Ciência de dados aplicada ao sistema de inteligência da Polícia Militar do Paraná

Data science applied to the intelligence system of the Military Police of Paraná

DOI:10.34117/bjdv9n1-405

Recebimento dos originais: 02/01/2022
Aceitação para publicação: 30/01/2023

Thaislainy Pereira Scolaro
Especialista em Inteligência Policial pela Polícia Militar do Paraná
Instituição: Polícia Militar do Paraná
Endereço: Av. Mal. Floriano Peixoto, 1401, Rebouças, Curitiba – PR, CEP: 80230-110
E-mail: thais.scolaro@gmail.com

Vagner Luiz Andreatta Bueno
Especialista em Inteligência Policial pela Polícia Militar do Estado de São Paulo
Instituição: Polícia Militar do Paraná
Endereço: Av. Mal. Floriano Peixoto, 1401, Rebouças, Curitiba – PR, CEP: 80230-110
E-mail: vlab83@gmail.com

RESUMO
O presente estudo aborda, através de pesquisa bibliográfica, a ciência de dados na inteligência da PMPR, com o fulcro de evidenciar desafios e formas de sua implementação. Para tanto, também analisa o cenário da Inteligência de Segurança Pública, atividade esta prestada pelo sistema de inteligência institucional. Ainda, constam-se apontamentos sugestivos no contexto policial militar, no sentido de integração de bancos de dados, qualificação profissional, e recursos e ferramentas compatíveis com os desafios que se apresentam. Nesta perspectiva, a inteligência deve ser entendida como um complexo sistema adaptativo no qual os processos de coleta, organização, triagem e análise de dados, se efetuados com métodos e instrumentos adequados, contribuem para a produção de conhecimentos diferenciados, capazes de gerar resultados mais efetivos à atividade de Inteligência de Segurança Pública e, por conseguinte, aos cidadãos, mediante ao preciso, oportuno e útil assessoramento ao processo decisório.

Palavras-chave: ciência de dados, recursos tecnológicos, inteligência de segurança pública, inteligência Policial Militar.

ABSTRACT
The present study addresses, through bibliographical research, data science in the intelligence of the PMPR, with the aim of highlighting challenges and ways of its implementation. To this end, it also analyzes the scenario of Public Security Intelligence, an activity provided by the institutional intelligence system. Still, there are suggestive notes in the military police context, in the sense of database integration, professional qualification, and resources and tools compatible with the challenges that are presented. In this perspective, intelligence must be understood as a complex adaptive system in

which the processes of collecting, organizing, sorting and analyzing data, if carried out with appropriate methods and instruments, contribute to the production of differentiated knowledge, capable of generating more effective results to the Public Security Intelligence activity and, consequently, to citizens, through accurate, timely and useful advice for the decision-making process.

Keywords: data science, technological resources, public safety intelligence, Military Police intelligence.

1 INTRODUÇÃO

O desenvolvimento de novas tecnologias e a emergência da chamada sociedade da informação e do conhecimento está forçando os entes públicos a se adaptarem a novas formas de governança e administração. Com o crescente e veloz desenvolvimento tecnológico, a gestão de dados está se tornando cada vez mais importante nas atividades de inteligência, o que significa que novos métodos, ferramentas, e tecnologias de informação e comunicação (TICs) devem contribuir para este processo. Essa exponencial evolução, na mesma medida em que torna facilitados os afazeres diários da sociedade, favorece a prática de atividades ilícitas, pois acaba-se extraindo os benefícios de tais avanços tecnológicos em favor de atos criminosos, os quais, progressivamente, se adaptam e se inovam, caracterizando-se, muitas vezes, pela difícil ou pela não rastreabilidade por parte das forças policiais.

As estruturas de segurança pública, nelas inserida a Polícia Militar do Paraná (PMPR), são minuciosas e fazem parte de um sistema social complexo. Neste contexto, como um fator dinâmico, o desenvolvimento de TICs necessita ser acompanhado em especial pela atividade de inteligência, visto que as mudanças científico-tecnológicas constituem-se como elementos estratégicos ao aperfeiçoamento deste serviço, sendo possibilitadas novas formas de trabalho e aumento qualitativo da capacidade de gestão de dados e conhecimentos, capazes de propiciar maior segurança aos cidadãos.

Neste cenário evolutivo, observa-se o aumento expressivo da quantidade de dados e informações disponíveis, que estão espalhados nos mais diversos bancos de dados, sendo primordial a disponibilidade de ferramentas que auxiliem tanto na coleta destes, como na organização e triagem de grande volume de dados.

Destaca-se neste artigo a importância do uso das TICs na área de inteligência e o reconhecimento de sua complexidade, como suporte para estratégias e ações no campo da segurança pública, uma vez que as formas tradicionais de intervenção em conflitos

visando à manutenção da ordem pública não apresentam resultados suficientemente necessários à prevenção da violência e do crime. Existe, portanto, a necessidade de investimento, monitoração e aplicação de inovações tecnológicas e de novos processos e métodos, de forma ao contínuo desenvolvimento destes aparatos, a fim de obter e analisar dados concernentes à segurança pública, potencializando o desempenho da atividade de inteligência.

O principal objetivo deste documento é examinar a ciência de dados na inteligência da PMPR, sob a ótica dos desafios e meios para a sua implementação. Para tanto, o estudo apresenta inicialmente a origem histórica da inteligência sob a ótica do processo evolutivo de produção e transmissão das informações, e contextualiza o campo da ciência de dados na Inteligência de Segurança Pública (ISP). Ao discorrer sobre os desafios concernentes à implementação da ciência de dados especificamente na inteligência institucional, considera todos os seus atores - os profissionais desta área, os usuários do conhecimento, e os gestores da Corporação em todos os níveis, e expõe três pilares norteadores: integração, aquisição de ferramentas tecnológicas e capacitação, que se conectam. E, pautado nisso, aponta sugestões de aplicação no cenário da inteligência da Instituição, perante aos desafios.

A contribuição teórica deste artigo diz respeito às oportunidades que os meios e as tecnologias de ciência de dados, aplicados a essa área, podem oferecer no campo da segurança pública e da proteção do cidadão, desde a prevenção até a repressão criminal qualificada, considerando a finalidade precípua da inteligência: o assessoramento ao processo decisório, mediante o uso efetivo de seu produto final – o conhecimento.

2 NOTA METODOLÓGICA

Essa pesquisa trata-se de revisão bibliográfica, constando-se conceitos e análises sobre a temática que envolve o uso de ciência de dados na atuação da inteligência da PMPR, ponto focal este que abrange desde formas de coleta de dados, até sua triagem, processamento, análise e armazenamento.

