

# **O Uso de Sistemas de Informação e Conhecimento nas Atividades de Inteligência do Estado: Um Olhar sob a Perspectiva da Segurança Pública**

Giovani de Paula, Paloma Maria Santos, Aires José Rover

Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento, Universidade Federal de Santa Catarina, Florianópolis – SC, Brasil  
depaula.giovani@gmail.com, paloma@egc.ufsc.br, airesjr@ccj.ufsc.br

**Resumo.** A complexidade da sociedade em que vivemos apresenta reflexos nos mais variados domínios da atuação humana, dentre os quais o da segurança pública. Neste domínio, a atividade de inteligência se institucionalizou como catalisadora das ações ligadas à produção de informação e conhecimento bem como a sua gestão. Considerando a dimensão complexa das organizações e do sujeito do conhecimento, o emprego de novas tecnologias no estabelecimento de canais de interlocução e construção de redes na era pós-moderna tornou-se necessário para a maior efetividade e eficiência da governança no domínio da segurança pública. Nesse contexto, este artigo busca discutir de que forma o governo eletrônico, por meio das ferramentas de tecnologia da informação e comunicação, possibilita que as funções governamentais inerentes à atividade de inteligência ampliem os conteúdos informacionais que são facilitadores das atividades de prevenção e resolutividade dos problemas vinculados a violência e a criminalidade.

**Palavras-chave:** Segurança Pública. Inteligência. Sistemas Baseados em Conhecimento. Gestão. Sistema Complexo.

**Abstract.** The complexity of the society we live is reflected in various fields of human activity, among which the public safety. In this domain, the intelligence activity has become institutionalized as a catalyst for the actions related to the information and knowledge production and its management. Considering the complex dimension of the organizations and the subject of knowledge, the use of new technologies in the establishment of communication channels and the construction of networks in the postmodern era has become necessary for greater effectiveness and efficiency of governance in the field of public safety. In this context, this article aims to discuss how the electronic government, through the tools of information and communication technology, allows that the government functions inherent to the intelligence activity may amplify the informational content that are facilitators of the activities of prevention and resolution of problems linked to violence and crime.

**Keywords.** Public Safety. Intelligence. Knowledge based Systems. Management. Complex System.

## **1. Introdução**

No complexo e diversificado mundo da pós-modernidade, o governo efetivo e legítimo deve devolver poderes e compartilhar a tarefa de controle social com organizações e comunidades [1].

A evolução das novas tecnologias e a emergência da chamada sociedade da informação e do conhecimento passam a exigir que as estruturas governamentais se adequem às novas formas de gestão e de administração, de forma a catalisar ações facilitadoras para a administração pública e para o administrado, o que se torna cada vez mais fundamental no domínio da segurança pública.

A dinâmica complexa das relações e dos fenômenos sociais bem como a preocupante sobre o controle dos conflitos, destacadamente os que culminam em violência e criminalidade, implicam na necessidade do estabelecimento de um conjunto de redes e conexões que permitam a gestão de informações e a produção novos conhecimentos que sejam capazes de prever cenários de riscos e aperfeiçoar as formas de intervenção sobre os mesmos, de forma a prevenir e minimizar os efeitos de eventos lesivos ao Estado e à sociedade.

As novas tecnologias e seu adequado manejo por parte do sistema de justiça criminal facultam uma série de facilidades para a administração e gestão pública que podem melhorar a vida dos cidadãos em termos de segurança. As políticas públicas e as ações, quer preventivas ou repressivas, aliadas as tecnologias avançadas, podem tornar o modelo de gestão pública mais participativo, eficiente, efetivo e transparente, melhorando e aperfeiçoando o relacionamento com o cidadão e a qualidade dos serviços de segurança prestados.

Este artigo busca discutir a importância das atividades de inteligência com o suporte das novas tecnologias para a adoção de estratégias e ações no âmbito da segurança pública visando à prevenção e intervenção nos conflitos e a manutenção da ordem pública.

O objeto central da análise visa averiguar se o sistema de justiça criminal tem aplicado a atividade de inteligência com o uso das novas tecnologias de gestão da informação e do conhecimento na prevenção e no enfrentamento à violência e à criminalidade, bem como nos processos de defesa e promoção da cidadania, considerando que as suas estruturas atuam como sistemas complexos.

