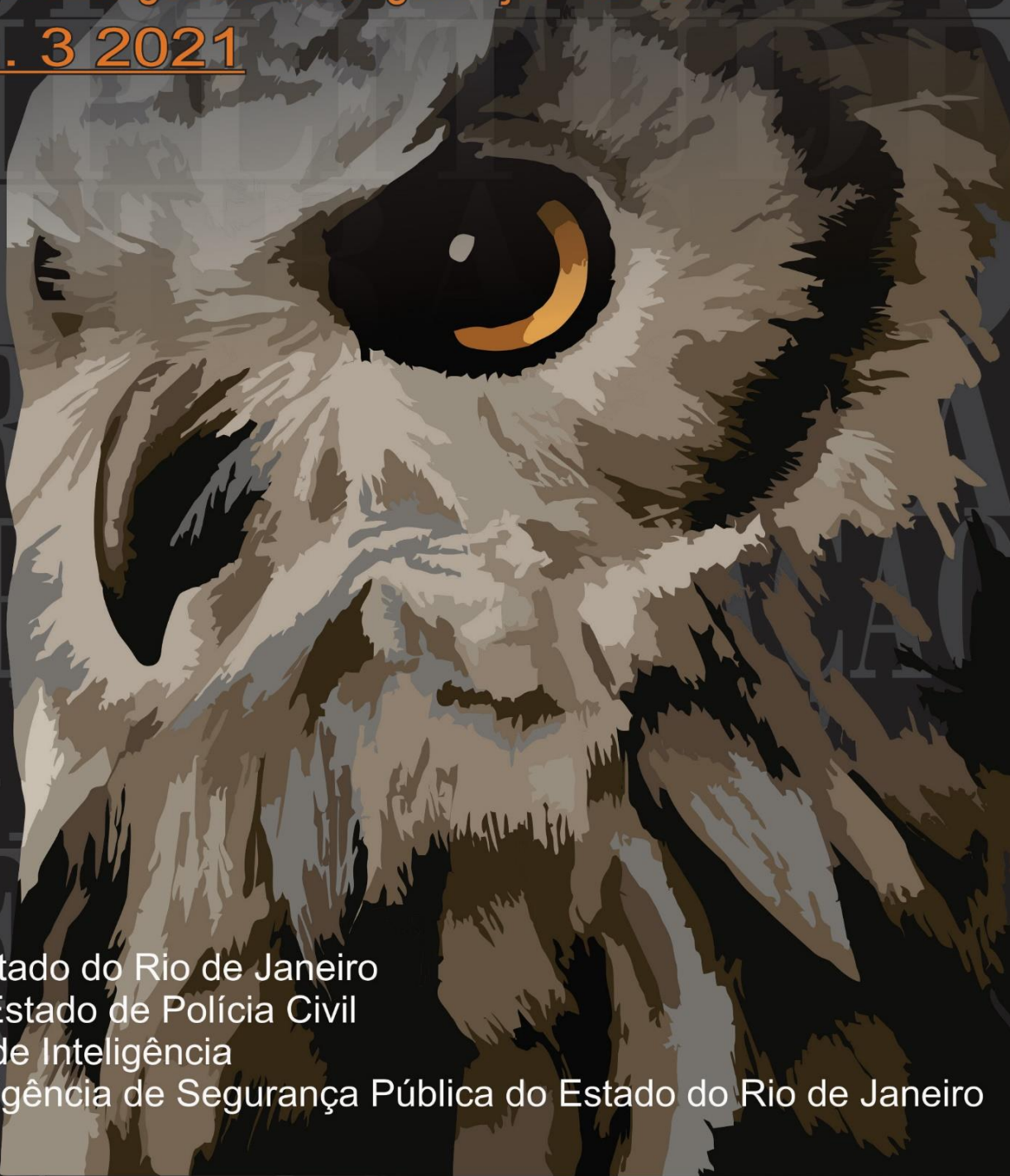
ISSN 2675-7168 (Impressa)
ISSN 2675-7249 (CD-Rom)

RISP

Revista de Inteligência de Segurança Pública

v. 3 n. 3 2021

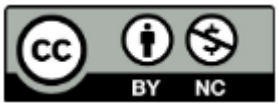


Governo do Estado do Rio de Janeiro
Secretaria de Estado de Polícia Civil
Subsecretaria de Inteligência
Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro

RISP – Revista de Inteligência de Segurança Pública

v. 3, n. 3, 2021

ISSN 2675-7168 (Impressa); 2675-7249 (CD-Rom)



EXPEDIENTE

Secretaria de Estado de Polícia Civil
Subsecretaria de Inteligência
Escola de Inteligência de Segurança Pública

Secretário de Polícia SEPOL
Allan Turnowski

Subsecretário de Inteligência
Fernando Antônio Paes de Andrade Albuquerque

Diretora Geral da ESISPERJ
Zoraia Saint'Clair Branco

Editora Chefe da RISP
Zoraia Saint'Clair Branco

Editor Executivo da RISP
André Luiz Franco Pereira

Revisora
Maria Di Luca Martino de Aguiar

Capa e Editoração Gráfica
Leandro Martins de Paiva Passos

Disponível em:
https://esisperj-ead.pcivil.rj.gov.br/login/index.php

RISP
Revista de Inteligência de Segurança Pública
ISSN 2675-7168; 2675-7249

Revista de Inteligência de Segurança Pública [Impressa] [Cd-Rom]/
Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro, Subsecretaria de Inteligência, Secretaria de Estado de Polícia Civil. V. 3, n. 3 (2021). Rio de Janeiro: ESISPERJ, 2021.
V.

Anual
ISSN 2675-7168(Impressa);2675-7249(CD-Rom)

1. Inteligência – periódicos. 2. Segurança Pública – periódicos. 3. Segurança e Defesa – periódicos. 4. Educação Profissional e Inteligência – periódicos. Secretaria de Estado de Polícia Civil, Subsecretaria de Inteligência, Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro.

CDD 300

Dados internacionais de catalogação na publicação (CIP)

RISP
Revista de Inteligência de Segurança Pública
ISSN 2675-7168; 2675-7249

Sumário

RISP
Revista de Inteligência de Segurança Pública
ISSN 2675-7168; 2675-7249

Editorial

A terceira edição da Revista de Inteligência de Segurança Pública – RISP, é editada neste ano de Pandemia, ano de 2021 que tantas perdas trouxe para toda a humanidade, para famílias e para a própria Inteligência de Segurança Pública. Zeca Borges, um dos iniciadores desta forma de se entender e de se fazer produção de conhecimento de forma integrada entre agências que tenham direta ou indiretamente atividades relacionadas à segurança pública nos deixou em 03 de dezembro de 2021, dias antes do fechamento desta edição. Deixamos aqui nossas eternas homenagens.

Destaque-se que não é possível que haja ensino, educação, sequer aprendizagem sem que haja pesquisa científica respaldando todos esses momentos da vida humana. Na primeira edição enfatizávamos a necessidade de espaço para divulgação de estudos científicos, locais onde houvesse a publicação de pesquisas, de melhores práticas, de manuais, dentre outros materiais sobre a Inteligência e mais propriamente da Inteligência de Segurança Pública (ISP).

Enfatizar o trabalho de equipe que é desenvolvido na Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro (ESISPERJ) da Subsecretaria de Inteligência (SSINTE) da Secretaria de Estado de Polícia Civil (SEPOL) é sempre salutar. Uma equipe múltipla em competências específias, assim como em origens de carreira, o que não poderia ser diferente, pois ISP é feita de integração e nossa Escola é constituída por profissionais de origens diversas, policiais civis, policiais militares e bombeiros militares, todos estaduais. É esta multiplicidade e esta união que nos proporciona planejar e executar ações de ensino tais como cursos, workshops, seminários, conferências, dentre outros, tanto na modalidade presencial quanto na de ensino à distância, sendo que para 2022 é planejada mais uma inovação, o primeiro curso na modalidade EaD, assíncrono, tendo por objeto a apresentação de uso de ferramentas a serem utilizadas pelo profissional de ISP e que poderá ser editado para todos aqueles que lidam com análise de vínculos.

Este espaço de difusão de conhecimento inicia com artigo de autoria de Marcus Castro Nunes Maia e de Marcelo dos Santos Dias Cola sob o título As Agências de Inteligência Intermediárias e a sua importância para aperfeiçoamento do Sistema de Inteligência da Secretaria de Estado de Polícia Civil do Rio de Janeiro, artigo que pretende expor a necessidade da ativação de Agências de

Inteligências intermediárias na estrutura do Sistema de Inteligência da Secretaria de estado de Polícia Civil do Rio de Janeiro (SISEPOL) a fim de permitir maior harmonia e eficiência.

No segundo artigo, os autores Filipe dos Santos Antunes, Carlo Pegoraro Nicoloso e Antônio José Ferreira Gomes, apontam para a necessidade de dar maior praticidade às tarefas rotineiras do agente de Inteligência que necessite coletar dados e conhecimentos em fontes abertas, especificamente em redes sociais, no artigo intitulado Busca de Dados em Fontes Abertas (Redes Sociais) e a Atividade de Inteligência de Segurança Pública.

Renato Pires Moreira e Imer Alves de Brito Júnior, no artigo sob o título Aspectos Teóricos e Doutrinários da Análise de Veracidade no âmbito da Inteligência de Segurança Pública revela os fundamentos teóricos e doutrinários relativos à Técnica Operacional de Inteligência (TOI) Análise de Veracidade, no âmbito da Inteligência de Segurança Pública.

Já no quarto artigo que compõe esta edição, Eliezer de Souza Batista Junior, Henrique de Queiroz Henriques e Rober Yamashita, sob o título e Relação entre Facções Criminosas e Crimes Cibernéticos, analisa a relação entre esses grupos marginalizados com as novas técnicas de crimes adotadas no ciberespaço no Brasil e também a partir do ano de 2012.

Por fim, o ensaio de Robson da Costa Ferreira da Silva, cujo título é Inteligênia de Segurança Pública e investigação criminal: aprender as diferenças para desenvolver a cultura de inteligência no âmbito da SEPOL/RJ. Neste ensaio é abordada a problemática da falta de cultura de inteligência no âmbito da Secretaria de Estado de Polícia Civil do Rio de Janeiro e a necessária diferenciação de Inteligência de Segurança Pública para Investigação criminal.

Produzir cientificamente e estimular o ato reflexivo sobre o tema Inteligência de Segurança Pública (ISP) é um dos elementos da missão da ESISPERJ/SSINTE/SEPOL, e assim, com dedicação e carinho de nossa equipe, trazemos ao leitor qualificado pelo interesse em ISP este exemplar, deixando aberta a possibilidade de participação de todos.

Saúde e paz!
Excelente leitura!

Zoraia Saint'Clair Branco
Editora Chefe da RISP

RISP
Revista de Inteligência de Segurança Pública
ISSN 2675-7168; 2675-7249

AS AGÊNCIAS DE INTELIGÊNCIA INTERMEDIÁRIAS E A SUA IMPORTÂNCIA PARA APERFEIÇOAMENTO DO SISTEMA DE INTELIGÊNCIA DA SECRETARIA DE ESTADO DE POLÍCIA CIVIL DO RIO DE JANEIRO

Marcus Castro Nunes Maia
Marcelo dos Santos Dias Cola

RESUMO: O presente artigo pretende expor a necessidade da ativação de Agências de Inteligências intermediárias na estrutura do Sistema de Inteligência da Secretaria de Estado de Polícia Civil do Rio de Janeiro (SISEPOL), a fim de permitir maior harmonia e eficiência. Para tanto, buscar-se-á apresentar conceitos básicos da Inteligência e sua incompreensão, a fim de apontar eventuais causas aparentes para entender esse vácuo estrutural que precisou ser preenchido e, posteriormente, indicar os resultados preliminares e positivos da atuação dessas agências na produção do conhecimento e no impacto na integração do sistema.

Palavras-Chaves: Inteligência de Segurança Pública. Agências Intermediárias. Integração. SISEPOL.

ABSTRACT: This article intends to expose the need to activate intermediary Intelligence Agencies in the structure of SISEPOL, in order to allow more harmony and efficiency. Therefore, we are going to present basic concepts of Intelligence and its misunderstanding, in order to indicate possible causes to understand this structural vacuum that needed to be filled and, later, specify the preliminary and positive results of the performance of these agencies in the production of intelligence and impact on system integration.

Keywords: Law Enforcement Intelligence. Intermediary Intelligence Agencies. Integration. SISEPOL.

INTRODUÇÃO.

A atividade de inteligência é assunto que ainda guarda uma aura mística, em razão da incompreensão que sempre envolve a atividade e em razão de um passado de regimes políticos autoritários (ANTUNES, 2005). Nesse obscurantismo, faz-se importante destacar conceitos primários e os alicerces atuais que embasam a Inteligência como atividade eminentemente de Estado, cujos fundamentos se materializam na preservação da soberania nacional, na defesa do Estado Democrático

de Direito e na dignidade da pessoa humana e cujos pressupostos se traduzem na fiel obediência à Constituição Federal e às leis no exercício do assessoramento especializado, ético, abrangente e permanente.

Diante desse cenário de ignorância acerca da atividade de inteligência, muitos conceitos foram mal interpretados e confundidos com outros relacionados a atividades diversas, embora vistas como semelhantes. A fim de retomar-se uma atuação técnica e profissional do Estado nessa atividade que essencialmente lhe pertence, tal equívoco deve ser desfeito, esclarecendo-se as causas que lhe deram origem e mapeando-se as consequências de sua ocorrência.

Por conseguinte, a questão dos Sistemas de Inteligência passa a ser assunto que nos parece essencial para iluminação das atividades de inteligência *de per si*. Por isso, serão apresentados, ainda que de forma suscinta, o Sistema Nacional de Inteligência (SISBIN), Subsistema de Inteligência de Segurança Pública (SISP), Sistema de Inteligência de Segurança Pública Estado do Rio de Janeiro (SISPERJ) e Sistema de Inteligência da Polícia Civil do Estado do Rio de Janeiro (SISEPOL). Suas apresentações, ao nosso ver, fazem-se imprescindíveis para compreensão da necessidade existente de articulação entre eles para o bom funcionamento da Inteligência, no que se refere à sua própria atividade.

Em outro segmento também se faz necessário discutir o processo de construção de conhecimento no contexto da atividade de inteligência, dando-se ênfase à sua etapa de difusão e o valor que atribui ao processo de concepção, valorização e integração dos Sistemas de Inteligência. *Pari passu*, a própria questão da eficiência deve ser pensada e sugerida a partir desses valores, a fim de possibilitar-se atuação harmônica, organizada e complementar entre eles.

Ultrapassados os fundamentos sugeridos, em especial, a diferenciação entre a atividade de inteligência e a atividade de investigação policial, poderemos avançar no tema, a fim de atingir o objetivo da proposta de analisar a estrutura e atuação do SISEPOL, assim como compreender o papel das agências de inteligência intermediárias e a sua importância para aperfeiçoamento do sistema.

1. INTELIGÊNCIA.

A modernidade adicionou outras acepções à palavra Inteligência, agregando à ideia aspectos emocionais (SALOVEY; MAYER, 1990), desenvolvimento de *software* (RICH, 1988) e outros segmentos (GARDNER, 1994). No caso em tela, buscamos analisar o conceito de Inteligência associado à construção do conhecimento, estabelecendo-se esta "como Instituição do Estado colocada à disposição dos governantes dos países para que eles se informem antes de tomar decisões [...]" e "[...] capaz de conhecer com profundidade os assuntos que envolvem os interesses nacionais" (RORATO, 2005, p. 36-37).