Considerando o que apresenta Richardson (2008), no que se refere ao método qualitativo, efetuado nesse estudo, através de descrições e análises, não se aplicam quantificações estatísticas acerca do tema, haja vista não consistir o objetivo da pesquisa em métricas ou quantitativos.

Ainda, esse artigo utilizou metodologia exploratória que, segundo Goulart (1998), tem como premissa "desenvolver, esclarecer e modificar conceitos e ideias, visando à formulação de problemas mais precisos e hipóteses pesquisáveis para estudos posteriores".

3 ORIGEM HISTÓRICA DA INTELIGÊNCIA COM ENFOQUE NOS PROCESSOS EVOLUTIVOS DE PRODUÇÃO E TRANSMISSÃO DE DADOS

A atividade intelectual sempre esteve presente na história da humanidade. Esta arte é mencionada nos escritos antigos de nossa civilização e tem tido uma influência direta e profunda nas relações humanas. A maioria dos historiadores cita a Bíblia como uma das fontes mais antigas desta atividade:

> No Antigo Testamento há, por exemplo, a passagem em que Moisés teria enviado espiões à Terra de Canaã, no que pode ser uma das primeiras "ordens de busca" de que se tem registro. Outra passagem bíblica muito referida é do envio por Josué, sucessor de Moisés, de dois espiões à cidade-fortaleza de Jericó, para coletarem informações para a campanha militar israelita. Isso teria acontecido por volta do ano 1.200 a.C. A Bíblia, de fato, está repleta de histórias de espiões. (GONÇALVES, 2008, p. 17).

As atividades de inteligência têm sido inerentes à humanidade desde as primeiras civilizações. Mesmo, até então, sem um conceito claro de inteligência, é possível estabelecer que ordens para buscar informações sobre outras pessoas ou lugares sempre estiveram presentes na vida cotidiana das sociedades.

Com relação às origens da inteligência como sistema organizacional institucionalizado, Cepik (2003) afirma que as primeiras organizações de profissionais de inteligência e segurança surgiram na Europa a partir do século XVI.

No século XX, as atividades de inteligência atingiram seu auge. Gonçalves (2008) argumenta que "nunca antes os serviços de inteligência estiveram tão ativamente envolvidos nas relações entre as nações e influenciaram as políticas internas e externas dos Estados em tempos de paz e guerra". O século XX viu a maior profissionalização e popularidade, e, como aponta Gonçalves (2008), foi apelidado de "século dos espiões", pois foi durante este período que os serviços secretos se consolidaram e vários métodos de inteligência foram aperfeiçoados, saindo da simples observação, memorização, descrição e transmissão de dados e informações via meios arcaicos, para uma produção de conhecimentos que se utilizava de metodologia específica e de documentos bem elaborados.

4 CIÊNCIA DE DADOS NA INTELIGÊNCIA DE SEGURANÇA PÚBLICA

Sabe-se que a denominada Inteligência de Segurança Pública (ISP) é executada por vários Órgãos a nível nacional, havendo, no âmbito do SISBIN, o Subsistema de Inteligência de Segurança Pública (SISP). No cenário estadual do Paraná, destaca-se o exercício desta atividade de ISP pelo Sistema de Inteligência da Polícia Militar do Paraná (SIPOM/PMPR), o qual integra o Sistema Estadual de Inteligência de Segurança Pública do Estado do Paraná (SEINSP).

Cumpre constar, também, a existência de documentos nacionais, estaduais e institucionais, norteadores das práticas atinentes à ISP, tais como a Política Nacional de Inteligência de Segurança Pública (PNISP) e seu decorrente documento de orientação estratégica, a Estratégia Nacional de Inteligência de Segurança Pública (ENISP), ambas materializadas por meio de Decretos Presidenciais; em âmbito estadual, instituído por Resolução governamental, o Plano Estadual de Inteligência de Segurança Pública; e no cenário da PMPR, a sua Política de Inteligência e a Estratégia do SIPOM, estipuladas através de Portarias do Comando-Geral da Corporação.

Tamanho aparato norteador da ISP denota a relevância desta atividade nos diferentes níveis de assessoramento em que é exercida, sendo possível observar nestas normativas quão evidenciada é, dentre outros aspectos, a emergência por tecnologias que atendam de forma plena o exercício da ISP, ponto focal deste artigo.

Nesse contexto, cumpre inicialmente definir a atividade de ISP, segundo a Política Nacional de Inteligência de Segurança Pública (PNISP):

> (...) o exercício permanente e sistemático de ações especializadas destinadas à identificação, à avaliação e ao acompanhamento de ameaças reais e potenciais no âmbito da segurança pública, orientadas para a produção e a salvaguarda de conhecimentos necessários ao processo decisório no curso do planejamento e da execução da Política Nacional de Segurança Pública e Desenvolvimento Social (PNSPDS) e das ações destinadas à prevenção, à neutralização e à repressão de atos criminosos de qualquer natureza que atentem contra a ordem pública, a incolumidade das pessoas e do patrimônio. (BRASIL, 2021).

Hamada e Moreira (2020, p. 10), ao discorrerem sobre inteligência estratégica, afirmam que, para que seja possível o alcance do ápice da funcionalidade desta atividade na esfera da segurança pública, ela deve basear-se em um trabalho permanente e sistemático pautado em, dentre outros fatores, ferramentas analíticas de inteligência com capacidade de prospecção e construção de cenários, isto é, visando identificar padrões e tendências correntes e emergenciais da criminalidade, das ameaças e das

vulnerabilidades, tornando possível desenvolver e aplicar a ISP nas organizações policiais.

No que concerne à prospecção de cenários, o ambiente cibernético é uma das principais esferas de potencial atuação à ISP, visto o seu crescente uso pela sociedade e, também, por ilícitos que neste espaço são praticados. A ENISP ressalta, nesse sentido, que "não somente os crimes já consumados, como também uma série de ameaças anunciadas ou em preparação, podem ser identificados com o uso de ferramentas de inteligência tecnológica e promover, assim, uma efetiva prevenção de transgressões à ordem pública".

Citam-se como alguns exemplos de atuação da ISP nesta esfera, o acompanhamento de manifestações sociais, de grupos previamente conhecidos por atuações em manifestações, de publicações que evidenciem possível planejamento de ataques a locais públicos (como é o caso de situações envolvendo atiradores ativos) e, até mesmo, prevenções a suicídios.

