e o cidadão. As cidades apresentam novas demandas e também novos desafios nas mais diversas áreas e a tecnologia da informação (TI) se apresenta como uma ferramenta de gestão também na área da segurança pública, que pode se utilizar dos mais variados sistemas e dispositivos e atuar com mais efetividade na gestão dos espaços e no combate à criminalidade.

Verificou-se que no atual cenário das cidades, a implantação de dispositivos e sistemas de informação e comunicação tem proporcionado maior potencial de atuação da atividade de inteligência de segurança pública, visto o grande volume de dados coletados, que pode ser considerado a “matéria-prima” da atividade de inteligência, tornando-se farta, no entanto, a área da inteligência, assim como os demais setores públicos e privados, têm o desafio de gerir a imensa quantidade de dados e da mesma forma deverá se socorrer de sistemas, visto que a atividade humana mecânica de controle não dará conta da gestão deste imenso volume de dados.

Feito um levantamento histórico da atividade de inteligência de segurança, se entendeu por enfatizar os marcos legais da atividade no Brasil. E se pôde verificar que a atividade de inteligência, outrora denominada de informação, apesar de ser instituída da década de 1920, no Brasil, num regime democrático, desenvolveu-se e teve relevante consolidação no período da ditadura militar. O desenvolvimento da atividade de inteligência, neste período, foi de grande importância, inclusive estratégica para o Brasil, incluindo posicionamentos quanto a decisões de governo de apoiar ou não movimentos militares, desenvolvimento das radiocomunicações, numa época em que se especializou a mão-de-obra militar, com troca de conhecimentos com o exterior, tanto com agentes externos quanto dos internos altamente qualificados.

Na época da ditadura foi de fundamental importância na repressão de atos dos rebeldes e contrários ao sistema instituído, especialmente após a instituição do AI 5, e conforme o movimento de redemocratização do país foi se fortalecendo e novos programas de governo sendo escolhidos a exemplo do período após 1990, cuja atividade, teve menos prestígio da parte do governo, mas mesmo assim, cada área, especialmente das forças armadas, marinha, exército e aeronáutica mantiveram suas atividades, assim como a polícia federal, as polícias estaduais civil e militar.

Entre os anos 2000 e 2018, no governo, por exemplo, foram publicadas as doutrinas, atualizados os documentos, no entanto, também sem muita ênfase em termos de destaque institucional.

Já, a partir de 2018, com a instituição do SUSP, começam a ser revistos os instrumentos e as políticas de inteligência, sendo definida e regulamentada a política nacional de Inteligência de Segurança Pública, estando a coordenação do Sistema Brasileiro de Inteligência (SISBIN), sob a responsabilidade da Agência Brasileira de Inteligência (ABIN), agora ligada à Casa Civil da Presidência da República.

Desde há muito tempo as cidades já possuem câmeras de vigilância instalada, no Brasil, começou na década de 1980, iluminação pública e outras instalações de infraestrutura. No entanto, recentemente, sensores foram embutidos nestas câmeras e também nos postes de iluminação pública, de forma que podem medir a temperatura, a umidade e poluição do ar, câmeras para contagem de veículos, o movimento dos carros, das pessoas, ou de situações perigosas, de forma que hoje se tem os chamados postes inteligentes, com câmeras inteligentes. Ou

seja, os sistemas e dispositivos são utilizados para diversas finalidades e ao mesmo tempo estão propiciando a atuação da inteligência de segurança pública, confirmando a hipótese de que os investimentos vêm favorecer a segurança pública no âmbito das cidades.

Há inúmeras câmeras em espaços públicos e privados, em casas, condomínios, carros, praças e os próprios aparelhos telefônicos que a todo momento captam dados e imagens. Tais dispositivos, na área de inteligência de segurança pública são muito úteis, visto que podem servir e ser acessadas pela área da segurança pública, tais como polícia militar, polícia civil, órgãos de investigação do ministério público, exército, polícia federal, secretarias municipais de segurança pública, entre outros.

A busca por aprimoramento e pelo conhecimento dos sistemas, o investimento em inovação tecnológica e capacitação técnica por outro lado é primordial, visto a velocidade de novos sistemas e tipos de ilícitos. E para antever, prevenir, a gestão pública terá que estar acompanhando as mudanças e mesmo se adiantando visando antever situações críticas que podem ser evitadas ou minimizadas. No entanto, é um desafio para os governos, dada a estrutura da atividade, que é institucionalizada. E o crime organizado, cibernético inclusive, tem uma massa grande de produtores, enquanto que a estrutura governamental é mais limitada.