Não obstante à delimitação imposta, ainda assim, os estudiosos apresentam diversas conceituações e compreensões sobre o assunto. Nessa gama de conceitos, trazemos algumas delas para ilustrar as possibilidades sob análise. Um dos autores tradicionais sobre o tema concebe o termo "inteligência" sob três significados: a) **produto** resultante do emprego de método cognitivo, racional e analítico a dados e informações; b) como **organização** que executa essa atividade; c) **processo**, ou seja, a própria atividade através das etapas do método aplicado à construção do conhecimento (KENT, 1967). Outro autor tradicional, Washington Platt, concebe a Inteligência como o processo intelectual para produção de informações, aplicando metodologias das ciências militares e sociais (PLATT, 1974). Nessa linha de pensamento, o dicionário do Departamento de Defesa Americano define o termo Inteligência como o processo resultante da coleta, processamento, integração, avaliação análise e interpretação das informações disponíveis - tradução livre (UNITED STATES, 2021). Mark Lowenthal acrescenta, ainda, a essa concepção processual o fato de que as informações de interesse devam ser disponibilizadas aos tomadores de decisão - "*policymakers*" (LOWENTHAL, 2003), ou seja, para Lowenthal, a obtenção de informações deve ser voltada às necessidades dos tomadores de decisão (GONÇALVES, 2018), a quem interessa em primeiro lugar.

Embora as breves e suscintas apresentações doutrinárias, utilizaremos a definição legal estampada na Lei Nacional nº 9.883/99, em seu Artigo 1º, § 2º, entendendo a Inteligência como:

> Para os efeitos de aplicação desta Lei, entende-se como inteligência 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 - *Grifo nosso*).

Seguindo os desdobramentos legais, a Política Nacional de Inteligência estabelecida através do Decreto nº 8.793, de 29 de junho de 2016, traz a Atividade de Inteligência como:

> [...] 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 (BRASIL, 2016).

Nesse contexto da ampla atuação da atividade de inteligência, a questão da Segurança Interna do país se reputa crucial. Com base nessa acepção, estabeleceram-se como principais ameaças e, assim, objeto da análise das atividades de inteligência, as seguintes: a Criminalidade Organizada; a Corrupção e as Ações Contrárias ao Estado Democrático de Direito**.** Para enfrentamento adequado dessas ameaças, exige-se a atuação integrada entre as forças de segurança nacional na produção de conhecimento para enfrentar as ameaças apontadas. Com vistas a esse desiderato, surge o Decreto nº 3.695/2000 "com a finalidade de coordenar e integrar as atividades de inteligência de segurança pública em todo o País, bem como suprir os governos federal e estaduais de informações que subsidiem a tomada de decisões neste campo" (BRASIL, 2000, Art. 1º). Esse mesmo ato legislativo permitiu que os estados membros da federação criassem as suas respectivas agências de inteligência para identificar, acompanhar e avaliar ameaças reais ou potenciais de segurança pública e produzir conhecimentos e informações que subsidiassem ações para neutralizar, coibir e reprimir atos criminosos de qualquer natureza (BRASIL, 2000, Art. 2º, § 3º).

Essa simbiose entre a Inteligência de Estado e Segurança Pública, consequentemente, levou à aproximação entre as atividades de inteligência e investigação policial causando, especialmente no público menos especializado, confusões que repercutem na compreensão das respectivas atividades, não só no que se refere ao processo da construção do conhecimento, mas também no que toca suas áreas de atuação, suas formas e destinação de suas atividades.

Ante sua relevância, trazemos, logo abaixo, algumas diferenciações que entendemos de suma importância para o melhor desenvolvimento deste artigo, seu objetivo e suas nuances (FRAZÃO, 2020). Um dos primeiros pontos que trazemos é concernente a sua amplitude. A atividade de inteligência pode atingir os mais diversos segmentos do interesse estatal, pois cabe-lhe informar ao tomador de decisões a identificação de ameaças, riscos e oportunidades, a fim de atingir os objetivos traçados e contribuir para a promoção da segurança e dos demais interesses do Estado e da Sociedade. Em contrapartida, a investigação policial está constrita à apuração das infrações penais e da sua autoria, conforme o Código

de Processo Penal e leis processuais penais especiais. Percebe-se, portanto, que os ordenamentos jurídicos que pautam a atividade de inteligência e as investigações policiais, embora ambos sob o manto da Constituição da República, são diversos e com objetivos diferentes. Ainda que haja a aparente interseção entre elas, os fins e os destinatários serão necessariamente diversos.

Outra diferenciação que se faz importante ressaltar reside na ideia de 'verdade'. A atividade de inteligência tem por característica a "verdade como significado", ou seja, como produtora de conhecimentos precisos, claros e imparciais, de forma que se busquem conhecer, de forma mais exata possível, os fatos, as situações e as intenções. A verdade, neste segmento, tem a acepção da construção da convicção subjetiva do próprio analista de inteligência, a partir de metodologia da produção do conhecimento, e podendo, de tal maneira, fazer uso de todos os dados disponíveis. No que concerne à verdade na investigação policial, esta significa perseguir os indícios que podem ser objetivamente comprovados e demonstrados acerca da autoria e materialidade de um delito, circunscrito ao balizamento legal vigente, sendo vedada a utilização de dados obtidos ilicitamente, sob pena de não ser permitida a sua cognição.

Subsidiariamente, há que se destacar que a atividade de inteligência não está restrita à fonte e aos meios de obtenção de dados (BASTOS, 2020). Os dados obtidos, independentemente de sua origem, podem e devem ser submetidos a processo de construção do conhecimento pelo analista, ainda que não precisem ser necessariamente reveladas, principalmente quando há o interesse direto na sua preservação. O que se busca transmitir é o conhecimento produzido da forma mais fidedigna possível ao assessoramento do tomador de decisão. A investigação policial, ao contrário, tem fiel compromisso com a fonte e os meios de obtenção, devendo sempre demonstrar a sua validade nos autos das investigações – compromisso com a noção de prova válida e admissível em Direito – pois deverá ser submetida, *a posteriori*, ao escrutínio da legalidade por terceiros (Juiz, MP ou Defesa), partindo-se dos meios utilizados e abrangendo-se resultados alcançados.

Logo, de forma singela e pragmática, percebe-se que a atividade de inteligência e investigação policial, embora possuam pontos aparentemente semelhantes, não são iguais. Tal diferenciação entende-se importante para mostrar as causas da marginalização da atividade de inteligência e a necessidade de estruturar agências técnicas e especializadas, que permitam uma análise diferenciada e equidistante entre a investigação e aquele conhecimento necessário ao tomador de decisão.

2. OS SISTEMAS DE INTELIGÊNCIA BRASILEIROS.

A própria ideia de Sistema remonta à concepção de organização, gerenciamento e controle de qualquer atividade, sobretudo aquelas que atuam num cenário complexo, como o caso da Inteligência. Ao definir essa estrutura, as atribuições e os mecanismos de exercício da atividade de inteligência, além de institucionalizar a atividade, tornam-na compatível com o Estado Democrático de Direito. Nesse sentir, o autor Marco Cepik destaca muito bem a relação entre a legitimidade e eficiência nos serviços de inteligência nas democracias (CEPIK, 2005, p. 69).

A partir dessa sistematização, a Lei Federal nº 9.883/99 (BRASIL, 1999) estabeleceu o Sistema Brasileiro de Inteligência (SISBIN) para integrar as ações de planejamento e execução das atividades de inteligência do País, com a finalidade de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional, impondo a Agência Brasileira de Inteligência (ABIN) na posição de órgão central do SISBIN e tendo como papel planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País.

Em paralelo a isso, o legislador, percebendo a complexidade das questões de Segurança Pública no país, também criou o Subsistema de Inteligência de Segurança Pública (SISP) para atuar de forma integrada e concomitante com órgãos de Inteligência de Segurança Pública dos Estados e do Distrito Federal para produção de conhecimento. Neste sentido cabe a todos integrantes do SISP, nos termos do artigo 2º, § 3 do Decreto 3.695/2000, o seguinte:

> Cabe aos integrantes do Subsistema, no âmbito de suas 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 (BRASIL, 2000).

Dentro do Sistema de Inteligência como um todo, seus princípios e suas características, o SISP tem como finalidade:

> Proporcionar diagnósticos e prognósticos sobre a evolução de situações do interesse da Segurança Pública, subsidiando seus usuários no processo decisório; Contribuir para que o processo interativo entre usuários e profissionais de Inteligência produza efeitos cumulativos, aumentando o nível de eficiência desses usuários e de suas respectivas organizações; Subsidiar o planejamento estratégico integrado do sistema de Segurança Pública e a elaboração de planos específicos para as diversas organizações que o compõem; Assessorar, com informações relevantes, as operações de prevenção e repressão, de interesse da Segurança Pública; Salvaguardar a produção do conhecimento de ISP (BRASIL, 2015).

Essa diretriz legislativa e de integração, é reforçada por alguns estudiosos:

> Essa expansão vertical do uso de métodos e técnicas de inteligência para a base dos sistemas policiais, em combinação com uma maior integração e busca de sinergia entre as unidades de inteligência policial e as agências nacionais de inteligência de segurança, pode ser apontada como uma tendência na direção da formação de subsistemas de inteligência de segurança (CEPIK, 2005, p. 96).

No âmbito do estado do Rio de Janeiro, há ainda dois outros subsistemas que compõem o SISP. O primeiro deles é o SISPERJ, disciplinado pelo Decreto nº 46.633 de 04 de abril de 2019 (RIO DE JANEIRO, 2019). Ele tem por escopo a necessidade do permanente processamento de dados, visando à produção e difusão de conhecimentos de inteligência, relativos à criminalidade e à violência, e a efetiva ampliação, integração e otimização da tramitação dos documentos de inteligência, conforme asseverado em suas justificativas. O SISPERJ é composto por agências efetivas, especiais e afins. As efetivas seriam aquelas que participam diretamente na produção de conhecimentos de interesse da Segurança Pública, no caso Subsecretaria de Inteligência da Secretaria de Estado da Polícia Civil do Estado do Rio de Janeiro (SSINTE/SEPOL/RJ), a Subsecretaria de Inteligência da Secretaria de Estado da Polícia Militar do Estado do Rio de Janeiro (SSI/PM) e a Subsecretaria de Inteligência do Sistema Penitenciário da Secretaria de Estado de Administração Penitenciária do Estado do Rio de Janeiro (SISPEN/SEAP). As Especiais são aquelas que participam direta ou indiretamente na produção de conhecimentos de interesse de Segurança Pública, p. ex. Núcleo de Inteligência da Secretaria de Governo (NUINT/SEGOV), enquanto as afins participam indiretamente na atividade, ex. Coordenadoria de Segurança Institucional do Ministério Público (CSI/MP).

O segundo subsistema que destacamos, também integrado à lógica do SISP e SISPERJ, é o Sistema de Inteligência da SISEPOL, previsto na Resolução SEPOL nº 114, de 09 de março de 2020 (RIO DE JANEIRO, 2020). O SISEPOL é constituído pelas próprias unidades da estrutura da Secretaria de Estado de Polícia Civil do Rio de Janeiro, como os órgãos de Correição e Fiscalização (CGPOL), os órgãos operacionais (ex. Departamentos Gerais e de Área e Delegacias de Polícia) e órgãos administrativos (ex. Departamento Geral de Administração e Finanças, Departamento Geral de Gestão de Pessoas, Comissão Permanente de Licitação etc).

Em ambos os Sistemas, SISPERJ e SISEPOL, a SSINTE é a Agência Central, cabendo-lhe conduzir, gerenciar e representar o estado do Rio de Janeiro junto ao SISP. Outra caraterística comum é estarem ambos os sistemas regidos pela mesma Doutrina de Inteligência de Segurança Pública do Rio de Janeiro (DISPERJ), disposta no Decreto nº 45.126/2015 (RIO DE JANEIRO, 2015), “primeira doutrina de ISP oficialmente aprovada no Brasil, em 01 de abril de 2005, revisada e formalmente

aprovada em sua segunda versão, em 13 de janeiro de 2015" (FERREIRA, 2020) e pautando a formulação da Doutrina de Inteligência e Segurança Pública em âmbito nacional. A DISPERJ é, portanto, a norma que rege toda a atividade de inteligência no âmbito dos citados sistemas, disciplinando os fundamentos teóricos, a produção de conhecimentos, a forma e conteúdo dos seus documentos de inteligências e as operações de inteligência da ISP.

3. A INTEGRAÇÃO DOS SISTEMAS.

Como já vimos, uma das essências da atividade de inteligência reside no processo de construção de conhecimento. Nesse processo, os documentos de inteligência são instrumentos formais à condução desses conhecimentos produzidos no âmbito da agência de inteligência. Para tanto, devemos compreender o processo de construção conhecido como a Metodologia da Produção de Conhecimento (MPC). Segundo a Doutrina Nacional de Inteligência de Segurança Pública (DNISP), o MPC é entendido como um processo formal, contínuo, sequencial e com fases (Planejamento, Reunião de Dados, Processamento, Formalização e Difusão), desenvolvidos de forma cronológica**.** Esse conjunto de ações sistemáticas produzem o conhecimento de inteligência que deverá ser materializado em documentos padronizados que circulam internamente ou externamente entre as Agências de Inteligências (DNISP, 2015).

A DISPERJ segue a mesma orientação afirmando que produzir conhecimento é transformar dados e/ou conhecimentos em outro conhecimento, adotando metodologia própria e específica (DISPERJ, 2015).

Podemos inferir que a principal força de qualquer sistema de inteligência situa-se na sua capacidade de produção de conhecimento, mais especificamente na sua aptidão de coletar/reunir dados, processá-los e difundir conhecimentos a quem necessite saber. Caso suprimida qualquer dessas etapas do Ciclo de Produção de Conhecimento, comprometida se faz a atividade de inteligência. A etapa da difusão, no entanto, aparentemente singela, merece alguns comentários.

Nota-se que a fase da difusão está associada a outras questões de grande valor à atividade de inteligência como a própria concepção de integração do sistema de inteligência, a partir da construção sobre quem necessite saber, sobre a compartimentação do conhecimento e sobre o próprio sigilo.

A produção de conhecimento e a sua não difusão atenta contra a própria ideia do Sistema, assim como sua difusão irrestrita também produz impacto negativo. Por isso, a fase da difusão deve ser vinculada à necessidade de saber por meio da identificação do destinatário do conhecimento produzido. Trata-se da análise do binômio interesse - utilidade. A não valoração dessas circunstâncias atinge elementos basilares das Agências de Inteligência e da própria atividade de inteligência, no que se refere ao sigilo e à segurança da informação. Elas garantem o próprio funcionamento do sistema e do conhecimento, de forma que balizam a divisão da Atividade de Inteligência em 2 ramos, o da Inteligência e o da Contrainteligência. Esta última deve sua criação basicamente em razão da necessidade de proteção, segurança e sigilo à própria atividade de inteligência. A difusão do conhecimento a quem não o necessite saber fragiliza, sem dúvida, esses pilares. Por isso aplica-se o princípio da compartimentação sobre a limitação de acesso ao conhecimento sigiloso.