Dentre as contribuições teóricas desta pesquisa, se enfatiza a que diz respeito às possibilidades que as atividades de inteligência e o uso das novas tecnologias podem trazer para o sistema de justiça criminal no domínio da segurança pública e defesa do cidadão, tanto no aspecto da prevenção como no da repressão criminal qualificada pela via da democratização e participação do cidadão em suas atividades.

## **2. A atividade de inteligência**

Desde os primórdios da civilização, a busca pelo conhecimento visando se desvendar os fatos e fenômenos da vida e proporcionar a satisfação das necessidades dos povos e

das pessoas, notadamente a segurança e a sobrevivência, tem feito parte da trajetória das sociedades. Esta busca figura o que podemos chamar de inteligência.

Desde a sua origem, a atividade de inteligência apresenta-se como recurso de que se valiam as sociedades antigas para atender os interesses da coletividade, sendo muitas vezes também empregada para fins de manutenção e a ampliação de relações de poder e controle de reis e monarcas.

Com o desenvolvimento dos povos, aliados aos novos conhecimentos, surgiram novas tecnologias, que se tornaram grandes coligadas das atividades de inteligência, tais como a fotografia, o uso de balões e aeronaves, a comunicação criptografada, o código Morse, o rádio, dentre outras. Em nosso tempo, 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 de segurança pública.

O desenvolvimento das funções informacionais teve apropriação direta por parte dos organismos dos Estados responsáveis pela segurança, tanto no contexto de defesa e diplomacia como também nas questões de segurança interna, como é o caso da manutenção da ordem pública.

Na atualidade pode-se conceituar a dimensão da atividade de inteligência com base no disposto no art. 1º, § 2º, do Decreto n. 4.376/2002 [2]:

Inteligência é a atividade de obtenção e análise de dados e informações e de produção e difusão de conhecimentos, dentro e fora do território nacional, relativos a fatos e situações de imediata ou potencial influência sobre o processo decisório, ação governamental, a salvaguarda e a segurança da sociedade e do Estado.

No Brasil, a atividade de inteligência foi conhecida historicamente por “atividade de informações”, a qual possui uma construção povoada de mistérios e, muitas vezes, questões nebulosas, isso em razão das relações de poder que a impulsionou desde o seu início.

Em suas origens, a atuação da inteligência era orientada para atender à polícia política e prestar assessoramento aos governos, que ocorreu inicialmente com o advento do Conselho de Defesa Nacional (CDN), mediante o Decreto n. 17.999, de 29 de novembro de 1927, cujo objetivo inicial era o controle dos opositores ao regime então vigente, ou seja, numa perspectiva que se alinhava com a concepção de inteligência clássica ou de “Estado” [3].

Antes desse período, a atividade de inteligência era exercida apenas no âmbito dos dois Ministérios Militares então existentes, que se dedicavam exclusivamente às questões de Defesa Nacional e atuavam em proveito das respectivas forças, ou seja, em defesa do Estado. Nesta época ainda não existia o Ministério da Aeronáutica (MAer) e a Força Aérea Brasileira (FAB), que foram criados em 1941 [4].

Com o advento da Constituição Outorgada em 1937, conhecida como “Polaca”, o seu artigo 162 passou a definir o Conselho Superior de Segurança Nacional apenas como “Conselho de Segurança Nacional”.

A atividade de inteligência passou a crescer em importância quando, em 14 de dezembro de 1949, o Decreto n. 27.583 aprovou o Regulamento para Salvaguarda das Informações de Interesse da Segurança Nacional [5].

O primeiro serviço de inteligência oficialmente criado no Brasil ocorreu em 1956, por ordem do então Presidente da República, Juscelino Kubitschek, e chamava-se Serviço Federal de Informações e Contra-Inteligência - SFICI, o qual funcionou até o golpe de 1964. Durante o período ou regime militar, foi substituído pelo Serviço Nacional de Informações, que participou ativamente da repressão à esquerda e aos movimentos sociais.