Assim, justifica-se que alguns governos efetuem parceria com empresas especializadas de sistemas para atuar em conjunto com o governo, no monitoramento, controle e defesa (contrainteligência).

É também ponto de consenso que a integração das forças de segurança é fundamental para o sucesso das atividades das diversas agências de segurança pública. Para gerir a enorme quantidade de dados produzido pelos diversos dispositivos, há necessidade de sofisticados sistemas de gestão, utilizando-se da tecnologia denominada “Big Data” servindo para atividade de inteligência na produção do conhecimento e para a melhoria da gestão pública. A segurança pública, por sua vez, é a justificativa que fundamenta a constante vigilância e captação de dados.

A formalização de parceria já ocorre, mas a intensificação nos convênios, para uso compartilhado de dados, a integração de sistemas, o uso de dados nacionais, sistema da carteira nacional de trânsito, carteira de identidade nacional,

uso dos sistemas nacional ou estadual (SISP) otimizando os recursos dos fundos públicos.

Por outro lado, fica aberta a questão da vulnerabilidade das pessoas que ficam expostas aos mais diversos dispositivos, como por exemplo as câmeras de vigilância, radares de fiscalização eletrônica do trânsito e leitores de placas de veículos com dispositivo de leitura automática de caracteres, que podem captar dados pessoais e individualizados e que, sem dúvida, requer uma conduta por parte dos atores da área de segurança pública, em todas as circunstâncias, baseada nos padrões éticos que vise sobretudo a proteção dos direitos fundamentais.

A segurança dos dados pessoais pelas empresas privadas que prestam serviços ao governo, portanto, é mais um desafio se impõe, visto que a empresa acaba por ter um poder na mão, o qual, mesmo que regulado, não é garantia de segurança, como por exemplo, a venda para outro país que não seja tão democrático ou que não tenha boa intenção, como uma guerra cibernética ou a obtenção de alguma vantagem comercial.

Em se tratando de implantação de cidades inteligentes ou *smart cities,* termo em inglês, se entendeu que é uma realidade decorrente do próprio desenvolvimento da tecnologia da informação e comunicação que permite de forma muito amplificada e ágil obter dados e desenvolver dispositivos e sistemas com vista a resolução de problemas que as cidades enfrentam no seu dia-a-dia.

Com o crescimento da população morando em aglomerados urbanos, os temas como a melhoria da infraestrutura e organização do trânsito, o controle da poluição do ar, da água, a correta gestão dos resíduos, a eficiência energética, a diminuição dos impactos ambientais decorrentes de novos materiais e processos, a reconstituição de espaços decorrentes de eventos climáticos são objeto dos sistemas desenvolvidos e melhorados a todo instante. Ou seja, nas atividades cotidianas mais diversas, os dispositivos individuais podem estar conectados diretamente com as forças de segurança transmitindo dados, em tempo real, visando resolver casos de crimes dos mais diversos ou suspeitas.

Importante destacar a necessidade de investimento em capacitação dos agentes públicos que trabalharão no planejamento dos espaços urbanos e nas contratações de sistemas, na gestão onde participem técnicos na área de informática, e que se invista também na educação voltada à população, saindo dos saberes tradicionais e incluindo os novos conhecimentos, como as novas

possibilidades das tecnologias de *blockchain*, computação e armazenamento de dados em nuvem, integridade de dados e proteção de dados individuais, economia inteligente, sustentabilidade inteligente, temas afetos as cidades mais inteligentes, sustentáveis e humanas.

Outro ponto que se verificou é a possibilidade de num futuro não distante, os limites territoriais, assim como a quantidade de pessoas, não terão tanta relevância para as cidades, mas sim a conectividade e o propósito das relações a serem estabelecidas com a cooperação entre as cidades e entre países, por várias tecnologias avançadas como inteligência artificial e internet das coisas, que serão muito importantes para a inteligência de segurança pública.

O Brasil tem buscado implementar cidades inteligentes, em que pese ainda a carência de investimentos em infraestrutura de rede de fibra ótica e da infraestrutura básica como esgotamento sanitário, abastecimento com água tratada e dos próprios sistemas viários que ainda se encontram em situações precárias. No entanto, as cidades necessitam estudar o seu potencial e os anseios locais, bem como avaliar as diferentes tecnologias.

No que se refere a normatização, temos no Brasil a Norma Brasileira ABNT NBR ISO 37122:2020 que especifica e estabelece definições e metodologias para um conjunto de indicadores de cidades inteligentes (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2020ª, p. [1]). No entanto, a aplicação da referida norma técnica demanda ser feita em conjunto com a NBR 37.120 e a NBR 37123, cujas normas trazem os indicadores de cidades, denominados "Desenvolvimento sustentável de comunidades" para serviços municipais e qualidade de vida, visando medir o progresso em direção a uma cidade inteligente.