A partir da compreensão da etapa da difusão, abordamos as questões da verticalidade e horizontalidade dos sistemas de inteligência. Usualmente, não há impedimento à difusão horizontal do conhecimento (RIO DE JANEIRO, 2020), ou seja, entre duas agências de inteligência que compõem o mesmo nível do sistema. Na verdade, o próprio sistema deve estimular o fluxo de dados e conhecimento entre elas, embora a visão dessas agências em particular ainda seja estreita em relação a todo o sistema em que elas se mostram inseridas. Ao agregarmos a percepção da verticalidade, descobrimos que, além do seu par, que pressupõe preencher o binômio do interesse-utilidade de saber, também deverá haver difusão à agência de inteligência postada logo acima. Denota-se que a agência que se encontra nesse nível superior, não de forma hierárquica, mas sim numa posição sistêmica, pressupõe olhar mais abrangente da atividade de inteligência e uma capacidade de análise ampliada, podendo identificar mais facilmente outros dados relevantes e outras agências que também tenham ou não o interesse-utilidade sobre aquele mesmo conhecimento. Essa difusão verticalizada permitirá também ao tomador de decisão, qualquer que seja o nível em que esteja, obter e agregar maiores dados e conhecimentos de outras agências e da sua própria, integralizando o conhecimento e contribuindo para melhor definição do planejamento, estratégias e ações, dentro de suas atribuições e campo de atuação. O corolário lógico da orientação verticalizada do sistema de inteligência leva ao tomador de decisão a uma maior capacidade de gerir, analisar e melhor encaminhar a solução à questão.

> Embora a atividade de inteligência, por si só, não garanta a eficiência no funcionamento de uma dada instituição, não há dúvida de que, com a sua implementação e estruturação, os riscos da tomada de decisões arbitrárias, desconexas,

> contraditórias, destoantes de uma estratégia racionalmente delimitada e em confronto com o interesse público primário serão bastante reduzidos (ALMEIDA NETO, 2009, p. 84).

Embora adotem-se a visão sistêmica verticalizada, a circulação do conhecimento através dos canais apropriados e técnicos e a adoção dos protocolos do ciclo de produção do conhecimento, ainda assim, poderá existir um certo distanciamento entre a agência central e as suas outras agências que compõe o aparato da estrutura de inteligência. Com base nessa questão constata-se a necessidade de integração dos sistemas de inteligência.

Sendo assim, a Política Nacional de Inteligência, dentro dessa mesma seara, assevera:

> A crescente complexidade das relações entre Estados e desses com as sociedades define o ambiente onde atua a Inteligência. Ameaças à segurança da sociedade e do Estado demandam ações preventivas concertadas entre os organismos de Inteligência de diferentes países, e desses com suas estruturas internas. **Esse universo acentua a importância do compartilhamento de informações e do trabalho coordenado e integrado,** de forma a evitar a deflagração de crises em áreas de interesse estratégico para o Estado ou, quando inevitável, a oferecer às autoridades o assessoramento capaz de permitir o seu adequado gerenciamento (BRASIL, 2016 – *Grifo nosso*).

Na mesma toada, a Política de Inteligência de Segurança Pública do Estado do Rio de Janeiro (POLISPERJ) também aponta no mesmo caminho:

> Considerando que o conceito de política é a arte de estabelecer objetivos, pode-se verificar, num sentido mais amplo, que o objetivo base deste documento é o de "Promover a integração do Sistema de Inteligência de Segurança Pública do Estado do Rio de Janeiro", pois ao atingi-lo, será resolvida a maioria dos problemas da atividade de Inteligência de Segurança Pública do Estado do Rio de Janeiro (RIO DE JANEIRO, 2018, p. 09).

Logo, entre os diversos Sistemas e subsistemas que compõem todo o arcabouço da atividade de inteligência é posta a necessidade de integração. No âmbito das próprias Instituições e suas agências vinculadas, que utilizam a atividade de inteligência, não há por que ser diferente, ainda mais naqueles sistemas que detêm uma grande capilaridade como os policiais. É dentro da perspectiva abordada de integração que as agências intermediárias passam a ter um papel crucial, pois permitiria, dentro dessa visão sistêmica da sua área de atuação e das suas atribuições, integrar as suas diversas outras agências, minimizando os esforços e potencializando os meios e conhecimentos produzidos, quando não agregando mais valor e outros conhecimentos, a partir daqueles que possui ou possuídos por outros, sobre o objeto em análise.

4. SISEPOL.

Além da estrutura e das características anteriormente apontadas, trazemos algumas importantes reflexões ao SISEPOL. Somente a estrutura da atividade fim, investigatória, é composta por 08 (oito) grandes Departamentos Gerais, distribuídos entre unidades circunscricionais e especializadas que perfazem a quantidade de 186 (cento e oitenta e seis) unidades de polícia judiciária voltadas direta e essencialmente à atividade fim de investigação criminal, espalhadas por todas as microrregiões e em quase todos os municípios do estado do Rio de Janeiro. Cada uma delas, por si só, é considerada uma agência de inteligência.

O Projeto Delegacia Legal, iniciado em 1999, pensou essa estrutura de agências e suas atividades, focando a atuação do policial civil como analista, através do Sistema de Inteligência Policial (SIP). O trabalho desse profissional na estrutura construída dava ênfase às análises das atividades investigatórias, inclusive adotando um sistema informatizado próprio.

> Trata-se de policiais especialmente treinados no Sistema de Inteligência Policial (SIP) para incluir, classificar e analisar informes, notícias e acontecimentos que podem ter relação com alguma ocorrência criminal ou com alguém nela envolvido, a partir das informações do Sistema de Controle Operacional (SCO), desenvolvido para colher as informações necessárias ao registro de ocorrências criminais. [...] Como está estruturado sob a forma de prontuários individuais com informações sobre os autores de crimes, envolvendo dados e características pessoais, fotografias, dados de relacionamentos, antecedentes criminais e modus operandi, esse sistema se constitui numa ferramenta utilizada tanto para as questões estratégicas quanto para as táticas existentes no trabalho policial (CAMPOS, 2012, p. 59).

A partir da leitura da Resolução da Secretaria de Segurança Pública do Rio de Janeiro (RIO DE JANEIRO, 2000), que dispunha sobre a Estrutura Organizativa e Operacional das Unidades de Polícia Judiciária e Administrativas da Polícia Civil inseridas no Programa Delegacia Legal, apontamos as algumas das atribuições dos agentes da SIP: realizar consultas referentes a antecedentes penais de investigado; pesquisar, consultar, informar, tabular, mapear e elaborar estatística geral de fatos vinculados às ocorrências policiais; analisar dados recolhidos nas investigações policiais ou outras fontes, cadastrando e arquivando informações.

Ao logo do tempo, desde a implementação da primeira unidade do Projeto Delegacia Legal até a presente data, o SIP vem sofrendo esvaziamento de suas funções, por inúmeros motivos e, muitas vezes, de forma combinada, seja pela falta de pessoal nas unidades, pela sobrecarga de atividades nas unidades policiais, pela incompreensão dos gestores e do próprio analista acerca da sua importância e

de seu papel dentro do ciclo de produção de conhecimento, da vocação do agente, das dificuldades nos sistemas informatizados, dentre outros.

A reforma ao Projeto de Delegacia Legal realizado, a partir da Resolução SESEG nº 1001, de 30 de agosto de 2016 (RIO DE JANEIRO, 2016), atribui ao SIP, expressamente, a função de "executar a atividade de inteligência policial", estampado no art. 9º, inciso I. Contudo, ao mesmo tempo, cria outro setor da estrutura nas Delegais Legais, o Grupo de Investigações Complementares (GIC). O GIC foi instituído, inicialmente, para atuar nas investigações de segmento, sempre que necessário; no monitoramento eletrônico; e em algumas investigações relativas aos inquéritos policiais instaurados na UPAJ, por determinação da Autoridade Policial. Eles passam a assumir de forma progressiva, em substituição à essência da atividade do SIP, o papel de coleta e análise dos dados relevantes das unidades, seja para as investigações policiais em curso, seja para assessoramento informal do tomador de decisão, no caso o Delegado de Polícia Titular da unidade. Os dados coletados, por exemplo, a partir de investigações e medidas cautelares (ex. interceptações telefônicas e telemática) e/ou recrutamento de colaboradores serviriam para subsidiar os demais dirigentes sobre eventos de repercussão na Segurança Pública, como eventuais instabilidades em áreas críticas, guerras de facções, ameaças a autoridades e outras situações.

Posteriormente, outro órgão na Polícia Civil surge (especialmente nas unidades de polícia especializadas), o Setor de Busca Eletrônicas (SBE), previsto formal (RIO DE JANEIRO, 2015) e informal em várias unidades da Polícia Civil. Caberia a ele, por exemplo: proceder e operacionalizar as medidas cautelares de interceptações telefônicas, a análise das informações, produzir informações e relatórios, realizar operações de inteligência, vigilância e monitoramento eletrônico. Na verdade, a criação do SBE responde à necessidade de especialização e dedicação dos membros do então GIC às atividades de coleta e análise de dados, a operacionalização de medidas cautelares, em especial as eletrônicas, e atuação nas investigações policiais complexas e de grande repercussão.

Trazemos essas observações para enfatizar a atuação e o entrelaçamento das atividades de inteligência e atividade investigatória desses setores instituídos – SIP, GIC e SBE na Polícia Civil do Rio de Janeiro. Neste meandro, reputa-se necessário resgatar as diferenciações e conceitos anteriormente postos, pois é na atuação desses órgãos, na percepção desnecessária da atividade de inteligência e aparente similitude com a investigação criminal que se fez que indubitavelmente se encobriu a atividade de inteligência. Em outras palavras, a relação aparentemente imbricada entre a

atividade investigatória e a atividade de inteligência, sob um olhar estreito, pragmático e do desconhecimento das diferenças, contribuiu à informalização e à marginalização dessa última nas unidades operacionais de Polícia Judiciária.

A consequência natural desse vácuo fez com que o sistema de inteligência na Polícia Civil tivesse um fluxo unidirecional e formal de conhecimento decorrente da atividade de inteligência em sentido estrito, da agência central às unidades operacionais. Reconhece-se, no entanto, que o caminho inverso sempre existiu, ainda que, usualmente, feito de maneira informal, de forma fragmentada, sem realização de análise mais robusta ou com emprego de metodologia apropriada. Esses dados ou informações eram repassados de forma não estruturada e não oficializada em documento formal de inteligência, deixando de seguir os canais técnicos e os protocolos estabelecidos no DISPERJ.

A despeito disso, a necessidade da obtenção do dado e sua análise, transformando-os em informação estruturada, útil, oficial e oportuna ao tomador de decisão, sempre se manteve ativa. Em 2019, com retorno da Polícia Civil do Rio de Janeiro à condição de Secretaria de Estado, o Departamento Geral do Polícia da Capital (DGPC) toma a iniciativa de ativar, estruturar e implementar um segmento intermediário entre a Agência Central do SISEPOL, o próprio Departamento Geral com os seus respectivos Departamentos de Área (DPA), em efetivas agências de inteligência a fim de dar assessoramento direto ao Diretor Geral, às próprias unidades subordinadas e facilitação da conexão entre elas e a agência central.

A inovação nascida trouxe vários méritos à atividade de inteligência no sistema da SISEPOL. A primeira delas que destacamos foi efetivamente o Diretor-Geral ser assessorado diretamente por uma equipe de analistas de inteligência, permitindo compreender e melhor adotar soluções às ameaças e às oportunidades que se apresentavam diante das suas peculiaridades, atribuições e missões. A esses analistas especializados cabiam a prospecção ativa de elementos de interesse e a adoção de uma postura sistêmica dentro do SISEPOL e do Departamento. Os dados de interesse que poderiam repercutir e/ou contribuir a mais, provindo de outra unidade, podiam ser mais facilmente percebidos, a partir desse olhar ampliado e especializado, preenchendo as lacunas, fomentando o intercâmbio e complementando as atividades.

Dentro dessa postura ativa, as diversas dificuldades impostas a quase todas as Delegacias no Rio de Janeiro, absorvidas pelas mais diversas demandas diárias, vinculadas aos limites impostos aos

objetos das investigações e a não compreensão do funcionamento e fins do sistema de inteligência, acabam sendo mitigados e, assim, maior eficiência à construção do conhecimento e ao assessoramento se faz presente.

Outro ganho a que se deve dar ênfase foi também o fomento à articulação entre a agência central e as unidades operacionais. A assunção dos Departamentos Gerais como uma instância intermediária permitiu maior aproximação, intercâmbio e fluxo de dados entre todas as agências da SISEPOL, assim como os dados passaram a ser mais bem estruturados, submetidos a um ciclo de produção de conhecimento adequado, passando a circular através dos canais técnicos de forma mais apropriada, protegendo os dados e informações e fomentando melhorias às bases de dados da inteligência.

O volume do fluxo de dados também foi uma percepção positiva que se fez sentir. Há indicativos de que, após um período de adaptação, estruturação e ajustes das agências intermediárias ao Sistema e metodologia de trabalho da inteligência, houve efetivo acréscimo do trânsito de documentos de inteligência entre o DGPC e suas unidades com a SSINTE.

O mesmo modelo de atuação foi implementado no DGPI a partir de novembro de 2019 e verificamos que, a partir das lições e ensinamentos auferidos nessa mudança de paradigma, adequando-se ao modelo proposto, os ganhos também foram positivos, seguindo a mesma linha do DGPC.

Outra consequência se fez sentir na SSINTE, de acordo com as medidas adotadas. Pôde-se observar diálogo mais intenso e de melhor qualidade entre suas agências, o que demonstrou importante aumento na análise de dados, processamento e difusão de conhecimentos.

CONCLUSÃO.

Ao longo do artigo, procuramos apresentar de forma didática, direta e suscinta, mas sempre técnica, o papel da Inteligência de Estado e o seu desdobramento para área da Segurança Pública. Dentro desse aspecto, se fez necessário retomar os alicerces para compreensão das temáticas de fundo sobre a atividade de inteligência e os sistemas de inteligência. Nesse diapasão, tornou-se crucial entender a importante diferenciação entre a atividade de inteligência e a atividade investigativa, comumente vistas como extremamente imbricadas, mas com nuances, atores, características e finalidades díspares para

atingir as causas, as consequências e o impacto no sistema de inteligência da Secretaria de Estado de Polícia Civil do Rio de Janeiro.

Em sendo assim, a exigência de integração dos sistemas tornou-se questão essencial e preliminar. Nesse ponto, trouxemos as políticas, doutrinas e demais fontes, que há muito vêm construindo e iluminando a atividade de inteligência no país. Nota-se que um dos pilares à ideia da integração se sustenta na própria eficiência e eficácia do sistema.

A partir da exposição dos conceitos e sua aplicabilidade precisou-se, então, entender e adequar as estruturas e funcionamento dos órgãos que exercem as funções da inteligência no SISEPOL. Ao apresentar e compreender a atuação isolada do SIP, GIC e SBE, pudemos perceber que o distanciamento entre as unidades operacionais e a agência central exigiu a ativação de agências intermediárias para expansão do exercício técnico, eficaz e sistêmico da atividade de inteligência.

Portanto, a partir dessa visão angular sobre o papel do Departamento Geral e/ ou DPAs como agências intermediárias de inteligência, adotando efetivamente a atividade de inteligência no seu sentido estrito, contribuiu-se à melhor interlocução entre a Agência Central e as unidades operacionais. Acrescenta-se, também, que houve aumento qualitativo e quantitativo do fluxo de dados e informações para atendimentos das demandas dos integrantes do SISEPOL, sem mencionar a compreensão do sistema de inteligência pelos seus integrantes, o melhor manejo dos ferramentais disponíveis, a própria finalidade e a percepção do papel dos Departamentos Gerais, dos DPAs e das Delegacias de Polícia como agências de inteligência propriamente ditas. A continuidade desse ciclo virtuoso, a seguir pelos dados preliminares colhidos e apresentados, permitirá a construção de cenários valiosos à Secretaria de Estado de Polícia Civil e a toda a Segurança Pública do Estado do Rio de Janeiro.