A partir daí, outras estruturas foram criadas:

- Serviço Federal de Informações e Contra-Inteligência: 1956-1964;
- Instituto de Pesquisas e Estudos Sociais: 1962-1964 (órgão particular que acumulava funções de inteligência. Reunia informações para um grupo de empresas privadas);
- Serviço Nacional de Informações – SNI: 1964-1985;
- Centro de Informações do Exército – CIEEx: 1967;
- Departamento de Inteligência: 1990-1992;
- Subsecretaria de Inteligência: 1992-1999;
- Agência Brasileira de Inteligência – ABIN: 1999 até a atualidade.

## **2.1 Dimensões do sistema brasileiro de inteligência**

Os paradigmas da pós-modernidade e os desafios diante dos novos conflitos impõem um modelo de inteligência em segurança pública que ultrapasse paradigmas e rompa preconceitos, reafirmando a importância das atividades de inteligência para o Estado e para a sociedade, e que auxilie na proteção dos cidadãos e na promoção da cidadania, com uma atuação em diversos campos inerente à sua complexidade.

Para se ter idéia da dimensão e complexidade do Sistema Brasileiro de Inteligência, destaca-se que é composto por:

- Casa Civil da Presidência da República, por meio do Centro Gestor e Operacional do Sistema de Proteção da Amazônia – CENSIPAM;
- Gabinete de Segurança Institucional da Presidência da República, órgão de coordenação das atividades de inteligência federal;
- Agência Brasileira de Inteligência – ABIN, do Gabinete de Segurança Institucional da Presidência da República – órgão central do Sistema;
- Ministério da Justiça, por meio da Secretaria Nacional de Segurança Pública, da Diretoria de Inteligência Policial do Departamento de Polícia Federal, do Departamento de Polícia Rodoviária Federal, do Departamento Penitenciário Nacional e do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional, da Secretaria Nacional de Justiça;
- Ministério da Defesa, por meio do Departamento de Inteligência Estratégica da Secretaria de Política, Estratégia e Assuntos Internacionais, da Subchefia de Inteligência do Estado-Maior de Defesa, do Estado-Maior da Armada, do Centro de Inteligência da Marinha, do Centro de Inteligência do Exército e do Centro de Inteligência da Aeronáutica;
- Ministério das Relações Exteriores, por meio da Coordenação Geral de Combate aos Ilícitos Transnacionais da Subsecretaria Geral da América do Sul;

- Ministério da Fazenda, por meio da Secretaria-Executiva do Conselho de Controle de Atividades Financeiras, da Secretaria da Receita Federal do Brasil e do Banco Central do Brasil;
- Ministério do Trabalho e Emprego, por meio da Secretaria-Executiva;
- Ministério da Saúde, por meio do Gabinete do Ministro de Estado e da Agência Nacional de Vigilância Sanitária – ANVISA;
- Ministério da Previdência Social, por meio da Secretaria-Executiva;
- Ministério da Ciência e Tecnologia, por meio do Gabinete do Ministro de Estado;
- Ministério do Meio Ambiente, por meio da Secretaria-Executiva;
- Ministério da Integração Nacional, por meio da Secretaria Nacional de Defesa Civil;
- Controladoria-Geral da União, por meio da Secretaria-Executiva.

As Unidades da Federação também podem compor o referido sistema mediante ajustes específicos e convênios, o que já ocorre, pois não há como conceber uma estrutura que fique adstrita ao formalismo político-administrativo do Estado ou mesmo ao corporativismo das organizações que possam obstar a construção de redes de transmissão de informação e conhecimento e inviabilizar uma rede sistêmica de cooperação na inteligência de segurança.

Essa é a concepção da Coordenação Geral de Inteligência (CGI) da Secretaria Nacional de Segurança Pública (SENASP), que busca atuar com fundamento em três pilares: Produção de Conhecimento, Compartilhamento e Integração.

A reunião de esforços desse conjunto de órgãos em torno da atividade de inteligência se pauta numa atuação articulada, a qual visa ampliar de forma interagencial e com uma visão sistêmica e plural o espectro de conhecimentos necessários às decisões estratégicas ou atuais para a preservação do Estado Democrático de Direito e a proteção da sociedade e dos cidadãos.

Ocorre que o tema da segurança compreende e enseja a participação de diversos atores e espaços de reflexão e de socialização, não sendo monopólio de um órgão específico do Estado, mas sim de toda a sociedade, razão pela qual as atividades de produção de conhecimento e informação podem viabilizar, mediante uma interoperabilidade sistêmica e com o uso de tecnologias, novas formas de enfrentamento ao fenômeno da insegurança, da violência e da criminalidade.