Ainda sobre o espaço cibernético, a ENISP assim destaca a importância da implementação de ferramentas tecnológicas avançadas:

> 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).

No contexto da inteligência tecnológica, também há que se falar em instrumentos que possibilitem a mineração de grande volume de dados. Chamada de "Data Mining" ou mineração de dados, é uma ferramenta de suma importância para o processo, pois:

> É uma técnica que faz parte de uma das etapas da descoberta de conhecimento em banco de dados. Ela é capaz de revelar, automaticamente, o conhecimento que está implícito em grandes quantidades de informações armazenadas nos bancos de dados de uma organização. Essa técnica pode fazer, entre outras, uma análise antecipada dos eventos, possibilitando prever tendências e comportamentos futuros, permitindo aos gestores a tomada de decisões baseada em fatos e não em suposições. (CARDOSO; MACHADO, 2007, p. 497).

Em outras palavras, de nada servem muitos dados sem que eles tenham sido devidamente analisados e processados pelo profissional de inteligência, o qual, então,

mediante a Metodologia de Produção do Conhecimento (MPC)[1], conseguirá interpretá-los e lhes atribuir significado, gerando o produto final da inteligência, que é o conhecimento, capaz de assessorar o processo decisório. Para tanto, necessita dos devidos instrumentos que subsidiam tais análises.

A ENISP também apresenta a preocupação com crimes interestaduais e transnacionais, mesmo em nível regional, ao mencionar que o uso de novas tecnologias no desenvolvimento da sociedade é acompanhado pelo aumento da mobilidade entre várias regiões. Nesse viés, aponta que a cooperação entre as Agências de Inteligência (AIs) de segurança pública "se reveste, portanto, de uma característica imperativa de intercâmbio de dados, conhecimentos e boas práticas na realização de suas atividades."

No âmbito do SIPOM/PMPR, ações pontuais e operações policiais desenvolvidas sob cooperação e integração interna e externa, com características de interestadualidade e intermunicipalidade, têm ocorrido, sendo possível observar o quão valor agregam ferramentas tecnológicas de obtenção e análise de grande volume de dados, tornando-se evidente e palpável a importância e imprescindibilidade de aquisição de instrumentos tecnológicos a todas as AIs da PMPR, de modo a viabilizar o trabalho sistemático frente a ações criminosas de interesse da segurança pública local, regional, estadual e, até mesmo, nacional, a depender da modalidade criminosa objeto do trabalho de inteligência. Nesse sentido, a ENISP abarca que a concretização do trabalho conjunto entre as agências de ISP "permite o enfrentamento padronizado da criminalidade, independentemente de seu local de origem ou consumação, colaborando para a proteção das fronteiras do País e dos limites entre as unidades federativas".

Ao trabalho de ISP, verifica-se que inerente é a ciência de dados, vez que a base desta atividade de inteligência é composta por eles, os quais serão, em um primeiro momento, coletados e organizados, e então analisados e processados, utilizando-se a MPC, para que se tenha, ao final, o conhecimento. Nesse cenário, tem-se que a ciência de dados surgiu perto dos anos 2000 com o intuito de analisar grandes volumes de dados digitais que apresentem uma ampla gama de informações produzidas de maneira célere (MATOS; CONDURÚ; e BENCHIMOL, 2022).

[1] Metodologia própria da atividade de inteligência caracterizada por um processo formal e regular composto por quatro fases (planejamento, reunião de dados, processamento, formalização e difusão), que visa à transformação do dado em conhecimento através do tratamento dos conteúdos coletados, que serão avaliados e interpretados.

Conste-se, ainda, que a ENISP elenca eixos estruturantes, objetivos estratégicos, oportunidades e desafios concernentes à ISP, dentre os quais ilustra-se o ponto focal deste artigo, sendo possível notar a constante evidenciação de aspectos ligados à integração, tecnologia e capacitação, três vertentes defendidas no presente estudo que, correlacionadas e, aplicadas, viabilizam plenamente a produção do conhecimento, de forma técnica e tempestiva, possibilitando o uso do produto final de inteligência oportunamente.

O eixo estruturante preconizado na ENISP que trata sobre integração é denominado de atuação em rede, no qual os componentes do SISP "compartilharão dados e conhecimento e realizarão ações específicas conjuntas, sempre em prol dos interesses da sociedade e do Estado". Também argumenta que a produção de soluções finais por parte de diferentes Órgãos, cada qual com suas perspectivas de abordagem, é mais eficaz quando eles estão articulados em rede.

Neste viés, mister salientar a forma como determinados grupos criminosos agem. Filho (2020, p. 156), ao discorrer sobre crimes violentos contra o patrimônio, menciona a expressão "grupos articulados", os quais se organizam em redes. O autor destaca que essa "arrumação criminosa em redes" (2020, p. 157) caracteriza-se por mais flexibilidade e dinamicidade, dificultando o trabalho policial, e ressalta:

> Patente que tais grupos articulados, assim dispostos em redes, apresentam maior resistência face a algum revés sofrido em virtude de interferência das forças de segurança do Estado, conseguindo se manter operando por mais tempo, mesmo com a neutralização de parte de seus integrantes. (FILHO, 2020, p. 157).

Nesse diapasão, Júnior (2020, p. 259) afirma que a "abordagem mecanicista definitivamente não tem como funcionar a contento em um contexto de constante mudança", e destaca que essa assertiva é ainda mais evidente no que tange ao combate policial à criminalidade articulada, ao aduzir a defasagem de meios frente à atuação criminal, diferença esta ocasionada por, dentre outros, dois fatores já mencionados neste artigo, as tecnologias de comunicação, e a grande mobilidade, capaz de atravessar fronteiras e competências quando das ações criminosas.

Em suma, resta evidente que a atuação em rede estipulada na ENISP é tão necessária quanto emergente. Para tanto, deve-se haver integração efetiva. Isso significa dizer que, no tocante ao compartilhamento de dados e conhecimentos, e à realização de ações específicas conjuntas, ferramentas tecnológicas adequadas devem estar disponíveis

para uso, sejam, por exemplo, desde bancos de dados integrados, *softwares* de mineração de grande volume de dados, até equipamentos de extrações telemáticas. Almejando-se consolidar a atuação cada vez mais tecnicista da inteligência, não se pode esquecer dos instrumentos tecnológicos adequados para tal e, por óbvio, da capacitação aos profissionais que com estas ferramentas lidarão. Deste modo, haverá pessoal cada vez mais especializado, e uma inteligência que caminha, senão à frente, então minimamente junto ao processo evolutivo da sociedade, na qual está presente o crime organizado que, por vezes, perfaz seu caminho à frente das forças policiais.