REFERÊNCIAS:

ALMEIDA NETO, Wilson Rocha de. **Inteligência e Contra-Inteligência no Ministério Público**. Belo Horizonte: Dictum. 2009.

ANTUNES, Priscila Carlos Brandão. **Argentina, Brasil e Chile e o Desafio da Reconstrução das Agências Nacionais Civis de Inteligência no Contexto de Democratização**, p. 256. Tese (Doutorado) - Instituto de Filosofia e Ciências Humanas. Universidade Estadual de Campinas (UNICAMP), Campinas, SP. 2005.

BASTOS, Marlon Garcia da Silva Bastos. **O Conceito de Fonte e suas Implicações na Atividade de Inteligência de Segurança Pública**. RISP - Revista de Inteligência de Segurança Pública**,** v. 1, nº 1, p. 64-79. 2020.

BRASIL. **Decreto nº 3.695, de 21 de dezembro de 2000**. Cria o Subsistema de Inteligência de Segurança Pública, no âmbito do Sistema Brasileiro de Inteligência, e dá outras providências. Disponível em: <*http://www.planalto.gov.br/ccivil_03/decreto/d3695.htm*>. acessado em 28/05/2021.

BRASIL. **Decreto nº 8.793, de 29 de junho de 2016**. Fixa a Política Nacional de Inteligência. Publicado no DOU de 30-6-2016. 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*>, acessado em 31/05/2021.

BRASIL. **Lei nº 9.883, de 07 de dezembro de 1999**. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Publicada no DOU de 08/12/1999. Disponível em: <*http://www.planalto.gov.br/ccivil_03/leis/l9883.htm#:~:text=L9883&text=LEI%20No%209.883%2C%20DE,ABIN%2C%20e%20d%C3%A1%20outras%20provid%C3%AAncias*>, acessado em 28/05/2021.

BRASIL. Ministério da Justiça. **Doutrina Nacional de Inteligência de Segurança Pública - DNISP**. Brasília, DF. 2015.

CAMPOS, César José. **O Programa Delegacia Legal e seus Impactos no Sistema de Segurança Pública no Estado do Rio De Janeiro: Uma Contribuição da Engenharia de Produção na Segurança Pública.** Dissertação (Mestrado em Engenharia de Produção). COOPEE/UFRJ, Rio de Janeiro. 2012.

CEPIK, Marco. **Regime Político e Sistema de Inteligência no Brasil: Legitimidade e Efetividade como Desafios Institucionais**. Rio de Janeiro: Revista de Ciências Sociais, V. 48, nº 1. 2005.

DISPERJ (2015). **Doutrina de Inteligência de Segurança Pública do Estado do Rio de Janeiro.** Rio de Janeiro - RJ. Secretaria de Estado de Segurança. 2015.

FERREIRA, Romeu Antonio. **Criação da ISP**. Rio de Janeiro, RISP - Revista de Inteligência de Segurança Pública, vol. I, nº 1. 2020.

FRAZÃO, José Maria Frazão Neto**. Inteligência Policial e Investigação Policial: Diferenças Básicas entre a Atividade de Inteligência e a Investigação Policial**. Rio de Janeiro, RISP - Revista de Inteligência de Segurança Pública, v. 2, nº 2, p. 32-47. 2020.

GARDNER, Howard. **Estruturas da Mente. A Teoria das Inteligências Múltiplas.** Porto Alegre: Artes Médicas. 1994.

GONÇALVES, Joanisval B. **Atividade de Inteligência e Legislação Correlata**. 6ª ed. Niterói: Impetus. 2018.

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

LOWENTHAL, Mark M. **Intelligence: From Secrets to Policy.** Washington, DC. CQ Press, 2ª ed., 2003.

PLATT, Washington. **A Produção de Informações Estratégicas**. Tradução de Maj. Álvaro Galvão Pereira e Cap. Heitor Aquino Ferreira. 2ª ed., Biblioteca do Exército. Rio de Janeiro. Editora e Livraria Agir Editora. 1974.

RICH, Elaine. **Inteligência Artificial**. São Paulo. McGraw-Hill. 1988.

RIO DE JANEIRO. **Decreto nº 29, de 26 de outubro de 2018**. Dispõe sobre a Política de Inteligência de Segurança Pública do Estado do Rio de Janeiro (POLISPERJ). Rio de Janeiro, 2018. Publicado no DOERJ em 31-10-18.

RIO DE JANEIRO. **Decreto nº 45.126, de 13 de janeiro de 2015**. Aprova a nova doutrina de inteligência de segurança pública do Estado do Rio de Janeiro (DISPERJ) e dá outras providências. Rio de Janeiro, 2015. Publicado no DOERJ em 14/01/2015.

DADOS DOS AUTORES:

Marcus Castro Nunes Maia

Delegado de Polícia há 19 anos. Graduação em Direito e História. Pós-Graduação em Direito Público (UERJ), Segurança Pública (FGV) e Inteligência Estratégica (ESG). *Counterterrorism Course* (ICCT / *National Defense University*) e *Stability Police Units Course* (SPU/CoESPU/Carabinieri). Atuou em diversos segmentos da Polícia Civil, em unidades de investigação distrital e especializada. Formado em operações táticas especiais no Brasil (Polícia Civil e Polícia Federal) e Exterior (*Swat School / Miami Police Dpto*). Atuou como assistente e coordenador da CORE (Operações Táticas Especiais) por 04 anos e liderou essas equipes na retomada do Complexo do Alemão (2010). Exerceu funções de Assessor Especial de Diretores Gerais e Subsecretários Operacional e Administrativo. Analista-Chefe de Inteligência nos Departamentos do Interior e Especializada. Exerce o cargo de Diretor-Geral de Inteligência da Secretaria de Estado de Polícia Civil do Rio de Janeiro.

Marcelo dos Santos Dias Cola

Oficial de Cartório da Polícia Civil durante 31 anos. Formação como Analista de Inteligência com diversos cursos na área. Atuação em diversos segmentos da Polícia Civil, em unidades de investigação distrital e especializada, destacando-se na função de Analista de Inteligência (SIP). Atuou também como Analista de Inteligência nos Departamentos do Interior, Especializada da Assessoria de Inteligência da Polícia Civil e na Subsecretaria de Inteligência. Exerce a função de Coordenador de Inteligência na Diretoria Geral de Inteligência da Subsecretaria de Inteligência da Polícia Civil do Estado do Rio de Janeiro.

RISP
Revista de Inteligência de Segurança Pública
ISSN 2675-7168; 2675-7249

BUSCA DE DADOS EM FONTES ABERTAS (REDES SOCIAIS) E A ATIVIDADE DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA

Filipe dos Santos Antunes
Carlo Pegoraro Nicoloso
Antônio José Ferreira Gomes

RESUMO: A preocupação básica deste estudo é dar uma praticidade maior as tarefas rotineiras do agente de Inteligência que necessite coletar dados e conhecimentos em fontes abertas, especificamente em redes sociais, tudo pautado nos aspectos legais e jurídicos. Além de estabelecer uma metodologia fácil de executar, junto com a construção de um relatório acionável nos níveis estratégico, tático e operacional, auxiliando assim, agentes principiantes e experientes na área de Inteligência com um método prático, fundamentado em consultas a documentos, normativos, livros e outros materiais disponíveis e intrínsecos a área. A utilização de informações oriundas das fontes abertas, se da de forma sistemática e a inteligência de segurança pública deve trabalhar com a organização e processamento desses dados que resultam em conhecimento para subsidiar à ação do tomador de decisão. Com a pesquisa concluímos que atualmente existe pouca produção literária em português, sendo preciso produzir academicamente textos sobre Fontes Abertas, essas que podem contribuir muito para a produção de conhecimento de inteligência de segurança pública e servir como base prática para o analista de Inteligência.

Palavras-Chaves**:** Inteligência. Fonte Aberta. Redes Sociais. Aspectos Legais.

ABSTRACT/RESUMEN: The basic concern of this work is to give more practicality to the routine tasks of the Intelligence analyst who needs to collect data and knowledge in open sources, specifically on social networks, all based on legal and juridical aspects. This work aims to establish an easy to execute methodology, allied to the construction of an actionable report at the strategic, tactical and operational levels, thus assisting beginners and experienced analysts with a practical method, based on consults in documents, regulations, books and other available materials in the area. The use of information from open source is done in a systematic way and the Public Security Intelligence sector must organize and process these data resulting in knowledge to support the action of a decision maker. It was concluded that there is few content in Portuguese with this approach in the literature but many published in english. It is necessary to research on open source and to produce new articles about it, that can greatly contribute to the production of knowledge on public security intelligence and serve as a practical basis for the intelligence analyst.

Keywords/Palabras Clave: Intelligence. Open Source. Social Networks. Legal Aspects.

INTRODUÇÃO.

Na atividade de Inteligência de Segurança Pública, diversas técnicas podem ser empregadas em conjunto para obtenção de dados e informações necessárias à investigação policial e assessoria dos tomadores de decisão. Neste contexto, o artigo realiza, através de revisão da literatura, uma exploração dos processos de coleta de dados em fontes abertas, especificamente em redes sociais, visando atestar sua relevância para a atividade de inteligência e desenvolver um método prático de coleta de informações. O objetivo da metodologia criada é facilitar as tarefas rotineiras do analista de Inteligência que necessita realizar a coleta de informações através das redes sociais, uma vez que há pouca literatura disponível que possa servir como base prática para esse tema. Partindo assim da elaboração de um passo a passo simples de ser executado e pautado na legislação, tornando possível padronizar o processo de coleta de informações nas redes sociais, construir um relatório útil à apresentação em juízo, além de torná-lo acessível ao assessoramento nos níveis, estratégico, tático e operacional.

1. ATIVIDADE DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA E REDES SOCIAIS.

A atividade de Inteligência de Segurança Pública (ISP) em seus dois ramos, Inteligência e Contrainteligência, pode ser resumida em o exercício permanente e sistemático de ações especializadas para identificar ameaças reais ou potenciais na esfera de Segurança Pública, orientada para a produção de conhecimento voltado ao objetivo de subsidiar os tomadores de decisão, no planejamento e execução de uma política de Segurança Pública e de ações para prever atos criminosos de qualquer natureza que atente contra a ordem pública, a incolumidade das pessoas e do patrimônio.

No emprego da atividade de ISP, por parte de muitos profissionais existe uma grande confusão ocasionada pelo ato de nela se fazer investigação de ISP (confundida com a investigação policial). A Investigação (do latim *investigatio – onis*[1], que significa Indagação ou "*pesquisa que se faz buscando*", examinando e interrogando) de ISP tem como objetivo produzir conhecimentos para assessorar o tomador de decisão através da identificação de ameaças reais ou potenciais, e como consequência tem a possibilidade da obtenção de provas em virtude de sua atividade investigativa. Já a Investigação Policial tem como objetivos produzir conhecimento e após isso, auxiliar na produção de provas.

[1]- Disponível em <*https://dicionario.priberam.org/investiga%C3%A7%C3%B5es*>, acesso efetuado em 02/11/2020.

Com isso, o analista de Inteligência pode organizar seu conhecimento produzido em um relatório de Inteligência, para assessorar o tomador de decisão, e poderá efetuar um relatório técnico, para este ser utilizado como prova judicial. Mas para isso todo os dados da construção do conhecimento devem ser obtidos dentro da legalidade.

É sabido que a atividade de Inteligência clássica, em todo o mundo, requer sigilo e, muitas vezes, clandestinidade. Entretanto, na estrutura do ordenamento jurídico brasileiro, os órgãos públicos e os agentes públicos necessitam de previsões legais para desempenharem as suas ações com eficiência, inclusive na prática da atividade de ISP.

De acordo com o ordenamento jurídico nacional, a atividade de Inteligência deve ser desenvolvida em conformidade com as disposições legais específicas, nas quais se contemplem: a finalidade institucional de atividade de Estado; as competências e as atribuições funcionais; a estrutura organizacional compatível com a sua missão; uma política de pessoal adequada às exigências de elevada qualificação profissional e de sólida formação ética; e os controles normativos exercidos pelo Executivo, Legislativo, Judiciário e Ministério Público.

Quanto a sua utilização, por tratar-se de um instrumento do Estado a atividade de Inteligência só deverá ser empregada em seu benefício. No que se refere aos limites de sua extensão, o uso dos meios e de técnicas sigilosas deverá atender irrestritamente a legislação pertinente à atividade, aos direitos e garantias individuais, à fidelidade às instituições, aos princípios éticos que regem os interesses e segurança do Estado e da sociedade.

A reunião de dados pelos operadores de Inteligência ocorre de forma constante e por longos períodos de tempo, para que a agência de Inteligência possa entender as dinâmicas das organizações criminosas e os perfis dos crimes praticados por essas, da criminalidade e suas tendências, assim como do comportamento dos criminosos dessas organizações. Para isso, o agente pode utilizar-se de técnicas operacionais como o recrutamento de informantes, a infiltração de agentes em organizações criminosas, vigilâncias de locais e pessoas, acesso a conversas entre pessoas e grupos ou coletas em fontes abertas (exemplo, as Redes Sociais), para assessorar as decisões estratégicas e organizacionais dos tomadores de decisão, possibilitando assim que as organizações possam se preparar para enfrentar a criminalidade e evitar novos crimes.

Com isso, entre outros, surgem os seguintes questionamentos, até onde essas ações são legítimas, qual o limite para que elas sejam consideradas invasões a direitos e até onde a proteção da segurança da sociedade e dos demais indivíduos justifica a ação desses órgãos de inteligência. Considerando que os Serviços de Inteligência, apesar de serem aceitos e terem a sua importância reconhecida em diversos países, ainda são estigmatizados pelas sociedades que neles habitam. Tal estigma está associado à conotação negativa que a atividade possui, dado o conflito entre a vigilância estatal que ela pressupõe e os direitos individuais do cidadão, e diante dos questionamentos e das incertezas trazemos à baila o *caput* do artigo 37 da Constituição Federal.

> Segundo este princípio, a Administração Pública só pode agir quando houver expressa autorização legislativa, ou, como ensina BANDEIRA DE MELLO (1994, p. 48), "assim, o princípio da legalidade é o da completa submissão da Administração às leis", a qual "deve tão-somente obedecê-las, cumpri-las, pô-las em prática". Todos os seus agentes são, com isso, "reverentes, obsequiosos cumpridores das disposições gerais fixadas pelo Poder Legislativo, pois esta é a posição que lhes compete no Direito Brasileiro".

Este que preceitua que a Administração Pública "obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência".

A falta de informação a respeito da atividade, aliada a questões históricas, evoca no imaginário coletivo esses questionamentos, por isso a atividade de Inteligência ainda hoje é estigmatizada e mal interpretada pela população. Essa que tem como um de seus objetivos a preservação e defesa do Estado e de seu povo, sendo através da análise da complexidade dos fenômenos criminais que ela se mostra elemento fundamental para a minimização do uso da força pelos órgãos de segurança pública, por isso, sua valorização e fortalecimento são elementos fundamentais tanto de políticas públicas, como de anseios sociais. Uma vez que a atividade de Inteligência se liga aos valores mais fundamentais do Estado, as ações de Inteligência devem ser desenvolvidas para proteger esses valores, inclusive os direitos e garantias individuais. Esses direitos e garantias não podem, contudo, ser usados para perpetrar ações que configurem crimes. Mais do que isso, os direitos e garantias individuais não podem ser utilizados para proteger o indivíduo na execução de ações que coloquem em risco a coletividade e outros indivíduos, ameaçando o próprio Estado e a sociedade. Os direitos individuais não podem servir de proteção para ações contra o Estado que deve ser garantidor desses direitos.