## **2.2 Subsistema de inteligência de segurança pública**

O Subsistema de Inteligência de Segurança Pública (SISP) foi criado com o Decreto n. 3.695, de 21 de dezembro de 2000, o qual tem por finalidade “coordenar e integrar as atividades de inteligência de segurança pública em todo o País, bem como suprir os governos federal e estadual de informações que subsidiem a tomada de decisões neste campo”, tendo como órgão central a Secretaria Nacional de Segurança Pública do Ministério da Justiça [6].

O SISP, por meio de ações de seus órgãos integrantes, tem as seguintes competências: “identificar, acompanhar e avaliar ameaças reais ou potenciais de

segurança pública e produzir conhecimentos e informações que subsidiem ações para neutralizar, coibir e reprimir atos criminosos de qualquer natureza” [6].

Essa forma de organização da atividade de inteligência em sistemas e subsistemas, assemelhada a um sistema complexo, resulta de uma concepção que busca o fluxo interativo de informações e conhecimentos que seja útil para ações de segurança, quer prevendo, antecipando ou resolvendo problemas e conflitos que possam vir a comprometer a segurança do Estado ou a ordem e a tranquilidade pública.

Essa forma de organização otimiza o input informacional, o que permite diminuir incertezas, ampliar as possibilidades dos processos decisórios e potencializar as ações e estratégias organizacionais e operacionais, facilitando os processos de gestão.

Nesse sentido, o conhecimento e sua gestão passam a ter papel relevante na medida em que, segundo Valentin [7]:

[...] a gestão da informação e a gestão do conhecimento atuam objetivando diminuir situações ambíguas e com alto índice de incerteza, possibilitando às pessoas da organização o acesso e o uso de informações que agirão sobre essas situações. O nível de complexidade da situação requer atenção quanto à precisão, relevância e propósito da informação. O ambiente organizacional complexo necessita de condições que amenizem a complexidade dos processos existentes neste âmbito, e a informação é um elemento que proporciona a diminuição dessa complexidade. Para isso é necessário que as organizações possuam um setor especializado que vise à gestão, organização, tratamento e disseminação da informação.

Enfatiza-se, assim, a importância e a necessidade da integração das estruturas de segurança pública e dos demais órgãos do sistema de justiça criminal mediante a cooperação entre suas estruturas de inteligência, aliado a investigação por meio de pesquisas aplicadas que visem à geração de conhecimentos essenciais para o estabelecimento de políticas públicas e ações na prevenção e no enfrentamento à violência e à criminalidade.

### **3. O uso das novas tecnologias na gestão da informação e do conhecimento**

As novas tecnologias e suas ferramentas auxiliam nos processos de gestão, organização, tratamento e disseminação da informação e construção de novos conhecimentos para as organizações, especialmente em razão de sua complexidade, uma vez que a informação não se encontra concentrada, mas sim invariavelmente difusa, e surge diante de interesses e competências específicos de atores, os quais devem continuar a ser o foco dessa produção de conhecimento, mas que devem interagir entre si, de forma a ampliar os fluxos informacionais.

Ressaltam-se, nesse contexto, os sistemas baseados em conhecimento (SBCs), que se utilizam de técnicas e ferramentas para a aquisição (etapa que visa capturar o conhecimento necessário para a resolução do problema) e representação de

conhecimento. Eles combinam estruturas de dados e procedimentos de interpretação que, se utilizados do modo certo por um programa, irão levar um sistema a apresentar um comportamento inteligente.

Segundo Embrey *et al* [8], os SBCs podem ser usados de três modos principais: para a disseminação do conhecimento entre as pessoas nas organizações; para ser reutilizado em situações e modos diferentes e finalmente, para o desenvolvimento de sistemas inteligentes que possam executar tarefas de grande complexidade.

No domínio da segurança pública, destaca-se o uso dos SBCs nas seguintes iniciativas: Investigação Criminal, Sistema de Identificação Criminal, Perícias, Sistema de Informações Policiais Judiciárias, Sistemas de Informações de Polícia Administrativa, Sistema Penitenciário, Defesa Civil, Inteligência Policial, Centro de Operações de Emergências, Análise Criminal, Geoprocessamento e Governo Eletrônico.