A arquitetura de sistemas eletrônicos implantada na denominada *smart city* pode ser utilizada pela atividade de inteligência de segurança pública das diversas agências que atuam na base territorial do município, o que vem favorecer o planejamento de ações operacionais de prevenção do crime e da violência, então, pode-se afirmar que é recomendado o investimento pelo município, podendo tal projeto colaborar para a melhoria da percepção da segurança e proporcionar uma melhor qualidade de vida de sua população.

A sugestão para futuros trabalhos é o estudo da regulamentação do uso de câmeras de Vigilância e reconhecimento facial, bem como, as questões éticas quanto ao uso de dados. Também o estudo da “cibersegurança” e a pesquisa de

novos dispositivos e avaliação do estágios das cidades na aplicação de sistemas inteligentes, visto os indicadores constantes nas normas internacionais e nas próprias normas técnicas brasileiras, este trabalho pode servir de partida para alguma área de interesse, seja de inteligência de segurança pública, seja quanto às cidades inteligentes, cujas áreas convergem, incluindo a própria revisão das normas e o direcionamento do planejamento da cidade, visando implantação de sistemas inteligentes que favorecerão as ações de Inteligência em segurança pública e o melhor desenvolvimento das cidades.

## REFERÊNCIAS

ALDAIRI, Anwaar; TAWALBEH, Lo'ai. Cyber security attacks on smart cities and associated mobile technologies. **Procedia computer science**, [S. l.], v. 109, p. 1086-1091, 2017.

ALVES, Fernanda Mendes Sales. Segurança pública, cidadania e controle social. p. 1384. **Revista de artigos do 1º Simpósio sobre Constitucionalismo, Democracia e Estado de Direito**, Marília, v. 1, nov. 2016. Disponível em: https://revista.univem.edu.br/index.php/1simposioconst/article/view/1179. Acesso em: 10 jul. 2021.

ANDRADE Transformação, Cristiana R. D'Oliveira; GONÇALO, Cláudio R.; SANTOS, André M. digital com agilidade: A emergente capacidade dinâmica de serviços complementares. **RAM:** Revista de Administração Mackenzie, [S. l.], v. 23, n. 6, p. 1-48, 2022. Disponível em: https://www.scielo.br/j/ram/a/jZctWGWmKHwyX6tLCTzH3jt/?format=pdf&lang=pt. Acesso em10 jul. 2021.

ARAÚJO, Romulo de Aguiar; CARDOSO, Naiara Deperon; PAULA, Amanda Marcélia de. Regulação e Uso do Reconhecimento Facial na Segurança Pública do Brasil. **Revista de Doutrina Jurídica**, Brasília, DF, v. 112, e021009, 2021. Disponível em: https://revistajuridica.tjdft.jus.br/index.php/rdj/article/view/734. Acesso em: 10 jul. 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 37122**: cidades e comunidades sustentáveis: indicadores para cidades inteligentes. 1.ed. Rio de Janeiro: ABNT, 2020a. Disponível em: http://www.abnt.com.br/smartcities.. Acesso em: 10 jul. 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Certificação de indicadores para cidades e comunidades sustentáveis**. Rio de Janeiro: ABNT, 2020b. Disponível em: https://www.abnt.org.br/smartcities/?cn-reloaded=1.. Acesso em: 10 jul. 2021.

BAUMAN, Ziygmunt, LYON, David. **Vigilância líquida**. Tradução: Carlo Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BRASIL. **Constituição da República Federativa do Brasil**, 5 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 10 jul. 2021.

BRASIL. **Decreto n. 10.778, de 24 de agosto de 2021**. Institui a Política Nacional de Inteligência de Segurança Pública. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-10.777-de-24-de-agosto-de-2021-340717199. Acesso em 03 set. 2021.

BRASIL. **Decreto n. 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: <http://www.planalto.gov.br/ccivil_03/decreto/d3695.htm>. Acesso em: 11 jul. 2021.

BRASIL. **Decreto n. 4.376, de 13 de setembro de 2002**. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei nº 9.883, de 7 de dezembro de 1999, e dá outras providências. Disponível em: <>. Acesso em: 08 set. 2021.

BRASIL. **Decreto n. 8.793, de 29 de junho de 2016**. Fixa a Política Nacional de Inteligência. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm#:~:text=DECRETO%20N%C2%BA%208.793%2C%20DE%2029,que%20lhe%20confere%20o%20art.>. Acesso em 03 set. 2021.