1.1 A internet e as redes sociais.

O fenômeno da globalização, a evolução tecnológica e a facilidade de acesso à internet ocorrida nos últimos anos, geraram grande quantidade de dados e enorme facilidade no acesso, fazendo com que a mesma seja cada vez mais utilizada, inclusive no compartilhamento de informações pessoais de maneira voluntária em fontes abertas, como nas redes sociais, essas que vem sendo utilizadas amplamente por diversas áreas para a compreensão das relações sociais entre os indivíduos. A internet se tornou um manancial inesgotável de conhecimento e uma fonte de dados determinante para a tomada de decisões, monitoramento econômico, social e político de um país.

A obtenção das informações contidas nessas redes pode ser utilizada quando for preciso realizar levantamentos em localidades de difícil acesso pelas forças de segurança, aumentando a margem de confiabilidade e diminuindo assim os riscos aos agentes nas ações de busca para obtenção dos dados de Inteligência, além do contingenciamento de despesas relacionadas a deslocamentos, viaturas e servidores, agindo de maneira precisa em uma ação pontual.

As redes sociais podem e devem ser utilizadas como meio de assessoramento do tomador de decisão, já a utilização da mesma como informação técnica em processos judiciais, deve seguir ritos de tratamento, sob pena de anulação da prova.

Segundo Hiroshi[2], a análise das redes sociais pode ser uma grande ferramenta de obtenção de dados, uma fonte de informações.

> [...] observa-se que as redes sociais podem servir para auxiliar autoridades policiais de várias formas, seja no monitoramento de situações como nos casos de manifestações que possam afetar a ordem pública, seja no confronto direto com a criminalidade, como na repressão ao tráfico de drogas e na identificação e localização de criminosos. Todavia, o vasto repertório de informações que tramita nas redes sociais deve ser tratado de forma adequada pois corre-se o risco de perda de objetividade e eficácia. Por isso...as organizações policiais precisam desenvolver estratégias que possibilitem redefinir processos, automatizar tarefas e conduzir com efetividade o fluxo de conhecimentos, aliado ao aparelhamento policial com modernas tecnologias (HIROSHI, Pág. 66, 2011).

[2] - Hiroshi. Hélio. Utilização das Redes Sociais na Produção de Conhecimentos de Inteligência de Segurança Pública. O Alferes, Belo Horizonte, (25): 11-46, jul./dez. 2011.

1.2 A importância do monitoramento de redes sociais.

A definição de fonte, segundo o dicionário Michaellis, dentre os vários significados, é a causa, origem e princípio. Barreto e Wendt (2013, p. 4) definem fontes abertas como:

> Qualquer dado ou conhecimento que interesse ao profissional de inteligência ou de investigação para a produção de conhecimentos e ou provas admitidas em direito, tanto em processos cíveis quanto em processos penais e, ainda, em processos trabalhistas e administrativos (relativos a servidores públicos federais, estaduais e municipais).

O Brasil é o 3º país com maior número de usuários conectados à rede social *Facebook*, estimando cerca de 134 milhões de usuários ativos, valendo dizer que 63,26% de seus habitantes[3], possuem conta na plataforma, conforme pesquisa efetuada em 2019, intitulada TIC Domicílios – 2019[4] pelo Centro Regional de Estudos para o desenvolvimento da sociedade da informação (CETIC.br), vinculado ao Comitê Gestor da Internet no Brasil. Na mesma pesquisa observa-se que cerca de 92% dos usuários utilizam aparelhos de smartfone para envio de mensagem por *WhatsApp*, *Skype* ou *Facebook* (contabilizando também o Messenger, aplicativo vinculado à plataforma).

Além disso, estudos efetuados pela *Hootsuite* e pela *We Are Social* demonstram que o Brasil registra média diária de 9 horas e 17 minutos por dia de conexão on-line em redes sociais, percentual de 38,68% do dia, demonstrando assim a quantidade de informações diárias geradas nesses canais.

Com essa quantidade de informações postadas diariamente (Cerca de 500 *terabytes* de informação) a atividade de Inteligência de Segurança Pública (ISP) precisa evoluir com o uso das novas tecnologias e recursos legais relacionados a coletas de dados em fontes abertas visando o fornecimento de materiais para construção de informação que venha auxiliar o tomador de decisão em seu planejamento de operações na área de segurança pública. Deve-se considerar que os dados encontrados nas redes precisam passar por um processo de filtragem, edição e validação com outras informações disponíveis, para que possam ter valor agregado.

A ISP comunga com a investigação criminal na busca por dados para compor um conhecimento sobre uma determinada realidade de interesse. A primeira tem por objetivo munir o

[3] - Em 01/07/2020 conforme divulgação do IBGE, a população do Brasil chegou a 211,8 milhões de habitantes, verificado em <*https://tinyurl.com/y636d34l*> acesso em 13/11/2020.
[4] - Sítio: <*https://cetic.br/pt/tics/domicilios/2019/individuos/*>, acesso efetuado em 02/11/2020.

tomador de decisão, seja um chefe de Estado ou de governo, ou secretário de segurança pública, do maior, mais preciso e confiável leque de informações sobre a situação ou cenário existente ou que se projeta existir, a fim de garantir a melhor decisão a ser tomada, enquanto que a segunda visa à obtenção de dados que revelem a ocorrência de um fato criminoso, suas circunstâncias e seu protagonista, tendo como destinatário a autoridade policial e o promotor de justiça num primeiro momento e, por fim, o juiz, no exercício da atividade de persecução criminal.

A *Open Source Inteligence* (OSINT) ou Inteligência em Fontes Abertas tem como matéria prima, vários tipos de informações, que estejam disponíveis ao operador de segurança, podendo valer-se de fontes midiáticas, circunstância em que sua matéria prima para processamento estará disponível originalmente em jornais, revistas, programas de televisão e de rádio, ou contida em outros tipos de fontes jornalísticas hoje existentes no ambiente virtual da rede mundial de computadores.

Históricamente, a OSINT reponta o começo de suas atividades no final da década de 1930, mais especificamente na Universidade de Princeton, localizada em Nova Jersey/Estados Unidos da América (EUA), com a criação da *Foreing Broadcast Information Service* (FBIS) que durante a segunda guerra mundial (1939-1945) teve a função de analisar noticiários internacionais captados por meio de rádio, além do monitoramento de publicações oficiais relacionadas aos países envolvidos, também tendo sido utilizada no período da Guerra Fria (1947-1991), vindo a perder sua função, sob a alegação de que não existia ameaça ou inimigo aos EUA, vindo a ser novamente utilizado após o atentado contra o *World Trade Center* e Pentágono, realizado em 11 de Setembro de 2001, culminando com a criação do *Open Source Center* (OSC[5]) em Novembro de 2005, localizado em Reston, Virgina/EUA, vinculado à estrutura da *Central Intelligence Agency* (CIA).

A Organização do Tratado do Atlântico Norte (OTAN)[6] defende a utilização de *OSINT* desde o ano de 2001.

Com o passar dos anos, a imagery intelligence (IMINT), relacionada à busca de informações obtidas com imagens (satélites ou aeronaves) também foi inserida como parte da busca de OSINT.

[5] - Site: <*https://osc.gov/*>, acesso em 01/11/2020.
[6]- Organização criada no ano de 1949 com o objetivo de garantir a defesa coletiva dos países membros (atualmente 28) em resposta a ataques sofridos.

No Brasil, os primeiros registros acadêmicos relacionados à técnica de busca de informação em fonte aberta são do ano de 2005, com artigo sobre a análise de vínculos criminal, cuja autoria é do Delegado de Polícia Civil Celso Moreira Ferro Junior, do Distrito Federal.

Doutor em Ciência Política, Marco Aurélio Chaves Cepik, professor titular da Universidade Federal do Rio Grande do Sul, e professor visitante na *Renmin University of China* (RUC), Instituto Superior de Relações Internacionais de Moçambique (ISRI), *Naval Post Graduate School* (NPS-USA), *Facultad Latino Americana de Ciências Sociales* (FLACSO-EC) e *Indiana University of Pennsylvania* (IUP) (2003, p. 51) assim define OSINT:

> [...] obtenção legal de documentos oficiais sem restrições de segurança, na observação direta e não clandestina dos aspectos políticos, militares e econômicos da vida interna de outros países ou alvos, do monitoramento da mídia (jornais, rádio e televisão), da aquisição legal de livros e revistas especializadas de caráter técnico-científico, enfim, de um leque mais ou menos amplo de fontes disponíveis cujo acesso é permitido sem restrições especiais de segurança. Ele ainda afirma que "a chamada inteligência de fontes ostensivas, ou OSINT (*open source intelligence*), sempre foi importante para qualquer sistema governamental de Inteligência [...] (CEPIK, 2013, p. 51).

Essa Inteligência também se vale de material proveniente do mundo virtual, sem que ele seja, entretanto, midiático. É esse o caso em relação a produtos das modernas comunidades sociais, em suas diferentes expressões. Uma característica marcante de tal tipo de fonte é o fato de ser de conteúdo gerado pelo próprio usuário. É esse o caso das Redes Sociais, sítios pessoais em geral, sítios de material visual compartilhado, *wikis*, *blogs* e similares.

As redes sociais têm impacto tão significativo no cotidiano das pessoas, que elas se tornaram para muitas a única fonte de informações, além de motor de buscas para encontrar respostas a perguntas específicas, tornando-se um mecanismo dinâmico de exposição de opiniões e experiências. Essas características as tornam uma oportunidade jamais vista pelas comunidades de inteligência e órgãos de segurança pública no quesito de ser um manancial perene de extração de dados e informações.

No entanto, no parecer de Barreto (2015) a utilização das fontes abertas pela polícia judiciária tem logrado êxito nas mais variadas investigações. Exemplo tangível dessa prática são as infrações penais praticadas por membros de torcidas organizadas ou facções criminosas que são postadas em ambientes virtuais. A partir da análise do conteúdo publicado em redes sociais é possível estabelecer o *modus operandi*, bem como coletar indícios de materialidade delitiva, além da possibilidade de identificação de autores que até então se julgavam inatingíveis por postarem conteúdo na *Web*.

Igualmente, na concepção desse autor, o emprego de fontes abertas prospera em casos de homicídio, quando se acessam informações disponíveis em perfis de redes sociais de criminoso e vítima; na utilização de softwares e aplicações gratuitas de internet que auxiliam no planejamento de operações policiais; na consulta de dados úteis sobre o investigado realizadas em sites de tribunais e na utilização de alertas para auxiliar na localização e captura de foragidos em outros estados.

2. O CICLO DE PRODUÇÃO DE CONHECIMENTO DE ISP.

O Ciclo de Produção de Conhecimento de ISP deve ser empregado pelo profissional de ISP, com metodologia própria da atividade, formada pelas seguintes fases lógicas e não necessariamente cronológicas: Planejamento, Reunião de Dados, Processamento e Utilização. Alguns autores como Santos[7] em "Análise de Inteligência" sugerem cinco fases para compor o ciclo, Planejamento, Reunião de Dados, Análise, Interpretação e Difusão.

É importante lembrar que, mesmo sendo no nível operacional ou tático a fase de Planejamento não deve ser considerada desnecessária ou de pouca importância, pois ela nos dará o norte a seguir.

2.1 O Planejamento.

Na fase de Planejamento o analista deve definir: o assunto a ser tratado, balizando as perguntas básicas "o que", "quem", "quando" e "onde"; delimitando a faixa de tempo para o assunto que deve ser enquadrado; quem será o usuário do conhecimento produzido e qual a sua finalidade; o prazo, que se relaciona ao tempo disponível para a entrega do conhecimento; os aspectos essenciais conhecidos, devendo separar as informações disponíveis em completas e incompletas, as que expressam certeza das que apresentam algum grau de incerteza; os aspectos essenciais a conhecer, listando dados ou conhecimentos a serem conhecidos e a forma que estes poderão ser obtidos, definindo o esforço de coleta e a dimensão da busca; outras medidas como o nível de sigilo necessário para a proteção dos envolvidos e da organização, quem tem a necessidade de conhecer, a necessidade de contatos com pessoas e organizações, assim como recursos financeiros.

[7]- Santos, Marco Antonio. Análise de Inteligência. Caderno de Estudos da Pós-graduação em Inteligência e Gestão Estratégica da Faculdade Unyleya. Brasília, DF. 2010.

2.2 Reunião de dados, coleta e monitoramento de dados de redes sociais.

Na fase de reunião de dados o analista deve procurar obter os dados ou conhecimentos que respondam ou complementem os aspectos essenciais que ele definiu como a conhecer, efetuando ações de coleta. Na reunião de informações em fonte aberta, as técnicas utilizadas para coleta e monitoramento dos dados encontrados especificamente em redes sociais, necessitam de atenção e grande capacidade de comparação da pessoa que está efetuando.

Na análise do material proveniente da OSINT, se faz necessário algumas ferramentas que auxiliam a não cair na teoria da "*árvore com frutos envenenados*"[8], vindo a trazer vício de licitude da prova obtida, tanto no contexto informação (Inteligência) como na eventual produção de prova (persecução penal), caso assim esteja sendo trabalhado, seguindo os seguintes passos:

1) A cada informação considerada relevante, efetue um quadro onde possam ficar disponíveis as seguintes informações, origem da informação (colocando o endereço na internet onde a mesma está disponível), dado encontrado (gerando histórico relacionado ao dado que foi encontrado) e condição (nesse caso, se o dado encontrado está de acordo com a informação a ser encontrada ou se o dado refuta a informação a ser encontrada), trazendo exemplo simples para isso:

[8] - RHC 51.531/RO, Sexta Turma do Supremo Tribunal de Justiça (STJ). Rel. Ministro Nefi Cordeiro. Diário de Justiça (DJ) de 09/05/2016, disponível em https://stj.jusbrasil.com.br/jurisprudencia/340165638/recurso-ordinario-em-habeas-corpus-rhc-51531-ro-2014-0232367-7/inteiro-teor-340165652, acesso em 01/11/2020.

Figura 1 – TABELA DE FILTRO DE INFORMAÇÕES

Origem da informação	Dado encontrado	Condição do Dado
https://www.facebook.com/Palha%C3%A7o-matador-372363649612477/	Site relacionado a apologia a crimes e possiveis participações de integrantes de organizações criminosas atuantes, criada em 28 de dezembro de 2014. Informações relacionadas ao Estado do Pernambuco.	Apoia a Teoria Atual
https://www.facebook.com/Palha%C3%A7o-Matador-177132679398192/	Site de grupo social, relacionado a rede social facebook, embora com conteúdo improprio, não estaria relacionado a integrantes de organizações criminosas. Informações relacioandas ao Estado de São Paulo	Refuta a Teoria Atual

Fonte**:** elaboração dos autores.

2) Verifique quais as lacunas existentes na informação analisada, e avalie o fomento de perguntas adicionais que devem ser respondidas para a complementação da informação que será efetuada, considerando as possibilidades que podem ocorrer.

3) Avalie a relevância e confiabilidade da informação, analisando principalmente a fonte da mesma, principalmente o histórico da fonte em relação ao dado abordado, descartando as informações que não possuem subsídio confiável, sempre atento a contrainformação e contrapropaganda.