Ressalta-se outro aspecto acerca da atuação em rede: ela exige também a devida proteção, tanto de fontes, como dos próprios profissionais e dos conhecimentos produzidos. Este aspecto da contrainteligência aqui descrita necessita, igualmente, de meios tecnológicos adequados para tal, que possibilitem a devida segurança orgânica.

O eixo estruturante denominado Tecnologia, propriamente dito, também previsto na ENISP, demonstra o que vem sendo discutido neste artigo:

> O investimento em tecnologias de ponta deve estar sempre presente nas pautas de discussões. O avanço tecnológico no tratamento e na análise de dados permeia e impacta fortemente a atividade de inteligência de segurança pública e potencializa a resposta do trabalho de assessoramento. (BRASIL, 2021).

Neste mesmo eixo, observa-se novamente a questão da integração, ao ser mencionado que o ambiente profissional da atividade de ISP "deve favorecer o compartilhamento de ideias, recursos e experiências, para que se estabeleçam as condições para a inovação e o uso de melhores práticas". Nesse sentido, pode-se falar em integrar bancos de dados, sistemas de armazenamento e processamento de dados, por exemplo, de outras Polícias, ou mesmo de outros Órgãos não policiais, integrantes do SISP, mediante devidos ajustes e termos de cooperação necessários. Verifica-se, pois, uma ampla gama de integração possível de ser realizada, seguindo os ditames legais.

Por fim, menciona-se o eixo estruturante da Capacitação, previsto na ENISP, o qual, conforme anteriormente discorrido neste estudo, relaciona-se com os outros eixos expostos. Ora, havendo a atuação em rede (integração) e a tecnologia, nos moldes do que vem sendo exemplificado neste trabalho, por certo precisa-se de profissional devidamente capacitado a operar esses bancos de dados, essas ferramentas tecnológicas, para que então o ativo da inteligência – o profissional de ISP, exerça de maneira técnica o processo de

produção de conhecimento, por meio de metodologia própria (MPC), sabendo que terá à mão instrumentos adequados às especificidades do seu objeto de trabalho.

No que concerne às oportunidades expostas na ENISP, destacam-se as seguintes, de acordo com o objeto do presente estudo: cooperação, desenvolvimento científico e tecnológico, e inteligência tecnológica. A cooperação, como oportunidade descrita, confirma o demonstrado até aqui, ressaltando que esforços para a consecução da atividade de inteligência são otimizados em havendo integração e cooperação entre agências e a comunidade de inteligência. Assim, novamente pode-se perceber a importância de se haver, de fato, integração de bancos de dados, de programas, para subsidiar o exercício desta atividade em ações conjuntas, por exemplo.

A oportunidade que diz respeito ao desenvolvimento científico e tecnológico, traz que a atividade de ISP deve acompanhar essa evolução, constituindo tal acompanhamento um elemento estratégico para a ISP, posto que contribui para a criação de novos meios de trabalho, para o avanço da capacidade de gestão de dados e conhecimentos e, consequentemente, para a melhoria da finalidade a que a atividade se propõe – o assessoramento.

Neste viés, no artigo anteriormente mencionado, que versa sobre inteligência estratégica, aborda-se a vitalidade com que se revestem o desenvolvimento e uso de tecnologias de informação:

> De acordo com Toffler e Toffler (1998), há algumas décadas, a "guerra da informação" é uma realidade para as organizações militares e grupos privados de estudos, com parte das discussões girando em torno da guerra eletrônica, defesa contra ataques cibernéticos e uso de equipamentos para enganar centros de comando, enviando sinais falsos, fazendo com que o desenvolvimento e o uso de tecnologias de informação e seus respectivos programas sejam componentes vitais para a estratégia do conhecimento que vise a antecipar as guerras do amanhã. (TOFFLER; TOFFLER, 2018, *apud* HAMADA e MOREIRA, 2020, p. 3).

E a terceira oportunidade a ser destacada é a inteligência tecnológica, que abarca o desenvolvimento de ferramentas de monitoramento, análise de dados e gestão de riscos etc, fatores que fizeram do espaço cibernético um elemento estratégico. Acompanhar tais avanços e desenvolver soluções são fundamentais à própria segurança das informações (contrainteligência), e à otimização de práticas proativas que geram a produção de conhecimentos. Assim é abordada a inteligência tecnológica como oportunidade da ENISP, corroborando com a problemática apontada neste artigo:

> Nesse sentido, a inteligência tecnológica é um campo a ser explorado pelos órgãos e pelas entidades responsáveis pela atividade de inteligência de segurança pública, com vistas à obtenção de melhores resultados e maior dinâmica na análise de dados e no compartilhamento de informações. Além disso, é um ambiente que necessita de acompanhamento sistemático devido a sua velocidade de evolução, com potencial para aprimorar e desenvolver práticas de inteligência de segurança pública. (BRASIL, 2021).

Citados os eixos estruturantes e os cenários de oportunidades da ISP, relacionados ao presente objeto de estudo, verifica-se que os objetivos estratégicos e os desafios dispostos na ENISP, igualmente se comunicam com a pauta em tela. Ao analisá-los, observa-se a correlação com os fatores norteadores que vêm sendo apresentados neste trabalho, quais sejam: a integração (interna e externa) de banco de dados diversos; a necessidade de uso de tecnologias de ponta, que viabilizam a coleta de dados; de uso de tecnologias de ciência de dados, as quais possibilitam o tratamento dos dados ora coletados; e, por fim, a qualificação dos profissionais para operarem tais tecnologias.

Frente à quantidade exponencialmente grande de dados disponíveis, ferramentas para a triagem devida deste grande volume são necessárias, pois proporcionam, a seu turno, a organização dos dados e, a depender do instrumento, a identificação de padrões destes. Do contrário, em não havendo tais ferramentas, tornar-se-á precária a interpretação dos objetos sob análise, comprometendo o processo da MPC. Com as devidos instrumentos que auxiliam o tratamento dos dados, ao profissional de ISP é possibilitada a realização, então, de análises mais efetivas, sabendo-se que está considerando o todo do universo sob análise, não deixando despercebido nenhum dado na imensa gama disponível, garantindo uma produção de conhecimentos mais segura, capaz de gerar resultados mais efetivos à segurança pública.