BRASIL. **Decreto nº 11.426, de 1º de março de 2023**. Altera o Decreto nº 11.327, de 1º de janeiro de 2023, o Decreto nº 11.329, de 1º de janeiro de 2023, o Decreto nº 9.435, de 2 de julho de 2018, e o Decreto nº 4.376, de 13 de setembro de 2002, para integrar a Agência Brasileira de Inteligência à Casa Civil da Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11426.htm. Acesso em 03 set. 2021.

BRASIL. **Lei nº 13.675, de 11 de junho de 2018**. Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública, nos termos do § 7º do art. 144 da Constituição Federal; cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS); institui o Sistema Único de Segurança Pública (Susp); altera a Lei Complementar nº 79, de 7 de janeiro de 1994, a Lei nº 10.201, de 14 de fevereiro de 2001, e a Lei nº 11.530, de 24 de outubro de 2007; e revoga dispositivos da Lei nº 12.681, de 4 de julho de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13675.htm#:~:text=LEI%20N%C2%BA%2013.675%2C%20DE%2011%20DE%20JUNHO%20DE%202018.&text=Disciplina%20a%20organiza%C3%A7%C3%A3o%20e%20o,do%20%C2%A7%207%C2%BA%20do%20art. Acesso em set. 2022.

BRASIL. **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: <http://www.planalto.gov.br/ccivil_03/leis/l9883.htm>, acesso em: 11 jul. 2021.

BRASIL. Ministério do Desenvolvimento Regional. **Carta Brasileira para Cidades Inteligentes.** [2020]. Disponível em: https://www.gov.br/mdr/pt-br/assuntos/desenvolvimento-urbano/carta-brasileira-para-cidades-inteligentes/20201208_carta-brasileira-para-cidades-inteligentes_final.pdf. Acesso em: 14 jul. 2021.

BRASIL. **Portaria Senasp nº 22 de 22/07/2009.** Disponível em: https://www.normasbrasil.com.br/norma/portaria-22-2009_212692.html. Acesso em: 14 jul. 2021.

BRIGHT CITIES: plataforma de diagnóstico de cidades. ]2023]. Disponível em: https://pages.brightcities.city/certificacao-cidades?gclid=CjwKCAjwv-2pBhB-

EiwAtsQZFGrWLGzM4J1YTqQUgbIJSRRGGFtroMiSXbOGa2lQzsAqF_hWYDrvxho CQMYQAvD_BwE. Acesso em 15 abr.2023.

BRUNO, Fernanda. Contramanual para câmeras inteligentes: vigilância, tecnologia e percepção. **Galáxia**, São Paulo, n. 24, p. 47-63, dez. 2012. Disponível em: http://redalyc.org/articulo.oa?id=399641250005. Acesso em: 14 jul. 2021.

BUZANELLI, Márcio Paulo. Evolução histórica da atividade de inteligência no Brasil. *In*: Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública, 9. 2004, Madrid, España. **Anais...** Madrid, España: [S. l.], 2004.

CARNEVALI, Marcos; ALCANTARA, Amanda Cecatto. Cidades inteligentes e a sustentabilidade urbana. **Caderno Intersaberes**, [S. l.], v. 9, n. 19, 2020. Disponível em: https://cadernosuninter.com/index.php/intersaberes/article/view/1240. Acesso em: 21 jul. 2021.

CARVALHO, Grazielle. **Cenários Futuros para Cidades Inteligentes**. 1. ed. São Paulo: Trilha Treinamentos e Consultoria, 2019. Disponível em: file:///D:/Vigilancia%20cercamento/2019_Livro_CENA%CC%81RIOSFUTUROS_Grazi%20Carvalho_CAPA%20VERDE.PDF. Acesso em: 21 jul. 2021.

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

CORDEIRO, Sílvia Lais *et al*. Percurso histórico da sustentabilidade, suas dimensões e objetivos de desenvolvimento sustentável. **Revista Professare**, Caçador, v. 10, n.1, p. 1-22, ab. 2021. Disponível em: https://periodicos.uniarp.edu.br/index.php/professare/article/view/2922. Acesso em: 21 jul. 2021.

CORRALO, Giovani da Silva; KEMMERICH, Jonathã. A estrutura do poder municipal e as políticas de segurança: um novo paradigma federativo. **Revista Brasileira de Segurança Pública**, São Paulo, v. 10, n. 1, p. 126-140, fev./mar. 2021. Disponível em: https://revista.forumseguranca.org.br/index.php/rbsp/article/view/596/231. Acesso em 13 jun. 2023.