4) Quando efetuar seu documento final, deve sempre se recordar do princípio da simplicidade, considerando o desconhecimento ou não por parte do tomador de decisão, evitando palavras dúbias ou prolixas que possam criar alguma tendência de má interpretação da informação que se planejou fomentar.

Em coleta e monitoramento de dados é possível utilizar, por exemplo, a plataforma de compartilhamento de vídeos da empresa Google[9], onde pode ser efetuado o monitoramento e coleta de

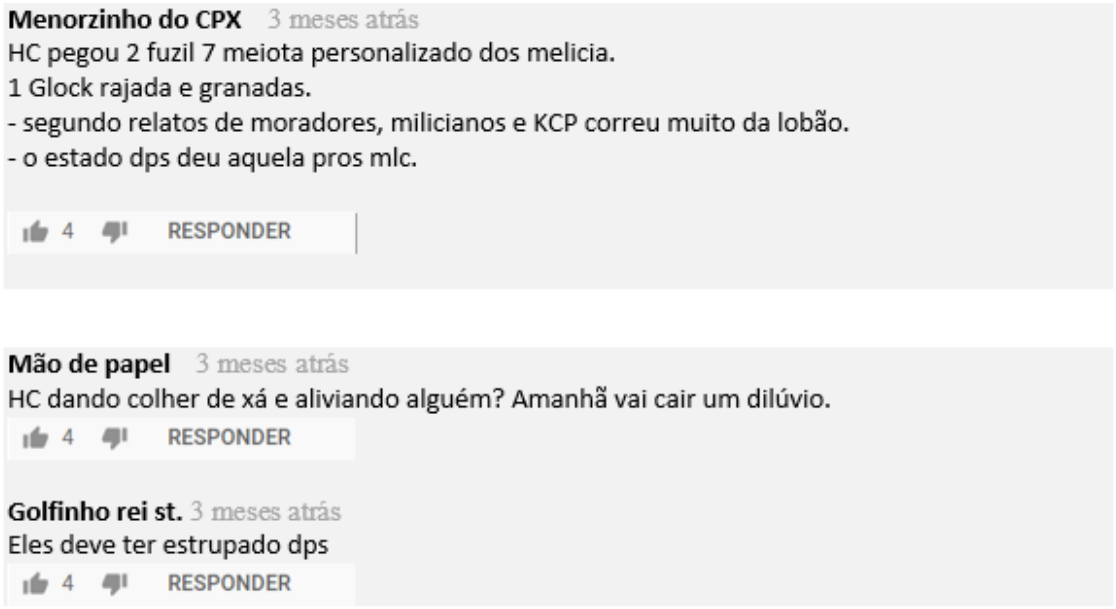
[9]- Google LLC é uma empresa multinacional de serviços online e software dos Estados Unidos. O Google hospeda e desenvolve uma série de serviços e produtos baseados na internet e gera lucro principalmente através da publicidade pelo AdWords. A Google é a principal subsidiária da Alphabet Inc.

informações sobre morte, mensagens, possíveis integrantes, simpatizantes, ideologia e músicas vinculadas à facção criminosa Comando Vermelho (CV), como no exemplo abaixo:

Usando como exemplo um site de rede social em plataforma de vídeos, que possibilita comentários de pessoas nos vídeos postados.

Nas postagens efetuadas nos vídeos, verificou-se comentários possivelmente vinculados a organizações criminosas, tal postagem possuía considerável quantitativo de visualizações, podendo ser avaliado o grau de popularidade do mesmo.

Figura 2 – MONITORAMENTO EM CHAT DE REDE SOCIAL DE VÍDEOS.



Fonte**:** elaboração dos autores.

As postagens verificadas trouxeram dados valiosos, que podem auxiliar de maneira mais assertiva na identificação de algum possível membro de organização criminosa, sendo ainda possível nos comentários efetuados, a verificação de embates contra outros grupos inimigos que porventura venham a acontecer.

No monitoramento de diversas Redes sociais, tais como F*acebook*, *Instagram*, dentre outras, a gama de posicionamentos do Supremo Tribunal Federal (STF) no tocante a utilização ou não de

postagens da plataforma, demonstra maior cautela do operador de inteligência, na utilização desse tipo de conteúdo.

Outra rede social, que teve sua utilização evidenciada e aumentada foi a plataforma *Twitter*[10] com sede em São Francisco, Califórnia, estimando cerca de 41 milhões de usuários somente no Brasil[11], tal quantidade perde somente para o quantitativo de usuários nos Estados Unidos da América (EUA), com cerca de 141 milhões.

O Twitter teve sua utilização aumentada por integrantes de comunidades e também do crime organizado no Brasil, para demonstração de fatos/situações ocorridas em seus locais de residência ou bases territoriais, acaba sendo utilizado como noticiário popular local, gerando grande quantidade de dados, que podem ser úteis na análise de informações.

Após a coleta e análise do material identificado, podemos utilizar este modelo simples e versátil de relatório, que pode ser aplicado durante a fase da Reunião de Dados, baseando-se nos aspectos essenciais a conhecer (fase de Planejamento), sempre obedecendo às regras de partir das ações mais simples para as mais complexas, com recursos de custos mais baixos e de menor risco de exposição para o analista e sua AI, às ações de maior custo e risco mais elevado, utilizando assim todos os meios disponíveis antes de acionar outra agência. Nesse modelo, as informações devem ser lançadas à medida que vão sendo observadas, dessa forma, além do próprio analista, outros podem no futuro acionar a informação ao acessar o arquivo, observando o caminho tomado do início ao final da coleta dos dados, além de também poder mensurar sua evolução, quanto ao tempo gasto na construção de cada relatório.

10 - Disponível em <*https://twitter.com*/>.
11 - Disponível em <*http://ecmetrics.com/pt/o-brasil-e-o-segundo-colocado-em-numero-de-usuarios-do-twitter/*>.

Figura 3 - MODELO DE RELATÓRIO DE MONITORAMENTO DE REDES SOCIAIS

RELATÓRIO DE FONTE ABERTA EM REDE SOCIAL	
DATA	01/01/2020
HORA	09h00m
COMENTÁRIO DO ANALISTA	Partindo dos aspectos conhecidos, sabe-se que o nacional de nome desconhecido, cujo o vulgo é JOAZINHO, é membro da facção local. Com base nos aspectos conhecidos, foi possível encontrar em fonte aberta uma imagem de um homem aparentando ser JOAOZINHO, em uma rede social cujo a identificação do perfil é "@JZO_CVL", na imagem uma pessoa, cujo o perfil é "@MARIAZINHA", se identificou com sua prima, comentando na imagem "saudades primo".
CAPTURA DA IMAGEM	
LINK	https://switter.com/log048759

Fonte: Autores.

Figura 4 - MODELO DE RELATÓRIO DE MONITORAMENTO DE REDES SOCIAIS

DATA	01/01/2020
HORA	09h05m
COMENTÁRIO DO ANALISTA	Através das imagens e comentários obtidos no perfil "@MARIAZINHA", foi possível encontrar em outra rede social a mesma pessoa, porém nesse perfil aberto a mesma se intitula como "MARIA LÚCIA NEVES" (maria_lucia.30). Em uma de suas fotos postada nesta rede, ela marcou o perfil de nome "JOAO NEVES" (joao.22?) e nos comentários escreveu "como o tempo nos fez bem primo, kkkkk"
CAPTURA DA IMAGEM	
LINK	https://www.tabecook.com/photo.php?fbid=704868&set=a.&theater

Fonte: Autores.

Há ainda a possibilidade de utilizar um outro modelo, mais completo e um pouco mais complexo, que pode ser empregado sempre que houver a necessidade de manter monitoramento por um período de tempo maior e com maior profundidade.

Figura 5 - MODELO DE RELATÓRIO DE MONITORAMENTO DE REDES SOCIAIS

DATA	DATA DO DIA EM QUE SE DEPAROU COM O DADO.
HORA	HORA QUE SE DEPAROU COM O DADO.
FONTE	SE O DADO FOI ENCONTRADO EM REDE SOCIAL, EM SITE, JORNAL, ATRAVÉS DE CONVERSA POR APP, ETC.
ASSUNTO	DESCRIÇÃO DO DADO QUE FOI ENCONTRADO.
IMAGEM	IMAGEM DO DADO OBTIDO.
CREDIBILIDADE	SE A FONTE OFERECE NENHUMA, BAIXA OU ALTA CREDIBILIDADE. OBSERVANDO SEMPRE A AUTENTICIDADE, CONFIANÇA E COMPETÊNCIA DA FONTE.
COERÊNCIA DO DADO	SE A INFORMAÇÃO É COERENTE OU CONTRADITÓRIA À OUTRAS JÁ OBTIDAS.
LINK	LINK DE OBTENÇÃO DO DADO DE FONTE ABERTA.

Fonte: Autores.

2.3 Análise, interpretação e difusão.

Na Análise é de suma importância ter o cuidado de verificar com atenção a credibilidade do conteúdo obtido, uma vez que as informações obtidas sobre o alvo podem incorrer em falsas verdades (quando achamos que um perfil por ter características físicas semelhantes, se trata do alvo, por exemplo), também é preciso avaliar a pertinência dos dados obtidos e a relevância dos dados selecionados. Após realizar isso, o analista deve determinar quais são as frações significativas para o conhecimento que se quer produzir, integrar os dados selecionados de forma coerente, ordenada, lógica e cronológica, a fim de interpretá-los e sintetizá-los em um conhecimento.

Na Interpretação o analista, utilizando-se de operações de raciocínio lógico, deve determinar de forma conclusiva o significado final do assunto tratado, atendendo os aspectos essenciais do assunto (fase de planejamento) e tendo o cuidado de ser claro e sucinto, de maneira que consiga fazer com que o leitor do conhecimento consiga entender exatamente o que ele quer passar. A interpretação é o resultado do trabalho do analista.

Por último, na fase de Difusão, o analista deve ter o cuidado de colocar as informações em documento próprio, obedecendo à estrutura preconizada em sua instituição, assim como a segurança necessária, pois muitas vezes um excelente trabalho pode se perder por ter sido enviado ao destinatário errado ou fora do momento oportuno.

CONCLUSÃO.

A Atividade de Inteligência tem como intuito reunir, processar e difundir conhecimentos com o maior nível de certeza possível para assessorar o tomador de decisão e os dados obtidos em fontes abertas (redes sociais), podem subsidiar a tomada de decisão com um alto grau de certeza em níveis estratégico, tático e operacional, satisfazendo assim suas necessidades informacionais, graus de profundidade e velocidade de resposta. Graças a revolução na tecnologia da informação, as fontes abertas (os dados) tornaram-se mais acessíveis, onipresentes e valiosas.

Os desafios enfrentados por uma Inteligência baseada em fontes abertas são muitos, pois, existem vários requisitos que necessitam de integração e equilíbrio para tornarem seus efeitos tangíveis, também não podemos esquecer que todo o processo de coleta deve estar dentro da legalidade.

À luz da Constituição Federal de 1988, a Inteligência em fontes abertas coaduna com o princípio da eficiência, pois potencializa o trabalho do analista de Inteligência em sua função precípua de assessorar os tomadores de decisão, além disso, o alto grau de oportunidade, aliado à grande quantidade de informações dispostas a baixo custo para obtê-las, também pode ser considerado.

Através da pesquisa tornou-se evidente que as fontes abertas propiciam um leque enorme de informações de domínio público, que se bem trabalhadas por profissionais de Inteligência capacitados, trazem enormes avanços para enfrentar os atuais desafios da área de Inteligência de Segurança Pública, no combate às organizações criminosas.

REFERÊNCIAS:

BARRETTA, Evandro Sponchiado. **A Utilização da Inteligência de Fontes Abertas nas Investigações Policiais**. 2018. Pg 54. Monografia (Pós-Graduação Lato Sensu em Inteligência de Segurança Pública), Universidade do Sul de Santa Catarina, Pato Branco. Disponível em:

<https://riuni.unisul.br/bitstream/handle/12345/9513/monografia%20OSINT.pdf?sequence=1&isAllowed=y>. Acesso em: 11 de novembro de 2020.

BARRETO, Alesandro Gonçalves. **Utilização de Fontes Abertas na Investigação Policial**. Direito e TI. 2015. Disponível em: *<http://direitoeti.com.br/artigos/utilizacao-de-fontes-abertas-na-investigacao-policial/>*. Acesso em: 10 de novembro de 2020.

BRASIL. **Decreto n° 8.793, de 29 de junho de 2016**. Fixa a Política Nacional de Inteligência. Brasília, Distrito Federal: Presidência da República, [2016]. Disponível em: *<http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm>*. Acesso em: 01 de novembro de 2020.

BRASIL. **Decreto 8.793, de 29 de junho de 2016**. Aprova a Estratégia Nacional de Inteligência. Brasília, Distrito Federal: Presidência da República, [2016]. Disponível em: *<http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/dsn/Dsn14503.htm>*. Acesso em: 04 de novembro de 2020.

BRITO, Vladimir de Paula. **Novos Paradigmas para a Inteligência Policial**. 2006. p. 161. Projeto Final - Especialização em inteligência competitiva. Universidade Federal do Amazonas, Manaus. 2006. Disponível em: *<https://pt.scribd.com/document/286831855/2-Novos-Paradigmas-Para-a-Inteligencia-Policial>*. Acesso em: 06 de novembro de 2020.

CEPIK, Marco Aurélio Chaves. **Espionagem e Democracia.** Rio de Janeiro: FGV, 2003. Disponível em: *<http://professor.ufrgs.br/marcocepik/files/cepik_-_2003_-_fgv_-_espionagem_e_democracia_21-apr-14_1.compressed.pdf>*. Acesso em: 01 de novembro de 2020.

HIROSHI, Hélio. **Utilização das Redes Sociais na Produção de Conhecimentos de Inteligência de Segurança Pública**. O Alferes, Belo Horizonte, nº 25, p. 11-46, jul./dez. 2011.

MINISTÉRIO DA JUSTIÇA (MJ). **Resolução nº 1, de 15 de julho de 2009**. Regulamenta o Subsistema de Inteligência de Segurança Pública - SISP. Brasília, Distrito Federal: Secretaria Nacional de Segurança Pública, [2009]. Disponível em: *<http://www.migalhas.com.br/Quentes/17,MI90861,91041-Justica+regulamenta+o+Subsistema+de+Inteligencia+de+Seguranca+Publica>*. Acesso em: 03 de novembro de 2020.

NICOLOSO, Carlo Pegoraro. **O Uso das Redes Sociais, pela Facção Primeiro Comando da Capital, para Disseminação de Informações e Práticas Criminosas**. Trabalho de Conclusão de Curso - Especialização em Inteligência Policial. Faculdade Unyleya, Florianópolis. 2018.

PROCURADORIA DA REPÚBLICA DO ESTADO DO PARÁ. **Catálogo de Fontes Abertas**. Belém: Ministério Público Federal, [2019].
Disponível em: *<http://bibliotecadigital.mpf.mp.br/bdmpf/handle/11549/188193>*. Acesso em: 10 de novembro de 2020.

SANTOS, Marco Antonio. **Análise de Inteligência**. Caderno de Estudos da Pós-Graduação em Inteligência e Gestão Estratégica da Faculdade Unyleya. Brasília, DF. 2010.

STEELE, Robert David. **Open Source Intelligence.** Forbes. 19/04/2006. Disponível em: <*https://www.forbes.com/2006/04/15/open-source-intelligence_cx_rs_06slate_0418steele*>. Acesso em: 02 de novembro de 2020.

DADOS DOS AUTORES:

Filipe dos Santos Antunes.