No âmbito das políticas de informação e gestão do conhecimento, a Secretaria Nacional de Segurança Pública do Ministério da Justiça [9], ao sistematizar as principais políticas para o setor, aponta que:

As políticas de informação e gestão do conhecimento têm como objetivo modernizar, ampliar e aperfeiçoar o Sistema de Gestão do Conhecimento e sistematizar as informações de segurança pública; estabelecer um ambiente de cooperação com os Estados, Distrito Federal e Municípios para qualificar a situação da criminalidade e violência; modernizar as agências de segurança pública e justiça criminal em termos de recursos físicos, humanos, tecnológicos e gerenciais para alimentar o sistema de gestão do conhecimento; promover ações integradas e o planejamento estratégico das instituições; identificar e difundir as melhores práticas, estratégias e tecnologias; incrementar o processo de divulgação das informações criminais e de inteligência para os públicos externo e interno das instituições de segurança pública e justiça criminal; e incrementar a produção de diagnósticos tecnicamente orientados para o planejamento e gestão das instituições de segurança pública.

A convergência de todos objetivos e aplicativos, aliada a outros canais de interlocução com a sociedade civil organizada, comunidades e setores públicos e privados, mediante a interoperabilidade sistêmica do conjunto das informações e dos conhecimentos produzidos, remetem-nos para a importância da atuação da atividade de inteligência, que com a concepção multidimensional e interagencial pode permitir uma maior funcionalidade, seja no plano estratégico, de gestão ou mesmo operacional.

Há que se levar em conta que os sistemas sociais têm padrões dinâmicos análogos a sistemas físicos, biológicos e computacionais, típicos de sistemas complexos, o que permite uma melhor compreensão das interações sociais e o apontamento de formas adequadas de intervenção nos ambientes, visando a sua evolução e aperfeiçoamento no sentido de mudanças sociais adequadas às novas realidades e necessidades humanas.

Portanto, novas estratégias devem compreender formas de gestão orientadas para a cooperação no sentido de possibilitar novos processos e troca de informações e conhecimentos, levando em conta os três aspectos essenciais: as pessoas, o processo e a tecnologia.

#### **4. Cenário da complexidade**

Conforme Rover e Carvalho [10]:

As tecnologias influem no desenvolvimento do pensamento e da inteligência, que resultam de redes complexas em que todos os elementos interagem, transformando o meio cultural no qual as representações se propagam. As tecnologias são caracterizadas por atributos como interatividade, mobilidade, convertibilidade, interconectividade, globalização e velocidade que se apresentam por meio de redes.

Nesse sentido, o governo eletrônico, conhecido também por “governo digital”, tem levado a democratização das decisões públicas mitigando as relações de poder, na medida em que possibilita a participação democrática de forma mais efetiva no trato das questões públicas fomentando novas formas de organização política e a construção de “redes sociais de cooperação”. Some-se a isso a economia com papéis e rotinas próprios da burocracia estatal, pois o uso de novas tecnologias faz com que a atuação das estruturas governamentais sofram processos de mudanças de transformações, eis que, conforme Rover [11]:

As tecnologias de informação e comunicação transformam radicalmente tudo, desde processos de trabalho e produção, até as formas de sociabilidade. Indivíduos e coletividades se movem e se reproduzem cada vez mais através das técnicas e procedimentos informáticos, mediados em âmbito local, nacional, regional e mundial. (...) Este não é apenas um processo de representação do mundo (conhecer), mas também um estado de ação no mundo, pressuposto para sua reconstrução.

O uso de procedimentos visando à obtenção de informação e conhecimento tendo como suporte o governo eletrônico possibilita uma imensa rede de comunicação e interação, cuja capilaridade pode viabilizar o envolvimento da sociedade e dos cidadãos no planejamento e na gestão pública, minimizando o monopólio estatal e permitindo a construção de novos relacionamentos e parcerias. Quando falamos em segurança pública, que como visto “é dever do Estado, direito e responsabilidade de todos” [12], essas redes e canais de interlocução são ainda mais fundamentais na chamada “sociedade do risco”.