COSTA, Carlos Augusto. Cidades inteligentes e big data. **Cadernos FGV Projetos**, Rio de Janeiro, ano, v. 10, n. 24, p. 108-122, 2014. Disponível em: https://fgvprojetos.fgv.br/sites/fgvprojetos.fgv.br/files/cadernos_fgvprojetos_smart_cities_bilingue-final-web.pdf. Acesso em: 21 jul. 2021.

COSTA, Rogério da. Sociedade de controle. **São Paulo em perspectiva**, [S. l.], v. 18, n.1, p. 161-167, 2004. Disponível em: https://www.scielo.br/j/spp/a/ZrkVhBTNkzkJr9jVw6TygVC/?format=pdf&lang=pt. Acesso em 01 ago. 2021.

DIARINHO (Ed.). STF inicia julgamento de ação que decide o futuro dos guardas municipais: primeiro voto, do ministro Alexandre de Moraes, reconhece guarda municipal como órgão de segurança. **Diarinho**, [S. l.], 24 fev. 2023. Disponível em:

https://diarinho.net/materia/641943/STF-inicia-julgamento-de-acao-que-decide-o-futuro-dos-guardas-municipais. Acesso em 14 jun. 2021.

EFICIENTIZAÇÃO da iluminação pública e infraestrutura de comunicações. [S. l: s. n], [2020?]. 1 folder.

EVANGELISTA, Rafael de Almeida; SOARES, Tiago C.; SCHMIDT, Sarah Costa e LAVIGNATTI, Felipe. DIO: um jogo em dispositivos móveis para mapear câmeras de vigilância. **Liinc em Revista**, Rio de Janeiro, v. 12, n. 2, p. 322-333, nov. 2016. Disponível em: https://revista.ibict.br/liinc/article/view/3731/3144. Acesso em 29 jul 2021.

FGV Projetos. **O que é uma cidade inteligente**? [2019]. Disponível em: https://fgvprojetos.fgv.br/noticias/o-que-e-uma-cidade-inteligente, Acesso em 29 jul 2021.

FIRMINO, Rodrigo José *et al*. Fear, security, and the spread of CCTV in Brazilian cities: legislation, debate, and the market. **Journal of urban technology**, v. 20, n. 3, p. 65-84, 2013. Disponível em: http://dx.doi.org/10.1080/10630732.2013.809221. Acesso em 29 jul 2021.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Políticas públicas**. [2023]. Disponível em: https://forumseguranca.org.br/publicacoes/politicas-publicas/. Acesso em 29 jul 2023.

FÓRUM ECONÔMICO MUNDIAL. **G20 Smart cities Alliance**. [2021a]. Disponível em: https://globalsmartcitiesalliance.org/?page_id=107. Acesso em: 13 jul. 2021.

FÓRUM ECONÔMICO MUNDIAL. **Regional city networks launch in Latin America and South Asia bringing the fourth industrial revolution to small and medium-sized cities**. 2021b.Disponível em: https://www.weforum.org/press/2021/04/regional-city-networks-launch-in-latin-america-and-south-asia-bringing-the-fourth-industrial-revolution-to-small-and-medium-sized-cities. Acesso em: 14 jul. 2021.

FÓRUM ECONÔMICO MUNDIAL. **World economic forum to lead g20 smart cities alliance on technology governance.** 2019. Disponível em: https://www.weforum.org/press/2019/06/world-economic-forum-to-lead-g20-smart-cities-alliance-on-technology-governance/. Acesso em: 14 jul. 2021.

FREIRE, Jocemar José; FURLAN, Sandra Aparecida; SILVEIRA, José Luiz Gonçalves da. **Gestão do conhecimento na atividade de inteligência de segurança pública:** uma abordagem prática e tecnológica. 1. ed. Curitiba: Appris, 2018.

HAN, Byung-Chul. **Sociedade da Transparência**. Tradução Ênio Paulo Giachini. Petrópolis, RJ: Vozes, 2017.

HIPÓLITO, Marcello Martinez; TASCA, Jorge Eduardo. **Superando o mito do espantalho**: uma polícia orientada para a resolução dos problemas de segurança pública. Florianópolis: Editora Insular, 2012.

INSTITUTO DE PESQUISA ECONÔMICA APLICADA. **Objetivos de desenvolvimento sustentável**. 2019. Disponível em: https://www.ipea.gov.br/ods/ods11.html/. Acesso em: 14 jul. 2021.

LEE, Bum Hyun. Smart City: **Estratégias da Coreia do Sul.** 1 Videoaula 1 (Koren Smart City Policy abd Strategy), 1h51min. Escola de Governo e Gestão de Niterói. EGG. Curso on line. Disponível em: https://egg.seplag.niteroi.rj.gov.br/conteudos/mod/url/view.php?id=7956. Acesso em: 14 jul. 2021.