5 OS DESAFIOS DA IMPLEMENTAÇÃO DE CIÊNCIA DE DADOS NA INTELIGÊNCIA DA POLÍCIA MILITAR DO PARANÁ

No cenário institucional, vê-se que a Política de Inteligência da PMPR, que corresponde ao documento de mais alto nível na inteligência da Corporação, com finalidade de orientar a execução desta atividade, preza pelo avanço tecnológico aplicado à inteligência, visando à manutenção da ordem pública, sob o prisma de uma sociedade em que as práticas criminosas tornaram-se evoluídas e inovadoras, logística e tecnicamente:

> A evolução de práticas criminosas das mais diversas, com inovações logísticas e tecnológicas exige, a seu tempo, atenção dedicada e específica da Polícia Militar nos esforços de prevenção. O desenvolvimento da tecnologia, presente em praticamente todos os setores da sociedade, fez migrarem oportunidades de realização de crimes para outros ambientes, demandando da PMPR respostas adequadas aos problemas da contemporaneidade. (PMPR, Portaria n.º 612, 2021, p. 10).

Em tempos informatizados e com veloz capacidade comunicativa, evidenciada das mais diversas formas e, muitas vezes, de difícil ou de não rastreabilidade pelas forças policiais, é imperioso que as estruturas de inteligência tenham, minimamente, ferramentas que possibilitem necessárias coletas e gestões de dados, nos termos de legislações vigentes.

Nesse sentido e, considerando o cenário policial militar, há que se falar nas operações integradas, notadamente ao Ministério Público e ao Poder Judiciário, visto que, nestas operações, tais procedimentos são possibilitados mediante ordens judiciais, por exemplo. A seguir tem-se uma explanação, segundo Machado (2021, p. 91196), acerca de operações integradas no contexto da PMPR:

> Conceitualmente, uma operação integrada de inteligência, para PMPR, sempre terá um ente externo (atuante no ambiente da segurança pública, mas não pertencente a PMPR). Gize-se que estes entes externos, segundo esse diapasão proposto, partilham da hercúlea missão de melhoramento da Segurança Pública, ao cidadão paranaense, e esta união de elementos e esforços, resta claro que amplia a atuação da inteligência da Corporação (potencializa missão e visão).

Após tais procedimentos serem possibilitados, através de ordens judiciais, e utilizando-se das ferramentas disponíveis à estrutura de inteligência, parte-se, então, para o processamento e avaliação do conteúdo gerado. Para tanto, instrumentos de mineração de grande volume de dados fazem-se necessários, visando à efetividade e otimização da análise e da produção do conhecimento, para que o produto final elaborado pelo analista de inteligência seja tempestivo, preciso, oportuno e útil. E, a partir disso, viabilizam-se novas ações policiais, a continuidade de operações integradas, mantendo-se constância neste ciclo operacional aqui ilustrado.

Todo esse conhecimento, se bem produzido, auxiliará de forma assertiva o planejamento das ações de policiamento ostensivo, o qual, então, estará aplicado com base em análises anteriores bem realizadas, que ensejam em conhecimentos confiáveis, tempestivos e úteis. Ainda, para além de assessorar o tomador de decisão em aspectos de planejamento e emprego do policiamento, conste-se a aplicação do efetivo em ações

pontuais, como abordagens específicas que objetivam a detenção de indivíduos por força de mandados de prisão ativos, abordagens outras direcionadas que culminam em ocorrências flagranciais; e em operações, como cumprimentos de mandados de busca e apreensão e de prisão, exemplos estes de uma inteligência acionável, cujo produto da análise (conhecimento) fora aplicado, gerando resultados práticos. O conhecimento produzido também pode ter como objetivo o combate às ameaças virtuais (cenário cibernético), a identificação de oportunidades e a antecipação de situações que possam oferecer riscos à segurança pública, proporcionando diagnósticos e prognósticos acerca da evolução destas. A atividade de inteligência, assim, atinge a sua finalidade precípua que é o assessoramento ao processo decisório, independentemente do nível em que está inserida - operacional, tático, estratégico.

Acerca desses aspectos, ao tratar da inteligência estratégica com base na definição de ISP, tem-se que:

> Fernandes (2011, p. 85) afirma que a primeira parte do conceito da inteligência de segurança pública, prevista na Doutrina Nacional de Inteligência de Segurança Pública (DNISP), "refere-se à inteligência estratégica de segurança pública ou inteligência policial estratégica quando trata da prospecção das ameaças que estão ocorrendo (reais) e daquelas que podem ocorrer (potenciais)". (FERNANDES, 2011, *apud* HAMADA e MOREIRA, 2020, p. 5).

A Política de Inteligência da PMPR é categórica ao afirmar que "cada vez mais se destaca na sociedade a importância da ciência de dados" (PMPR, Portaria n.º 612, 2021, p. 18), e estipula como uma das diretrizes que devem nortear a atuação da inteligência institucional, a promoção de uma cultura de ciência de dados, sustentando a imprescindibilidade de se promover uma inteligência apoiada nisso, frente às ameaças envoltas no cenário da segurança pública, conforme nota-se a seguir:

> O grande volume de dados produzidos nas rotinas mais comuns por toda a população gera diariamente um potencial de conhecimento já explorado por organizações em todo o mundo. Assim, para que a Inteligência praticada na PMPR possa fazer frente às ameaças aqui elencadas, é imprescindível a promoção de uma inteligência que se apoie, também, na ciência de dados. Há um enorme potencial nos arquivos, bancos de dados e informações geradas diariamente, na Corporação e no SIPOM, que deve ser aproveitado de modo sistêmico e segundo metodologia efetiva para a geração de conhecimento útil e oportuno, sem prejuízo da adição de quantos dados estiverem disponíveis em outras fontes legalmente acessadas. (PMPR, Portaria n.º 612, 2021, p. 18).

Este estudo aponta alguns pilares referentes aos desafios da implementação de ciência de dados na inteligência da PMPR: integração, aquisição de ferramentas

tecnológicas, e capacitação. Em linhas gerais, esses três elementos, que serão detalhados adiante, constituem-se também como instrumentos da inteligência institucional, segundo a sua respectiva Política, sendo estes o "conjunto de elementos essenciais à implementação de seus objetivos" (PMPR, Portaria n.º 612, 2021, p. 12).