Graduado em Psicologia pela Associação Brasileira de Ensino Universitário - UNIABEU (2017). Pós-Graduado em Neuropsicologia pela Universidade Candido Mendes - UCAM (2019), Pós-Graduado em Inteligência e Gestão Estratégica pela Faculdade UNYLEYA (2020). Atualmente é Policial Militar e atua como analista de Inteligência.

Currículo Lattes: http://lattes.cnpq.br/3385668698399319

ORCID: https://orcid.org/0000-0002-9463-9475?lang=pt

Carlo Pergoraro Nicoloso.

Bacharel em Ciências Contábeis pela Universidade do Planalto Catarinense (2002). Especialista em Gestão de Administração Pública pela Universidade Castelo Branco, Cátedra da UNESCO, em convênio com o Exército Brasileiro (2010), Especialista em Gestão e Política de Segurança Pública pela Universidade Estácio de Sá (2012), Especialista em Inteligência Policial pela Faculdade Unyleya (2018), Especialista em Inteligência Competitiva e Contrainteligência Corporativa pela Faculdade Unyleya (2019), atualmente especializando-se em Cybercrime e Cybersecurity - Prevenção e Investigação de Crimes Digitais (2020). Docente da Academia de Administração Prisional e Socioeducativa do Estado de Santa Catarina (ACAPS), Docente da Secretaria Nacional de Segurança Pública na disciplina de Inteligência de Segurança Pública. Atualmente é Policial Penal do Estado de Santa Catarina. Atua nos seguintes temas:

Administração Pública, Inteligência de Estado, Direitos Humanos, Fontes Abertas, Política Pública e Defesa Nacional.

Currículo Lattes: http://lattes.cnpq.br/1082774934921625

ORCID: https://orcid.org/0000-0002-2533-8249

Antônio José Ferreira Gomes

Pós-Graduado em Inteligência Policial e Penitenciária pela Faculdade Verbo Educacional (2020); Pós-Graduado em Docência do Ensino Superior pela Faculdade Metropolitana São Carlos (2020). Possui o Curso Superior em Tecnologia em Segurança Pública pela Universidade Estácio de Sá (2017). Atualmente é Policial Militar na Secretaria de Estado de Polícia Militar do Rio de Janeiro, e também, é Instrutor no Centro de Formação e Aperfeiçoamento de Praças - CFAP/SEPM.

Currículo Lattes: http://lattes.cnpq.br/1598883818728413

ORCID: https://orcid.org/0000-0001-6936-8135

RISP
Revista de Inteligência de Segurança Pública
ISSN 2675-7168; 2675-7249

ASPECTOS TEÓRICOS E DOUTRINÁRIOS DA ANÁLISE DE VERACIDADE NO ÂMBITO DA INTELIGÊNCIA DE SEGURANÇA PÚBLICA

Renato Pires Moreira
Imer Alves de Brito Júnior

RESUMO: O presente artigo tem por objetivo revelar os fundamentos teóricos e doutrinários relativos à Técnica Operacional de Inteligência (TOI) - Análise de Veracidade, no âmbito da Inteligência de Segurança Pública. A Inteligência de Segurança Pública possui um rol de Técnicas Operacionais de Inteligência, sendo uma destas a Análise de Veracidade, que tem sua importância justamente por auxiliar o Agente de Inteligência a discernir quando alguém mente ou fala a verdade, trazendo informações de melhor qualidade e confiabilidade, principalmente quando utiliza a Entrevista como Ação de Busca. O foco deste trabalho será verificar a relevância desta técnica na atividade de ISP por meio da bibliografia pesquisada. Desta forma é verificada neste artigo a importância da TOI - Análise de Veracidade para a Inteligência de Segurança Pública nas diversas Ações e Operações de Inteligência que podem ser realizadas, conforme será demonstrado.

Palavras-Chave: Inteligência de Segurança Pública. Análise de Veracidade. Entrevista.

ABSTRACT: The porpose of this article is to reveal the theoretical and doctrinal foundations related to Operational Intelligence Technique - Verification Analysis, at the scope of the Public Security Intelligence. Public Security Intelligence has a roll of Operational Intelligence Techniques, one of these Verification Analysis, which is only important in helping the Intelligence Agent discern when someone lies or speaks the truth, bringing better quality information and reliability, especially when using Interview as a Search Action. The focus of this work will verify the relevance of this activity in the ISP through the searched bibliography. Thus, it is verified in this article the importance of TOI Verification Analysis for Public Security Intelligence in the various Intelligence Actions and Operations that can be performed, as will be demonstrated.

Keywords: Public Security Intelligence. Veracity Analysis. Interview.

INTRODUÇÃO

O presente estudo tem origem na importância que a atividade de inteligência dispõe sobre os aspectos teóricos e doutrinários da análise de veracidade, notadamente, daquelas que culminam em ações com reflexos sociais quando do entendimento da verdade.

Desde os mais antigos registros sobre atividade humana, é sabido que a informação é fator decisivo para a sobrevivência de um grupo, assim como para seu avanço nas mais variadas áreas, seja tecnológica, econômica ou em qualquer outra área. Porém, quando se detém uma informação e esta não é possível de definir sua autenticidade, ela se torna duvidosa e pode custar muitos recursos, a quem à detém ou fornece, de forma desnecessária, bem como pode ocasionar um enorme prejuízo devido à falta de ação, pela falta de credibilidade.

Uma das fontes mais importantes de informação é o próprio ser humano, sendo que este pode valer-se de mentiras e omissões devido à interesses próprios, pressão de terceiros, entre outras situações que motivariam um ser humano a esconder a verdade. Para tanto, sob a ótica da doutrina de Inteligência de Segurança Pública, existem basicamente dois momentos em que a informação será checada: na fase de reunião de dados, quando o agente de inteligência estiver recebendo informações diretamente da fonte humana, momento este em que poderá utilizar da Técnica de Operações de Inteligência de Análise de Veracidade da Doutrina Nacional de Inteligência de Segurança Pública (DNISP), ou na terceira fase da MPC, a fase de processamento, momento no qual o analista irá sopesar algumas variáveis procedendo a avaliação do conhecimento em relação à pertinência e o grau de credibilidade dos dados e/ou conhecimentos reunidos.

Para o presente artigo científico, o foco será na análise de veracidade enquanto Técnica Operacional de Inteligência. Ainda, demonstrar-se-á Inteligência Humana como fonte de dados, ao invés da Inteligência Eletrônica. Dessa forma, serão elencados os principais fatores que tratam sobre a Análise de Veracidade no âmbito da atividade de Inteligência de Segurança Pública.

A atividade de Inteligência de Segurança Pública, segundo a DNISP (BRASIL, 2014), tem como uma de suas finalidades a identificação, avaliação e acompanhamento de ameaças reais ou potenciais que acontecem no âmbito da Segurança Pública para subsidiar planejamentos futuros que irão prevenir, neutralizar e reprimir atos criminosos de qualquer natureza que atentem à ordem pública, à incolumidade das pessoas e do patrimônio.

Para identificar e avaliar ameaças reais, faz-se necessário e impetuoso que as informações sejam autênticas, providas de verdade. Dessa forma, na Metodologia de Produção do Conhecimento, teremos dois momentos em que haverá a apuração da verdade. Durante a fase de Reunião de Dados e/ou Conhecimentos e durante a fase de Processamento.

Na fase de Reunião de dados, utilizando-se da Técnica de Análise de Veracidade, segundo o próprio conceito existente na DNISP (BRASIL, 2014), "Utilizada para verificar, por meio de recursos tecnológicos ou metodologia própria, se uma pessoa está falando a verdade sobre fatos e situações". Ainda, o Agente de Inteligência irá atrás do dado negado a ser obtido por meio de Inteligência Humana ou Inteligência Eletrônica, e verificará se a pessoa está falando a verdade sobre fatos e situações. Ocorre que o estudo da Análise de Veracidade nos traz ferramentas para verificar o grau de veracidade de algo que foi dito, assunto que será trabalhado no desenvolvimento deste trabalho.

A outra etapa onde a veracidade é avaliada seria na terceira fase da MPC, ou seja, a fase de processamento, porém esta fase não será objeto deste estudo, uma vez que o foco deste trabalho científico será enumerar e identificar a metodologia empregada durante a execução da técnica de Análise de Veracidade em ações e operações de inteligência no âmbito da Inteligência de Segurança Pública (ISP).

No caso de um agente sem treinamento, ou que aprendeu de forma inadequada a metodologia de execução da Técnica de Análise de Veracidade, executar missão que exija a aplicação desta técnica, os danos colaterais de uma falha em tal ação/operação podem ser críticos ao Agente de Inteligência, a Agência de Inteligência e ao Sistema de Inteligência, uma vez que a falha pode vir a causar superexposição da Atividade de Inteligência.

A pesquisa é de cunho qualitativo e pautou-se na coleta de informações e análise crítica por meio do estudo do fenômeno e sua relação com os diversos contextos sociais, em especial às contribuições da atividade de inteligência. O procedimento adotado nesta pesquisa será o bibliográfico.

Destaca-se que o presente artigo científico demonstrará a Análise de Veracidade enquanto imprescindível à atividade de Inteligência de Segurança Pública, uma vez que é uma técnica acessória que garante a veracidade das informações e subsidia dessa maneira a tomada de decisões com confiabilidade, seguindo os princípios da Atividade de Inteligência.

1 ANÁLISE DE VERACIDADE, COMPARAÇÕES ENTRE DOUTRINAS.

A DNISP menciona a Análise de Veracidade como sendo uma técnica operacional de ISP que "utilizada para verificar, por meio de recursos tecnológicos ou metodologia própria, se uma pessoa está faltando a verdade sobre fatos e situações (BRASIL, 2014).

Contudo a Doutrina de Inteligência de Segurança Pública do Estado do Rio de Janeiro - DISPERJ (2015) *apud* Pinto (2020) define Análise de Veracidade da seguinte forma: “é a TOI utilizada para analisar, por meio de recursos tecnológicos, se há veracidade no que uma pessoa esteja falando”.

Segundo Pinto (2019), o qual pertence ao Instituto Brasileiro de Análise de Veracidade e autor do artigo: “Análise de Veracidade: diferentes abordagens doutrinárias no âmbito da Inteligência de Segurança Pública”, explica as diferenças entre os conceitos:

> [...] Em primeiro lugar, observa-se o fato de que enquanto a DNISP atribui à Análise de Veracidade o objetivo de "verificar (...) se uma pessoa está dizendo a verdade sobre fatos e situações" (grifo do autor), a DISPERJ - por outro lado - opta por utilizar o verbo" analisar (...) se há veracidade no que uma pessoa esteja falando" (grifo do autor). De fato, há uma substancial diferença entre verificar e analisar um determinado fenômeno [...] (PINTO, 2019).

O autor supracitado afirma que comparando os dois verbos verificar e analisar, destaca-se que o verbo verificar relaciona-se melhor com o verbo observar, constatar se algo (já esperado) aconteceu ou não, comparando o resultado constatado com um padrão já estabelecido anteriormente; já o verbo analisar, amolda-se à identificação de fatores que influenciaram na ocorrência ou não de dado fenômeno, ou seja, leva em consideração o contexto e as diferenças a que cada pessoa que é submetida a análise se encontra.

Verifica-se com o estudo das várias metodologias existentes que tratam acerca de Análise de Veracidade que não há um padrão único que estabelecerá se o que foi dito pela pessoa é verdade ou não. Destarte disso, para que a técnica seja corretamente aplicada deve-se levar em conta todas as especificidades do alvo a ser analisado, assim como o ambiente em que se encontra e contexto da situação (PINTO, 2019).

Segundo Pinto (2019), outra diferença entre as doutrinas reside no fato de que a DNISP (2014) prevê que “Análise de Veracidade tem por objetivo ‘verificar [...] se uma pessoa está dizendo a verdade sobre fatos e situações”. Já a DISPERJ (2015) *apud* Pinto (2020), diferencia o conceito afirmando que [esta técnica consiste em "analisar [...] se há veracidade no que uma pessoa esteja falando”.

É verificável constatar que, segundo a experiência, esta mostra que na maioria das vezes, o agente de inteligência, não possui condições, durante a execução da missão, de avaliar de forma absoluta e desprovida de erros, se o que foi dito pelo alvo representa a verdade ou não; o que é possível naquele momento é a execução de uma análise de veracidade, empregando as metodologias corretas

para obter um grau de veracidade no que foi dito. A palavra verdade indica a exata correspondência entre o que foi dito e o que realmente aconteceu, já a palavra veracidade representa o grau em que a declaração parece ser verdadeira, associando-se com o conceito de credibilidade (PINTO, 2019).

Dessa forma a diferença de conceitos de verdade e veracidade é um dos tópicos importantes para se entender a ideia da finalidade para a qual existe a técnica de Análise de Veracidade. Esta não menciona a garantia perfeita e límpida de que foi contada a verdade ou não, mas sim estabelecer um grau de credibilidade na informação utilizando-se das metodologias próprias e adequando-as ao contexto e ambiente onde se encontra o alvo.

Por último, entrando ainda mais na diferença entre os conceitos existentes na DNISP e na DISPERJ *apud* Pinto (2020), verifica-se que na primeira verifica-se a possibilidade da execução da técnica de Análise de Veracidade com metodologias próprias além dos recursos tecnológicos, diferente do que é mencionado na DISPERJ *apud* Pinto (2020) que traz o uso apenas de recursos tecnológicos. Verifica-se, com a experiência, que os Agentes de Inteligência se deparam com muito mais oportunidades de utilizar a técnica de Análise de Veracidade por meio de interação pessoal verbal com o alvo do que se utilizando de tecnologias como polígrafo ou outros equipamentos eletrônicos destinados à esta finalidade. Dessa forma entende-se que o conceito mais abrangente é mais adequado para a atividade de ISP.

2 AÇÕES E OPERAÇÕES DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA.

Para a Doutrina Nacional de Inteligência de Segurança Pública (BRASIL, 2014), Ações de Inteligência de Segurança Pública são:

> [...] todos os procedimentos e medidas realizadas por uma AI para dispor dos dados necessários e suficientes para a produção do conhecimento, centrados, de um modo geral, em dois tipos de ações de Inteligência: Ações de Coleta e Ações de Busca (BRASIL, 2014).

Além disso, é importante conceituar ações de coleta e ações de busca, para melhor entender sobre o assunto desenvolvido. Por ações de coleta entende-se como:

São todos os procedimentos realizados por uma AI, ostensiva ou sigilosamente, a fim de obter dados depositados em fontes disponíveis, sejam elas oriundas de indivíduos, órgãos públicos ou privados.

a) Coleta Primária: envolve o desenvolvimento de ações de ISP para obtenção de dados e/ou conhecimentos disponíveis.

b) Coleta Secundária: envolve o desenvolvimento de ações de ISP, por meio de acesso autorizado, por se tratar de consulta a bancos de dados protegidos (BRASIL, 2014).

Em relação às ações de busca, discorre-se como sendo:

> [...] todos os procedimentos realizados pelo Elemento de Operações (ELO) de uma AI, envolvendo ambos os ramos da ISP, a fim de reunir dados protegidos e/ou negados em um universo antagônico. Os procedimentos de Ações de Busca são: reconhecimento, vigilância, recrutamento operacional, infiltração, desinformação, provocação, entrevista, entrada, ação controlada e interceptação de sinais (BRASIL, 2014).

Especificamente em relação às ações de busca que, conforme a DNISP, descreve enquanto procedimentos de ações de busca, temos no seu escopo um rol de ações que interessam à atividade de ISP.