LEMOS, André *et al*. Câmeras de vigilância e cultura da insegurança: percepções sobre câmeras de vigilância da UFBA. **Alceu**, [S. l.], v. 12, n. 23, p. 143-153, jul./dez. 2011. Disponível em: https://silo.tips/download/cameras-de-vigilancia-e-cultura-da-insegurana-percepoes-sobre-as-cameras-de-vigi. Acesso em 16 jun 2021.

MACHADO, Mário Luiz. **A segurança pública e seus desencontros**. Ponta Grossa: do Autor, 2000.

MEDEIROS, Francisco José Fonseca de. **A atividade e inteligência no mundo atual**. [2009]. Disponível em: https://www.academia.edu/download/35155310/a_atividade_de_inteligA%C2%AAncia_no_mundo_atual.pdf. Acesso em 09 set. 2021.

MELLO, Rogério Luís Marques de. Câmeras de vigilância nas ruas e qualidade dos espaços públicos urbanos. **Revista Levs**, Marília, n. 3, p.1-16, 2009. Disponível em: Revistas.marilia.unesp.br/index.php/levs/article/view/1092. Acesso em 16 jun. 2021.

MOSETIC, Vinícius Almada; BARBIERO, Diego; BARBIERO, Diego Roberto. Surveillance e a teoria da ponderação: o conflito entre o direito à privacidade e segurança no Brasil. **Revista Argumentum:** Argumentum Journal of Law, v. 23, n. 1, p. 223-243, jan./abr. 2022. Disponível em: http://ojs.unimar.br/index.php/revistaargumentum/article/view/1268/984. Acesso em: 21 jul. 2021.

MOTA, Gibran Ayupe *et al*. Constitucionalização da atividade de inteligência-perspectivas e desafios brasileiros. **Revista Brasileira de Segurança Pública**, [S. l.], v. 12, n. 1, p. 134-150, 2018.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Os Objetivos de Desenvolvimento Sustentável no Brasil.** 2020. Disponível em: https://brasil.un.org/pt-br/sdgs. Acesso em 14 de jul. 2021.

PAULA, Giovani de. **Atividade de inteligência de segurança pública:** um modelo de conhecimento aplicável aos processos decisórios para a Prevenção e Segurança no Trânsito. Tese (doutorado) - Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento, Universidade Federal de Santa Catarina, Florianópolis, 2013.

PINHEIRO, Patrícia Peck (Coord.). **Segurança digital**: a proteção de dados nas empresas. são paulo, atlas, 2021.

RÊGO, Cláudio Andrade (Org.). **Doutrina e método da escola superior de inteligência**. 4. ed. Belo Horizonte: Antecipar Inteligência Aplicada, 2012.

REMEDIO, José Antonio; DA SILVA, Marcelo Rodrigues. O uso monopolista do big data por empresas de aplicativos: políticas públicas para um desenvolvimento sustentável em cidades inteligentes em um cenário de economia criativa e de livre concorrência. **Revista Brasileira de Políticas Públicas**, [S.l.], v. 7, n. 3, p. 671-693, 2017.

SANTOS FILHO, José Valentim dos; COÊLHO, Álvaro Vinicius de Souza. Cidades Inteligentes: desafios e tecnologias. **Revista de Tecnologia da Informação e Comunicação,** [S. l.], v. 8, n. 2, p. 69-76, 2018. Disponível em: http://rtic.com.br/index.php/rtic/article/view/106/104. Acesso em 19 jul 2021.

SILVA, Edson Emanuel Nonato; ROLIM, Vanderlan Hudson. **A importância da atividade de inteligência de segurança pública na prevenção criminal**. O Alferes, Belo Horizonte, v. 70, n. 27, p. 139-168, jan./jun. 2017. Disponível em: https://revista.policiamilitar.mg.gov.br/index.php/alferes/article/view/155acesso em 02 set. 2021.

SILVA, José Afonso da. **Aplicabilidade das normas constitucionais**. 8. ed. São Paulo: Malheiros, 2012.

SILVEIRA, José Luiz Gonçalves. **Cercamento eletrônico**. 2021. [mensagem pessoal]. Mensagem recebida por whatSapp m 12 jan. 2021.

VAZ-FERREIRA, Luciano; RORIGUES, Filipe B. O Ransonware como ameaça à cibersegurança da gestão pública de dados no Brasil**. Revista Intellector**, Rio de Janeiro, ano 17, v. 18, n. 35, p. 34-44, jan./jun. 2021.

XAVIER, Alexandre Tito. **Tito Geopolítica**. 2022. Disponível em: https://www.atitoxavier.com/post/as-empresas-privadas-de-seguran%C3%A7a-cibern%C3%A9tica-desafio-ou-oportunidade-para-a-intelig%C3%AAncia/. Acesso em 12 de fevereiro de 2023.