5.1 INTEGRAÇÃO

Quanto ao aspecto da integração, além do anteriormente discorrido sobre a ISP, ilustra-se, agora, o cenário específico da inteligência da PMPR. Uma das diretrizes da inteligência da Instituição é o fomento à integração no âmbito do SIPOM:

> Uma característica importante da Atividade de ISP é o seu alcance. Um conhecimento completo, abrangente, preciso e oportuno, cujos dados possam ser extraídos de todas as fontes possíveis, com análise do máximo de variáveis implicadas, é o objetivo a ser atingido. Nesse contexto, os órgãos componentes do SIPOM devem operar em um regime de constante interação, relacionando-se e estabelecendo ligações no sentido de otimizar esforços conjuntos para alcançar os seus propósitos. (PMPR, Portaria n.º 612, 2021, p. 16).

Para além do fomento à integração interna (âmbito do SIPOM), a Política de Inteligência institucional (PMPR, Portaria n.º 612, 2021, p. 12) também apregoa como um dos instrumentos desta atividade, o intercâmbio de dados e conhecimentos no âmbito do SISP e SEINSP, nos termos da legislação em vigor, ou seja, com outros Órgãos da comunidade de inteligência, ratificando o que vem sendo apresentado neste trabalho.

Nesse sentido, a integração externa também é abordada na Estratégia de Inteligência do SIPOM, corroborando com o apresentado acerca da necessidade de integração de bancos de dados diversos, não apenas no âmbito da Corporação, afirmando que "ao mesmo tempo em que se utiliza de uma enorme rede de agências, com atuação em praticamente todo o território do Paraná, o SIPOM necessita de subsídios externos à esta rede local" (PMPR, Portaria n.º 611, 2021, p. 11).

Classifica-se, na referida Estratégia, como essencial ao desenvolvimento da inteligência na PMPR, o fortalecimento dos setores de TIC em todos os níveis do Sistema, e consta que "parece haver espaço para uma expansão da capacidade atual dos bancos de dados já existentes, da integração entre aqueles utilizados pelo SIPOM e para a agregação de novos, tantos quantos se fizerem úteis para o cumprimento das missões da Corporação" (PMPR, Portaria n.º 611, 2021, p. 10).

Outrossim, a Política aqui elencada destaca como outra diretriz, a promoção da cultura de ciência de dados (PMPR, Portaria n.º 612, 2021, p. 18), ressaltando "a

necessidade de ampla, irrestrita e completa cessão de todos os acessos aos bancos de dados existentes na Corporação para utilização do SIPOM, consideradas suas atribuições peculiares e a própria necessidade de conhecer".

5.2 AQUISIÇÃO DE FERRAMENTAS TECNOLÓGICAS

No que tange à vertente de aquisição de ferramentas tecnológicas à inteligência, tem-se que também é um dos instrumentos apresentados na Política de Inteligência da PMPR: "pesquisa e desenvolvimento tecnológico para as áreas de Inteligência e Contrainteligência de Segurança Pública" (PMPR, Portaria n.º 612, 2021, p. 12). No que tange à Contrainteligência, a Estratégia do SIPOM apresenta como um de seus desafios o "fortalecimento da segurança das comunicações e informações" (PMPR, Portaria n.º 611, 2021, p. 18), assegurando ser primordial às ações deste Sistema e, consequentemente, da PMPR, a proteção de dados, informações e conhecimentos, e afirmando que a garantia de canais seguros para transmitir mensagens, além de subsidiar tempestivamente o policiamento, protege os ativos de ISP.

Esse ponto referente à tecnologia aplicada à inteligência na PMPR também se relaciona ao acompanhamento de ações efetuadas no espaço cibernético. Inclusive, a Política de Inteligência da Instituição aponta as ações contrárias à segurança pública no ambiente cibernético como uma das principais ameaças à sociedade paranaense, com grande potencial lesivo:

> São ações, de caráter ilícito ou não, perpetradas através da utilização de recursos tecnológicos em espaço cibernético com potencial de comprometer a ordem pública, a incolumidade das pessoas, do patrimônio e do meio ambiente e/ou de manipular a opinião pública, obtendo vantagem indevida de setores públicos e privados. A utilização massiva de tecnologias da informação e comunicação torna vulneráveis todos os setores da sociedade, sendo possível registrar nos anos recentes a ampliação e migração de práticas ilícitas para o espaço virtual e que além dos impactos na sociedade paranaense, demandam ações de Polícia Militar. (PMPR, Portaria n.º 612, 2021, p. 13).

Nesse viés, ressaltam-se os exemplos mencionados anteriormente acerca de ameaças anunciadas ou em preparação no ambiente cibernético, que podem ser identificadas utilizando-se ferramentas de inteligência tecnológica, como situações de ataques a locais públicos (atiradores ativos), manifestações públicas, etc.

Ainda sob a ótica da tecnologia, outra diretriz da Política de Inteligência da PMPR consiste no aperfeiçoamento das inteligências cibernética e de sinais (PMPR, Portaria n.º 612, 2021, p. 15-16), afirmando-se que é "imprescindível e urgente aperfeiçoar as

tecnologias existentes e promover a especialização em inteligência cibernética e de sinais como ferramenta de enfrentamento ao crime organizado, à corrupção e às ações de competência da PMPR".

Ao garantir que a questão tecnológica é basilar para haver respostas adequadas, a Estratégia aduz que "a criminalidade violenta e a criminalidade organizada, como ameaças, podem ao mesmo tempo tanto se servir de instrumentos de tecnologia para a execução de crimes quanto serem combatidas pela utilização das melhores ferramentas tecnológicas" (PMPR, Portaria n.º 611, 2021, p. 11).

5.3 CAPACITAÇÃO

Quanto ao pilar da capacitação mencionado neste artigo, tem-se que se comunica com um dos instrumentos da Política de Inteligência da Corporação, qual seja: "capacitação, formação e desenvolvimento de profissionais para a Atividade de ISP" (PMPR, Portaria n.º 612, 2021, p. 12).

A vertente da capacitação elencada no presente artigo diz respeito aos profissionais que atuam na área de inteligência da PMPR e, notadamente, aqueles que lidam com operações de inteligência, receberem qualificação especializada, de modo que tenham o conhecimento técnico necessário para a utilização das ferramentas tecnológicas colocadas ao seu dispor e, ainda, operando-as, tenham a capacidade proativa de manterem-se atualizados, inclusive buscando acompanhar o processo evolutivo de novos métodos, novas possibilidades de coleta de dados em fontes abertas e fechadas, dentre outros aspectos.

A Estratégia de Inteligência do SIPOM (PMPR, Portaria n.º 611, 2021, p. 16) apregoa que a "formação de qualidade, capacitação e aprimoramento constantes devem ser estimulados como forma de especializar o pessoal atuante no SIPOM". E afirma:

> Ampliar a oferta de cursos, promovendo eventos de formação, capacitação e aprimoramento dos quadros do Sistema, além de fomentar o intercâmbio com instituições congêneres, em nível nacional e internacional, é fundamental para a consecução dos objetivos do SIPOM. (PMPR, Portaria n.º 611, 2021, p. 16).