A intervenção eficaz nas instituições e estruturas perpassam, portanto, pela compreensão de sua dimensão como sistema complexo e também por pesquisas sobre suas diferentes formas de interação, a fim de que os processos de mudanças ocorram alinhados com as transformações sociais, uma vez que a chamada “Era da

Informação” modificou a concepção de mundo, fez emergir um nova maneira de pensar, de baixo para cima, associada a Sistemas Adaptativos Complexos, facilitando a compreensão das pessoas de como os processos políticos, sociais e econômicos realmente funcionam e mudam, ou podem mudar, as coisas à nossa volta.

No âmbito das atividades de inteligência em segurança, considerando sua complexidade, deve-se considerar que suas produções são precisamente caracterizadas pelas possibilidades de influências e interferências em fatos presentes e futuros, diante do conjunto de probabilidades que podem apresentar em termos de informação e de novos conhecimentos.

Utilizar o conhecimento da complexidade para fazer melhor e compreender a complexidade significa, tipicamente, viver com ela, e até tirar proveito dela, ao invés de tentar ignorá-la ou eliminá-la [13].

Morin [14] nos elucida que:

O desafio da complexidade nos faz renunciar para sempre ao mito da elucidação total do universo, mas nos encoraja a prosseguir na aventura do conhecimento que é o diálogo com o universo. O diálogo com o universo é a própria racionalidade. Acreditamos que a razão deveria eliminar tudo o que é irracionalizável, ou seja, a eventualidade, a desordem, a contradição, a fim de encerrar o real dentro de uma estrutura de ideias coerentes, teoria ou ideologia. Acontece que a realidade transborda de todos os lados das nossas estruturas mentais. [...] O objetivo do conhecimento é abrir, e não fechar o diálogo com esse universo. O que quer dizer: não só arrancar dele o que pode ser determinado claramente, com precisão e exatidão, como as leis da natureza, mas, também, entrar no jogo do claro-escuro que é o da complexidade.

Por outro lado cabe perceber que a complexidade é característica da organização, mas também é uma característica da violência e da criminalidade, que compreende uma “teia” de interações e “relações” conflitivas que estão em constante variação e transformação, razão pela qual se evidencia a necessidade de novos métodos que permitam a reunião de várias fontes em torno do objetivo comum da segurança pública, funcionando, segundo Morgan [15], tal qual um cérebro vivo com memória adaptada à Era Digital e suas novas necessidades, e não refém da memória humana e suas limitações.

Para Ferro Júnior [16]:

A inteligência da organização deve considerar a eficácia global da organização do ponto de visão da sua inteligência total, ou sua habilidade para fazer coisas de um modo inteligente. A Inteligência organizacional pode ser definida como a capacidade da organização para mobilizar toda a capacidade intelectual a fim de alcançar sua missão. Organizações anacrônicas, fortemente burocráticas e hierarquizadas, tendem a se derrotarem, desperdiçando energia humana e falindo na capitalização da inteligência das pessoas. Organizações “inteligentes” tendem a ter sucesso pela multiplicação da inteligência pelas pessoas em um processo colaborativo.

Depreende-se que a agregação do ser humano a novas redes e a novas tecnologias e sua capacitação diante de um cenário de complexidade poderá dar maior tangibilidade na produção e prospecção de informação e conhecimento no domínio da segurança pública.

## **5. Considerações Finais**

Historicamente, as sociedades e os Estados têm recorrido à atividade de inteligência como forma de assegurar sua proteção e domínio.

A evolução dos serviços de inteligência no País tem avançado nos últimos anos, se desprendendo de uma visão ideologizada de defesa do Estado e despontando como essencial para as ações de segurança pública e de promoção da paz social.

Nesse contexto, cada vez mais se faz afirma a necessidade da incorporação de novas tecnologias, com destaque para as tecnologias da informação e da comunicação (TICs), que em sistemas complexos e em processos sociais complexos têm um papel fundamental em razão das possibilidades que apresentam em termos de prognoses sobre cenários úteis para as estratégias e ações em segurança, permitindo um olhar ampliado para o mundo, suas relações e novas dinâmicas.

Diante dos novos riscos e situações de conflitos em nossa sociedade surge a necessidade de permanente desenvolvimento organizacional, em que a busca de conhecimento deve ser vista como um processo inerente às organizações e suas relações com o ambiente, intimamente ligado à mudança e sua capacidade adaptativa, tal qual um “ser vivo”, compreendido como um sistema orgânico interdependente de seu meio. As estruturas de inteligência devem ser percebidas dessa forma.