## ANEXO A - Indicadores de cidades inteligente

| | Indicadores da ABNT NBR ISO 37.122:2020, revisada em 2021 |
|---|---|
| 1 | Economia |
| | Porcentagem dos contratos de prestação de serviços municipais que disponham de política de dados abertos |
| | Taxa de sobrevivência de novos negócios por 100.000 habitantes |
| | Porcentagem da força de trabalho empregada em ocupações no setor de tecnologia da informação e comunicação (TIC) |
| | Porcentagem da força de trabalho empregada em ocupações nos setores de educação, pesquisa e desenvolvimento |
| 2 | Educação |
| | Porcentagem da população da cidade com proficiência profissional em mais de um idioma |
| | Número de computadores, *laptops, tablets* ou outros dispositivos de aprendizagem digital disponíveis por 1.000 estudantes |
| | Número de graduados em ensino superior nas áreas de Ciência, Tecnologia, Engenharia e Matemática (STEM) por 100.000 habitantes |
| 3 | Energia |
| | Porcentagem de energia elétrica e térmica produzida a partir do tratamento de águas residuais, resíduos sólidos e outros processos de tratamento de resíduos líquidos e outros recursos de calor residual, como uma parcela do *mix* total de energia da cidade de um determinado ano |
| | Energia elétrica é térmica (GJ) produzida a partir do tratamento de águas residuais *per capita* por ano |
| | Porcentagem da energia elétrica consumida na cidade produzida por meio de sistemas descentralizados de geração energética |
| | Capacidade de armazenamento de rede de energia, relativamente ao consumo total de energia da cidade |
| | Porcentagem de pontos de iluminação pública gerenciados por sistema de telegestão |

| | |
|---|---|
| | Porcentagem de pontos de iluminação pública que tenham sido remodelados e recém-instalados |
| | Porcentagem de edifícios públicos que necessitam de renovação/remodelagem |
| | Porcentagem de edifícios na cidade com medidores inteligente de energia |
| | Número de estações de carregamento de veículos elétricos por veículo elétrico registrado |
| 4 | Meio ambiente e mudanças climáticas |
| | Porcentagem de edifícios construídos ou reformados, nos últimos cinco anos, em conformidade com os princípios da construção verde |
| | Número de estações remotas de monitoramento da qualidade do ar interior |
| 5 | Finanças |
| | Receita anual obtida a partir da economia compartilhada, como porcentagem da receita própria |
| | Porcentagem de pagamentos para a cidade realizados por meio eletrônico |
| 6 | Governança |
| | Número anual de visitas *on-line* ao portal municipal de dados abertos por 100.000 habitantes |
| | Porcentagem de serviços urbanos acessíveis e que podem ser solicitados *on-line* |
| | Tempo médio de resposta a chamados realizados por meio de sistema de chamados não emergenciais da cidade (dias) |
| | Tempo médio de inatividade da infraestrutura de TI da cidade |
| 7 | Saúde |
| | Porcentagem da população da cidade com prontuário eletrônico unificado, acessível *on-line* pelos provedores de serviço de saúde |
| | Número anual de consultas médicas realizadas remotamente por 100.000 habitantes |

| | |
|---|---|
| | Porcentagem da população da cidade com acesso a sistemas de alertas públicos em tempo real sobre condições de qualidade do ar e da água |
| 8 | Habitação |
| | Porcentagem de domicílios com medidores inteligentes de energia |
| | Porcentagem de domicílios com medidores inteligentes de água |
| 9 | População e condições sociais |
| | Porcentagem de edifícios públicos acessíveis por pessoas com necessidades especiais |
| | Porcentagem do orçamento municipal alocado a ações de apoio, dispositivos e tecnologias assistivas a cidadãos com necessidades especiais de mobilidade |
| | Porcentagem do orçamento municipal alocado a programas voltados à redução da exclusão digital |
| 10 | Recreação |
| | Porcentagem de serviços públicos de recreação que podem ser observados *on-line* |
| 11 | Segurança |
| | Porcentagem da área da cidade coberta por câmeras de vigilância digital |
| 12 | Resíduos sólidos |
| | Porcentagem de centros de coleta (contêineres) de resíduos equipados com telemetria |
| | Porcentagem da população da cidade que dispõe de coleta de lixo porta a porta com monitoramento individual das quantidades de resíduos domésticos |
| | Porcentagem da quantidade total de resíduos empregada para gerar energia |
| | Porcentagem da quantidade total de resíduos plásticos reciclados na cidade |
| | Porcentagem das lixeiras públicas que são dotadas de sensores |