A Política de Inteligência da PMPR possui alguns pressupostos, dentre os quais está a especialização, que, segundo o referido documento, é decorrente de constante capacitação: "produzir conhecimento requer a aplicação de técnicas, metodologias e

ferramentas próprias, somente passíveis de pleno uso sob profissionais especializados" (PMPR, Portaria n.º 612, 2021, p. 11).

5.4 SUGESTÕES FRENTE AOS DESAFIOS DE IMPLEMENTAÇÃO DA CIÊNCIA DE DADOS NA INTELIGÊNCIA DA PMPR

Para que se tenha a elaboração de um conhecimento completo, preciso e oportuno, sólido está que são necessárias ferramentas tecnológicas que permitam a extração de dados de todas as fontes possíveis, sejam elas abertas ou fechadas, ou seja, dados disponíveis ou negados. Assim, e com demais instrumentos que auxiliem na organização destes dados coletados, torna-se possível o processamento do máximo de variáveis implicadas no cenário sob análise.

Vê-se, com isso, que os pilares apontados neste estudo se conectam. Significa dizer que, para haver uma efetiva integração - a própria integração entre AIs e, notadamente, integração de bancos de dados diversos -, precisa-se ter ao dispor do profissional de inteligência ferramentas aptas à coleta e extração de dados de quantas fontes possíveis forem, e aptas à organização e processamento destes dados angariados. E, para tanto, é necessária a oferta de ensino e capacitação a estes profissionais, de modo a garantir a qualidade técnica e especializada do serviço efetuado. Nesse sentido, a ENISP traz que a atividade de ISP "figura como 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".

Essa inter-relação é demonstrada também na Estratégia de Inteligência do SIPOM, quando denota a relevância da tecnologia da informação e comunicação:

> O aperfeiçoamento das ferramentas de TIC no SIPOM deverá agir como facilitador para o fortalecimento da integração entre as diversas agências que o compõe. O trânsito ágil e oportuno de dados e conhecimento servirá para ampliar a capacidade de assessoramento de todos os integrantes do Sistema. (...) De igual modo, a integração e a profissionalização caminham em linha com as novas exigências decorrentes do desenvolvimento da sociedade e da tecnologia e, por consequência, da criminalidade. (PMPR, Portaria n.º 611, 2021, p. 10-11).

Ressalta-se, ainda, que alguns dos desafios elencados na referida Estratégia, de igual forma se comunicam com o objeto do presente estudo, segundo os eixos aqui apresentados (integração, aquisição de ferramentas tecnológicas, e capacitação), sendo os seguintes: promoção do uso da ciência de dados na produção de conhecimento;

reequipamento das agências; fortalecimento da segurança das comunicações e informações; consolidação da atuação especializada; estímulo à formação e capacitação de pessoal em ISP.

Quanto ao desafio específico da promoção do uso da ciência de dados no processo de produção de conhecimento, tem-se que:

> Uma Inteligência voltada para a análise de dados não pode olvidar, no momento atual, da utilização das principais ferramentas à sua disposição. A ciência de dados surge, nesta dimensão, como um importante caminho para a produção de conhecimentos cada vez mais precisos e realistas. (PMPR, Portaria n.º 611, 2021, p. 17)

Ainda, a referida Estratégia é categórica ao mencionar que "é essencial prover aos integrantes do SIPOM as melhores ferramentas disponíveis e possíveis para a realização de suas tarefas" (PMPR, Portaria n.º 611, 2021, p. 17), e afirma que a implementação de mecanismos tecnológicos que permitam tratar e interpretar grande volume de dados, e analisá-los com base em metodologia científica, potencializa os resultados esperados do SIPOM.

Desse modo, considerando a consolidação dos serviços prestados pela atividade de inteligência através da integração e intercâmbio de dados e conhecimentos, da adoção de tecnologias, e do ensino e capacitação, conste-se, a seguir, sugestões específicas frente aos desafios da implementação da ciência de dados na inteligência da PMPR, sendo algumas referentes a ferramentas e suas funcionalidades, sugestionamentos estes a serem empregados/adquiridos a nível do sistema de inteligência institucional, considerando cada uma de suas agências, para maximizar e fortalecer as suas respectivas atuações.

Quanto à ampla gama de meios para coleta de dados de interesse da inteligência, sugestiona-se primeiramente a integração, especialmente externa, de bancos de dados, como por exemplo integração com Órgãos públicos de saúde, haja vista geralmente possuírem dados atualizados que podem auxiliar o processo de produção do conhecimento efetuado pela AI.

Em segundo espectro, mencionam-se ferramentas e tecnologias, em um cenário de operações integradas de inteligência. Sugestionando-se, como alguns exemplos, acesso aos sistemas "VIGIA" das operadoras de telefonia, e desenvolvimento de projeto para aquisição do programa "Cellebrite", ambos visando às coletas de dados, as quais, naquele, ocorrem remotamente, e neste, de forma física através de aparelhos celulares devidamente apreendidos. Este segundo programa supracitado, além de coletar dados, também os

organiza, gerando relatórios acerca das extrações efetuadas. Frise-se que, no cenário de operações integradas mencionado, onde ambas as ferramentas se situam, são necessárias ordens judiciais autorizadoras destas coletas.

Igualmente importantes se apresentam os instrumentos de ciência de dados, a partir do momento em que estes já foram coletados nas mais diversas fontes possíveis. Sugere-se, nesse aspecto, visando à triagem e organização dos elementos sob análise, a aquisição do *software* "IBM I2 Analyst's Notebook", capaz de processar grandes volumes de dados e identificar padrões destes.

Por fim, na vertente do ensino, sugestiona-se a criação de curso de capacitação em inteligência de Sinais, voltado aos profissionais do SIPOM, abrangendo, no cenário das operações integradas de inteligência, desde a inteligência tecnológica (manuseio e aplicabilidade de ferramentas tecnológicas para coleta, triagem e processamento de dados), até a inteligência telemática (coleta e análise de dados negados contidos em plataformas diversas), possibilitando o aprimoramento de competências, técnicas e processos.