Isso porque as novas tecnologias, a informação e o conhecimento se difundem por todas as redes sociais e organizacionais, os limites dos fluxos de comunicação se expandem, os pontos de controle se tornam intangíveis e as fontes estão em muitas partes, o tempo todo se difundindo e transformando-se, o que exige novos procedimentos e novas técnicas na seara da segurança que permitam reunir e tornar úteis o que for produzido.

Disso decorre que a prospecção e a gestão da informação e do conhecimento, compreendida na sua dimensão complexa e sistêmica e com análise de cenários de riscos faculta uma forma de atuação preventiva, nas origens dos conflitos e de situações que geram ou possam vir a gerar insegurança, minimizando a necessidade de intervenção repressiva ou de atuação limitada sobre os resultados de eventos, tais como os acidentes, os desastres e as tragédias.

A inteligência de segurança cada vez mais exige sofisticação e aperfeiçoamento crescente e o uso de novas tecnologias e sistemas diante da complexidade dessa atividade faculta a prevenção e resolução de crimes de forma mais efetiva, o que perpassa pela construção de plataformas de dados e sistemas de informações que, compartilhados, permitam uma maior integração das organizações e do Estado com a sociedade, redundando numa nova forma de prover a defesa do cidadão e de sua cidadania.

Aliado a necessidade de incessante aprendizagem organizacional, a produção de informações estratégicas no âmbito das atividades de inteligência, a pesquisa e a

sistematização de informações e de dados estatísticos visando apoiar os órgãos integrantes do sistema de justiça criminal, permitem um imperativo suporte e apoio à tomada de decisão nas ações de segurança.

A gestão da informação e do conhecimento com diagnósticos mais qualificados mediante o uso das TICs e com novos canais de interlocução e construção de redes permitem um planejamento e implementação de ações que tornam os processos decisórios no domínio da segurança pública mais efetivos e a capacidade de resposta do Estado mais adequada e alinhada a um Estado de “paz”, e não de “guerra”.

## Referências

1. Garland, David. A cultura do controle: Crime e ordem social na sociedade contemporânea. Coleção Pensamento Criminológico nº16. Rio de Janeiro: Editora REVAN, 2008.
2. Brasil. Decreto-lei n. 4.376, de 13 de setembro de 2002.
3. Brasil. Decreto n. 17.999, de 29 de novembro de 1927.
4. Revista Nossa História, ano 3, n. 34, 1996.
5. Brasil. Decreto n. 27.583, de 14 de dezembro de 1949.
6. Brasil. Decreto n. 3.695, de 21 de dezembro de 2000.
7. Valentim, M. L. P. (Org.). Gestão da informação e do conhecimento no âmbito da Ciência da Informação. São Paulo: Polis: Cultura Acadêmica, 2008.
8. Emberey, Clive L. et al. Application of Knowledge Engineering Methodologies to Support Engineering Design Application Development in Aerospace. 7th AIAA Aviation Technology, Integration and Operations Conference, Belfast, Northern Ireland, 2007.
9. Brasil. Ministério da Justiça. SENASP. VADE MECUM Segurança Pública. Brasília: Secretaria Nacional de Segurança Pública, 2010.
10. Rover, A. J.; Carvalho, M. A. (Organizadores). O sujeito do conhecimento na sociedade em rede. Florianópolis: Fundação José Boiteux, 2010.
11. Rover, A. J. Inclusão digital e governo eletrônico. Zaragoza: Prensas Universitarias de Zaragoza, 2008.
12. Brasil. Constituição da República Federativa do Brasil de 1988.
13. Axelrod, R.; Cohen, M. D. Harnessing Complexity: organizational implications of a scientific frontier. New York: The Free Press, 2000.
14. Morin, E. Ciência com consciência. Trad.: Maria D. Alexandre e Maria Alice Smpaio Dória. 2a ed. Rio de Janeiro. Bertrand Brasil, 1998.
15. Morgan, G. Imagens da Organização. São Paulo: Editora Atlas, 2006.
16. Ferro Junior, C. M. A Inteligência e a Gestão da Informação Policial. Brasília: Fortium, 2008.