| | |
|---|---|
| | Porcentagem de resíduos elétricos e eletrônicos da cidade que são reciclados |
| 13 | Esporte e cultura |
| | Número de reservas *on-line* para instalações culturais por 100.000 habitantes |
| | Porcentagem do acervo cultural da cidade que foi digitalizado |
| | Número de livros disponíveis em bibliotecas públicas e e-books por 100.000 habitantes |
| | Porcentagem da população da cidade que é usuária ativa de bibliotecas públicas |
| 14 | Telecomunicação |
| | Porcentagem da população da cidade com acesso à banda larga suficientemente rápida |
| | Porcentagem de área da cidade sob uma zona branca/ponto morto/não coberta por conectividade de telecomunicações |
| | Porcentagem da área da cidade coberta por conectividade à internet fornecida pelo município |
| 15 | Transporte |
| | Porcentagem de ruas e vias da cidade cobertas por alertas e informações de tráfego *on-line* em tempo real |
| | Número de usuários de sistemas de transporte baseados em economia compartilhada por 100.000 habitantes |
| | Porcentagem de veículos registrados na cidade que são veículos de baixa emissão |
| | Número de bicicletas disponíveis por meio dos serviços municipais de compartilhamento e bicicletas por 100.000 habitantes |
| | Percentual de linhas de transporte público equipadas com sistema acessível ao público em tempo real |
| | Porcentagem dos serviços de transporte público da cidade cobertos por um sistema de pagamento unificado |
| | Porcentagem de vagas de estacionamento público equipadas com sistemas de pagamento eletrônico |

| | |
|---|---|
| | Porcentagem de vagas de estacionamento público equipadas com monitoramento de disponibilidade em tempo real |
| | Porcentagem dos semáforos que são inteligentes |
| | Área da cidade mapeada por sistemas interativos de mapeamento de vias públicas em tempo real, como porcentagem da área total da cidade |
| | Porcentagem de veículos na cidade que são veículos autônomos |
| | Porcentagem de linhas de transporte público dotada e conectividade à *Internet* para os usuários, oferecida e/ou gerenciada pelo município |
| | Porcentagem de vias em conformidade com sistemas de condução autônomos |
| | Porcentagem da frota de ônibus da cidade movida por sistemas limpos |
| 16 | Agricultura local/urbana e segurança alimentar |
| | Porcentagem do orçamento municipal anual destinada a iniciativas de agricultura urbana |
| | Total de resíduos alimentares coletados anualmente enviados a instalações de processamento para compostagem *per capita* (em toneladas) |
| | Porcentagem da área da cidade coberta por sistema *on-line* de mapeamento de fornecedores de alimentos |
| 17 | Planejamento urbano |
| | Número anual de cidadãos engajados no processo de planejamento urbano por 100.000 habitantes |
| | Porcentagem das solicitações de licenças de construção submetidas por sistema eletrônico |
| | Tempo médio para aprovação de licença de construção (dias) |
| | Porcentagem da população da cidade que reside em zonas de média ou alta densidade populacional |
| 18 | Esgotos |
| | Porcentagem de águas residuais tratadas que é reutilizada |

| | |
|---|---|
| | Porcentagem de biossólidos que são reutilizados (massa de matéria seca) |
| | Energia derivada de águas residuais como porcentagem do consumo de energia total da cidade |
| | Porcentagem da quantidade total de águas residuais da cidade que é empregada para geração de energia |
| | Porcentagem da rede de coleta de esgotos que é monitorada em tempo real por sistema de sensores |
| 19 | Água |
| | Porcentagem da água potável cuja qualidade é monitorada em tempo real por estações remotas |
| | Número de estações de monitoramento de qualidade da água ambiental em tempo real por 100.000 habitantes |
| | Porcentagem da rede de distribuição de água da cidade monitorada por sistemas inteligentes |
| | Porcentagem dos imóveis da cidade que possuem medidores inteligentes de água |
| 20 | Relatório e manutenção de registros |
| Anexo | Anexo A (informativo) Mapeamento de indicadores da ABNT NBR ISSO 37122 para áreas de ação e propósitos da ABNT NBR ISSO 37101 |
| Anexo | Anexo B (informativo) Mapeamento de indicadores da ABNT NBR ISSO 37122 para os Objetivos de Desenvolvimento Sustentável das Nações Unidas (ODS) (2015) |
| Figura | Figura 1 – Desenvolvimento sustentável de comunidades – Relação entre a família de Normas para indicadores de cidades |

**Fonte**: adaptado de Associação Brasileira de Normas Técnicas (2020).