6 CONSIDERAÇÕES FINAIS

A adaptação contínua do aparato policial militar em termos de inteligência, é condição essencial para a segurança pública fazer frente aos métodos e tecnologias empregados nas mais diversas ações ilícitas, sejam elas em ambiente físico ou cibernético, cujos autores usufruem dos avanços tecnológicos para, logística e tecnicamente, perpetrá-las, cientes da condição de difícil e/ou de ausente rastreabilidade por parte das autoridades. Em consequência e, dado o potencial lesivo à ordem pública, demonstrou-se neste trabalho a imprescindibilidade de especial atenção por parte das instituições de segurança pública, para que estejam cada vez mais preparadas para lidar com uma ampla gama de conflitos e ameaças à ordem pública e à paz social.

Com o acompanhamento e fomento à evolução científico-tecnológica, materializados em investimentos na área de inteligência para aquisição dos devidos recursos, aliado à qualidade técnica de pessoal, é possível a prospecção e antecipação de cenários, a identificação de tendências, ações policiais preventivas e repressivas, acompanhamentos sistemáticos de temas específicos de interesse à segurança pública, mediante à melhoria na capacidade de assessoramento do serviço de inteligência ao tomador de decisão.

Nesse sentido, considerando o cenário da PMPR, este artigo, ao constar apontamentos sugestivos referentes à integração de bancos de dados, a tecnologias de ponta e de ciências de dados – que abarcam desde a coleta destes até seu processamento, e ao aprimoramento das ações de ensino e capacitação aos profissionais de inteligência, objetivou, acima de tudo, garantir um efetivo processo de produção de conhecimento, cujo objeto final seja preciso, útil e oportuno, de modo a prevenir e mitigar as consequências de situações atinentes à segurança pública, democratizando a ação da inteligência em favor dos direitos do cidadão.

Diante do estudo em tela, no que tange aos desafios da implementação de ciência de dados, conclui-se que as sugestões aplicáveis ao SIPOM/PMPR, considerando cada uma de suas Agências, contribuem para a consolidação da atividade de inteligência exercida pela Instituição, como instrumento essencial ao assessoramento no processo decisório das autoridades em segurança pública. Assim, denotando a importância estratégica de um sistema de inteligência técnico e efetivo.

REFERÊNCIAS

ALVES, Marcos César Rodrigues. Inteligência Artificial na prevenção criminal pelas Polícias Militares do Brasil. In: HAMADA, Hélio Hiroshi; MOREIRA, Renato Pires (org.). Gestão do Conhecimento e boas práticas na área de segurança pública. Catu: Bordô-Grená, 2021.

BRASIL. Decreto n.º 10.777, de 24 de agosto de 2021. Institui a Política Nacional de Inteligência de Segurança Pública. Brasília, 2021.

BRASIL. Decreto n.º 10.778, de 24 de agosto de 2021. Aprova a Estratégia Nacional de Inteligência de Segurança Pública. Brasília, 2021.

CARDOSO, Olinda Nogueira Paes. MACHADO, Rosa Teresa Moreira. Gestão do conhecimento usando data mining: estudo de caso na Universidade Federal de Lavras. Rev Adm Pública [Internet]. 2008May;42(Rev. Adm. Pública, 2008 42(3)).

CEPIK, Marco Aurélio Chaves. Espionagem e Democracia: agilidade e transparência como dilemas na institucionalização de serviços de inteligência. Rio de Janeiro: Editora FGV, 2003.

DAVENPORT, Thomas. Big Data no trabalho: derrubando mitos e descobrindo oportunidades. Tradução: Cristina Yamagami. Rio de Janeiro: Alta Books, 2017.

FILHO, Hélio de Carvalho Freitas. Alteração da Lei 13.260/2016 (Lei Antiterrorismo) Como Forma Mais Adequada de Ação do Estado. In: FRANÇA, Lucélio Ferreira Martins Faria (Organizador). Alpha Bravo Brasil – Crimes Violentos Contra o Patrimônio. Curitiba: Volume 1, Editora CRV, 2020.

GONÇALVES, Joanisval Brito. SED QUIS CUSTODIET IPSO CUSTODES? O controle da atividade de inteligência em regimes democráticos: os casos de Brasil e Canadá. 2008. Tese (Doutorado em Relações Internacionais) – Instituto de Relações Internacionais, Universidade de Brasília, Brasília, 2008.

GOULART, Íris Barbosa. Estudos exploratórios em Psicologia organizacional e do Trabalho. Psicologia do trabalho e gestão de recursos humanos: estudos contemporâneos. São Paulo: Casa do Psicólogo, 1998.

HAMADA, Hélio Hiroshi. MOREIRA, Renato Pires. A inteligência estratégica como atividade essencial para as instituições de segurança pública. Cadernos de Segurança Pública, Ano 12, Número 12, setembro de 2020.

JÚNIOR, Rogério Dourado Silva. Integração ou Morte da Segurança Pública: Teoria e Prática no Combate ao Crime Violento Contra o Patrimônio. In: FRANÇA, Lucélio Ferreira Martins Faria (Organizador). Alpha Bravo Brasil – Crimes Violentos Contra o Patrimônio. Curitiba: Volume 1, Editora CRV, 2020.

MACHADO, Cleverson Rodrigues. As ações de inteligência financeira menos complexas nas Operações Integradas de Inteligência. Brazilian Journal of Development, Curitiba, v. 7, n. 9, p. 91193-91209, sep. 2021.

MACHADO, Felipe Nery Rodrigues. Big data: o futuro dos dados e aplicações. São Paulo: Érica, 2018.

MATOS, Maurício Torres de; CONDURÚ, Marise Teles; BENCHIMOL, Alegria Celia. Interseções na produção científica da ciência da informação e ciência de dados. Acervo, [S. l.], v. 35, n. 2, p. 1–18, 2022. Disponível em: https://revista.an.gov.br/index.php/revistaacervo/article/view/1804. Acesso em: 20 jan. 2023.

PARANÁ. Resolução 143, de 28 de maio de 2019. Aprovar e instituir o Plano Estadual de Inteligência de Segurança Pública. Curitiba, 2019.

POLÍCIA MILITAR DO PARANÁ. Portaria do Comando-Geral n.º 612, de 29 de junho de 2021. Aprova a Política de Inteligência da Polícia Militar do Paraná. Curitiba, 2021.

POLÍCIA MILITAR DO PARANÁ. Portaria do Comando-Geral n.º 611, de 29 de junho de 2021. Aprova a Estratégia do Sistema de Inteligência da Polícia Militar do Paraná (SIPOM/PMPR). Curitiba, 2021.

RICHARDSON, R. J. Pesquisa Social - Métodos e Técnicas. 3. ed. São Paulo, Atlas, 2008.