Interessante notar que, em coleta a vários trabalhos acadêmicos atinentes à atividade de ISP, podemos encontrar este rol de ações de busca. Neste sentido, para Silva (2019):

> A concreção da Atividade de Inteligência no campo operacional dar-se-á pelo emprego de técnicas operacionais. Para Oliveira (2010. p. 66), "técnicas operacionais são métodos utilizados para a obtenção de conhecimento utilizável, negado ou não, através das operações de inteligência"

Neste diapasão, quando descreve sobre ações de inteligência, importante mencionar, em linhas gerais, acerca das Operações de Inteligência de Segurança Pública e, assim, retomar aos aspectos conceituais de ações de busca e técnicas operacionais de ISP. Operações de Inteligência de Segurança Pública possuem o seguinte conceito:

É o exercício de uma ou mais Ações e Técnicas Operacionais, executadas para obtenção de dados negados de difícil acesso e/ou para neutralizar ações adversas que exigem, pelas dificuldades e/ou riscos iminentes, um planejamento minucioso, um esforço concentrado, e o emprego de pessoal, técnicas e material especializados (BRASIL, 2014).

Por oportuno, os trabalhos realizados no âmbito das Operações de Inteligência de Segurança Pública vinculam-se à obtenção de dados, provenientes, segundo a sua confidencialidade, de fontes abertas, por meio de coleta, ou de fontes classificadas (dado negado), quando se realizam as buscas.

Nestes termos, deve ser acionado o Agente de Inteligência, por intermédio do Elemento de Operações, para fins de obtenção dos dados negados ou não disponíveis o que corrobora, oportunamente, no desenvolvimento das operações de inteligência.

Vale acrescentar também, conforme menciona Pacheco (2006), que as operações de inteligência são "ações realizadas com a finalidade de obter dados não disponíveis em fontes abertas. Elas podem ter por alvo pessoas, locais, objetos ou canais de comunicação" e são implementadas com a utilização de técnicas operacionais (LIMA, 2011).

Gonçalves (2009, p. 63) também leciona sobre as operações de inteligência, que correspondem ao "conjunto de ações técnicas destinadas à busca do dado negado". Ao ampliar esse entendimento, Gonçalves (2009, p. 54) assinala que nenhum órgão de inteligência, que produz conhecimentos, pode deixar de utilizar dados negados obtidos do setor de operações, mesmo que de outro órgão (LIMA, 2011).

Para Almeida Neto (2009, p. 58-59 *apud* LIMA, 2011), operações de inteligência referem-se ao "conjunto de ações planejadas, com o emprego de técnicas operacionais e meios especializados para a realização da busca". Acrescenta, ainda, de um recurso auxiliar da inteligência, em sentido estrito, e da Contrainteligência, para a obtenção de dados negados ou indisponíveis, bem como para neutralizar ações adversas, em determinadas situações.

Na seara da legislação brasileira, destaca-se a Lei nº 9 883/99:

> Art. 3º [...]
>
> Parágrafo único: As atividades de inteligência serão desenvolvidas, no que se refere aos limites de sua extensão e ao uso de técnicas e meios sigilosos, com irrestrita observância dos direitos e garantias individuais, fidelidade às instituições e aos princípios éticos que regem os interesses e a segurança do Estado (BRASIL, 1999).

Lima (2011) descrevendo sobre as Operações de Inteligência também aborda:

> Logo, operações de inteligência podem ser compreendidas como o somatório de ações devidamente planejadas, concatenadas e suplementadas com a aplicação de técnicas próprias e meios especializados, para assegurar, além da neutralização de ações adversas, a execução sigilosa de buscas, inclusive coletas, dentro de um propósito definido, com vistas à obtenção de dados negados ou não-disponíveis. Acrescente-se, como não poderia deixar de ser considerado, com fiel observância aos direitos e garantias individuais.

Dentro do que foi exposto, é muito pertinente à observação de Gonçalves (2009, p. 63) ao considerar as operações de inteligência como a parte mais "polêmica" afeta atividade de inteligência, uma vez que seus "métodos envolvem, necessariamente, técnicas e ações sigilosas". É de se considerar que as operações de inteligência é o momento do elemento de operações, lotado no setor de operações do órgão de inteligência, lançar-se no ambiente operacional – no local onde se desenvolve a operação de inteligência, segundo a Senasp (2007, p. 30) – para realizar as buscas, as quais se constituem em diligências necessárias à obtenção do dado negado ou não disponível e, às vezes, conforme salienta Cepik (2003, p. 28), sem o "consentimento, a cooperação ou mesmo o conhecimento por parte dos alvos da ação".

Diante do exposto, realizada uma breve síntese das Operações de Inteligência, importante mencionar sobre as ações de busca e as técnicas operacionais de ISP. Para melhor compreensão do presente artigo, utilizar-se-ão as classificações extraídas de Brasil (2014), referentes às ações de buscas e técnicas operacionais. O QUADRO 1 apresenta o rol das ações de buscas aplicáveis às operações de inteligência.

QUADRO 1: AÇÕES DE BUSCAS APLICÁVEIS ÀS OPERAÇÕES DE INTELIGÊNCIA.

AÇÕES DE BUSCA	DESCRIÇÃO
Reconhecimento	Granjear dados sobre quaisquer coisas disponíveis, como ambiente, objetos e pessoas. Subsidia preliminarmente os preparativos de uma operação de inteligência.
Vigilância	Manter um ou mais alvos em contínua observação, sem que o elemento de operações seja percebido. Os alvos podem ser uma pessoa, um objeto, um veículo, ou seja, tudo aquilo que se deseja manter sob constante vigilância.
Recrutamento Operacional	Angariar uma pessoa e persuadi-la a colaborar com o órgão de inteligência, seja para trabalhar no próprio órgão, seja para o fornecimento de informações necessárias aos trabalhos de Inteligência.
Infiltração	Consiste em colocar uma determinada pessoa próxima ao alvo, com o intuito de buscar informações de interesse do órgão de inteligência. É sigilosa e necessita de autorização judicial.
Desinformação	Confundir, intencionalmente, alvos, a fim de instigá-los a cometer erros de apreciação, levando-os a executar determinado comportamento pré-determinado. Muito utilizada na contrainteligência.

Provocação	Com alto nível de especialização, consiste em fazer com que uma pessoa/alvo altere as rotinas de suas atividades e passe a executar algo desejado pelo órgão de inteligência, sem que o alvo desconfie da ação.
Entrevista	Implementada para obtenção de dados por meio de conversação, com propósitos definidos, planejada e controlada pelo entrevistador, que capta a realidade de um fato pela visão do entrevistado.
Entrada	Realizada para obter dados em locais onde o acesso é restrito e sem que seus responsáveis tenham conhecimento da ação realizada. É sigilosa e necessita de autorização judicial.
Interceptação de sinais e dados	Desenvolvida com o uso de mecanismos elétricos/eletrônico, tendo como operadores os próprios elementos de operações. É sigilosa e necessita de autorização judicial.

Fonte: Adaptado de Brasil, 2014.

Em relação às técnicas operacionais, refere-se "às habilidades desenvolvidas por meio de emprego de técnicas especializadas que viabilizam a execução das ações de buscas, maximizando potencialidades, possibilidades e operacionalidades". O QUADRO 2 sintetiza as técnicas operacionais utilizadas nas operações de inteligência.

QUADRO 2: TÉCNICAS OPERACIONAIS APLICÁVEIS ÀS OPERAÇÕES DE INTELIGÊNCIA.

AÇÕES DE BUSCA	DESCRIÇÃO
Processo de identificação de pessoas	Identificar ou reconhecer pessoas por meio de suas principais características. Utiliza-se DNA, retrato falado, fotometria.
Observação, Memorização e Descrição	Observar, memorizar e descrever corretamente os alvos, de modo a transmitir dados e informações úteis para a identificação.
Estória-cobertura	Dissimular para encobrir reais identidades, para facilitar a obtenção do dado, com a preservação da segurança e sigilo.
Disfarce	Modificar aparência física, com o uso de recursos naturais ou artificiais, a fim de evitar ser reconhecido e adequar-se a uma estória-cobertura.
Comunicações sigilosas	Empregar formas e processos especiais convencionados para transmissão de mensagens, ou passar objetos, durante uma operação de inteligência.
Leitura de fala	Identificar padrões de fala numa conversação para compreensão dos assuntos tratados.

Análise de veracidade	Verificar se uma determinada pessoa está dizendo a verdade sobre situações ou fatos, com emprego de metodologia e recursos tecnológicos.
Emprego de meios eletrônicos	Capacitar elemento de operações na utilização adequada dos equipamentos de captação, gravação e reprodução de sinais, imagens e dados.
Fotointerpretação	Identificar os significados das imagens obtidas.

Fonte: Adaptado de Brasil, 2014.

Ainda segundo Lima (2011), vale acrescentar:

> No tocante ao desenvolvimento das operações de inteligência, o emprego das ações de buscas e das técnicas operacionais é conjugado, sendo que aquelas se referem aos procedimentos a serem implementados e estas dizem respeito ao modo de atuação para viabilizar a execução das referidas ações.

Em síntese, se o escopo da inteligência é produzir conhecimentos por intermédio da obtenção e análise dos dados, estejam eles em fontes abertas ou classificadas, bem como adotar medidas de salvaguarda, a relevância da atividade está centrada na habilidade operativa do elemento de operações ao desenvolver as ações de buscas e aplicar as técnicas operacionais, e, também, na capacidade dos analistas para elaboração de conhecimentos que atendam às demandas do usuário.

Apesar deste diálogo acerca as ações de busca e técnicas operacionais de ISP, interessa para o presente artigo o que se fala em relação à ação de busca Entrevista e a técnica operacional de ISP - Análise de Veracidade.

Conforme supramencionado, a Ação de Busca Entrevista é a "obtenção de dados por meio de uma conversação, mantida com propósitos definidos". A Entrevista, como Ação de Busca, é a principal fonte de dados para utilização da Técnica de Análise de Veracidade. A primeira possibilita a interação entre o Agente e o Alvo, criando um canal de comunicação verbal e não verbal. A segunda irá auxiliar o Agente a destilar a verdade da mentira, por meio de indicadores, que isoladamente não são precisos, porém em conjunto, aliados ao contexto da entrevista, levando-se em variáveis diversas irão dar um norte sobre se o que está sendo dito é verdade ou não.

A entrevista, em síntese, requer um estudo mais aprofundado. Entretanto, vale mencionar alguns aspectos mencionados por Cardoso Júnior (2005):

Acredita-se que as principais fases de uma entrevista devam corresponder ao seguinte dimensionamento: aproximação, reforço aos pontos fortes, cerco ao objetivo e finalização:

> - Para a aproximação, o entrevistador deverá granjear a confiança do entrevistado, provocando associações agradáveis e procurando deixá-lo à vontade, o que faz com que projete nele uma boa imagem. Em muitos casos, o entrevistador deve ajudar o sujeito a falar, conduzindo o fluxo de conversação à maneira do próprio sujeito. Nesse ínterim, poderá identificar com facilidade as suas carências emocionais;
>
> - Na fase do reforço aos pontos fortes, o entrevistador deverá falar sobre o que o entrevistado gosta, aceitando a imagem que ele "vende". Precisará reforçar as suas vaidades e atuar sobre as necessidades e carências que já identificou (durante a aproximação), lançando os estímulos que o sujeito deseja. Terá então que compartilhar dos seus interesses, enfatizando os valores por ele cultivados e fazendo-o sentir-se bem por expor as suas ideias ou por explicar determinado assunto;
>
> - Durante a fase do cerco ao objetivo, o entrevistador deverá garantir o controle da entrevista, mantendo a iniciativa e conduzindo a troca de ideias na direção do objetivo planejado. Precisará comunicar-se usando o corpo (toque no lugar na hora certa, olhar interessado, manutenção da distância aceitável, posicionamento corporal compatível etc) e atentar para a necessidade de segurança do sujeito. Deve ser compreendido que o sujeito só vai atender às demandas do entrevistador se e quando tiver certeza de que isso não vai, de alguma forma, prejudicá-lo. O entrevistador procurará entender as respostas, buscando caminhos satisfatórios para novas perguntas, separando fatos de opiniões, e não tirar conclusões precipitadas da entrevista baseando-se em conhecimentos anteriores. Haja o que houver, ele não deverá jamais hostilizar o entrevistado, mesmo quando atacado por ele; e
>
> - Para a finalização, o entrevistador deverá fazer o desligamento de forma progressiva, esfriando a conversação com o cuidado de não permitir a perda da ligação emocional. Ele poderá criar as condições para realização de futuros contatos e não deverá permitir (sob hipótese alguma) que o entrevistado saia com a sensação de perda, de que foi usado. A entrevista deverá ser concluída com palavras de encorajamento (CARDOSO JÚNIOR, 2005, p. 99-100).

Já a Análise de Veracidade como Técnica Operacional de Inteligência, visa dar a capacidade ao Agente de Inteligência de analisar os dados negados que estão na memória de uma pessoa e conseguir separar através de metodologia própria o que é tido como verdade para aquela pessoa do que não é.

Dessa forma, para tal é importante que seja feita uma Entrevista com a pessoa alvo que possui os dados negados. Enquanto esta entrevista é realizada, naquele momento busca-se utilizar da Técnica de Análise de Veracidade para buscar a verdade por trás das palavras do entrevistado.

3 APLICABILIDADE DA ANÁLISE DE VERACIDADE NA INTELIGÊNCIA DE SEGURANÇA PÚBLICA

A Análise de Veracidade, enquanto técnica operacional de inteligência no âmbito da ISP, possui vasta aplicabilidade, uma vez que em várias missões o Agente de Inteligência irá necessitar de

conversar com alguma pessoa, ainda que não tenha a intenção de entrevista-la propriamente, mas apenas pedir alguma informação ou ganhar acesso a algum lugar. Dessa forma, saber quando a pessoa está tentando ocultar a verdade é uma ferramenta e tanto nas mãos do Agente de Inteligência.

Levando a utilização da Técnica de Análise de Veracidade para um patamar mais elevado, observa-se sua importância para as Operações de Inteligência, que visa evitar algum crime grave ou o desenvolvimento de alguma quadrilha do crime organizado uma entrevista bem sucedida, onde se consegue separar a verdade de afirmações falsas, conseguindo mais dados concretos para uma Operação de Inteligência ou diligência futura.

Segundo Oliveira (2015), a busca pela autoria de um crime essencialmente possuirá entrevistas ou interrogatórios, com pessoas de diferentes envolvimentos, tais como vítimas, testemunhas, autores, suspeitos, ou informantes, a comunicação pode ser de forma verbal ou não verbal, emocional ou não emocional, auxiliando o responsável pela entrevista a descobrir pormenores que estariam ocultos de certa forma.

Oliveira (2015) ainda relata que comportamentos verbais e não verbais são aspectos sintomáticos acerca da sinceridade do entrevistado, seja ele suspeito, testemunha ou vítima, e as diferenças no comportamento do indivíduo são características de inocência ou mentira. Descreve ainda que um indivíduo que tenha cometido crime escolhe de forma consciente resistir às perguntas do entrevistador voltadas a alcançar a realidade acerca dos fatos que tangenciam a entrevista, dessa forma o indivíduo entrevistado mantem uma estrutura de mentiras verbais que são contraditas por tensões e conflitos internos que se evidenciam no comportamento não verbal. Este comportamento não verbal é percebido por meio dos movimentos corporais, expressões faciais, a forma como o contato visual é realizado, atitudes e posturas também tem possibilidade de indicar a veracidade ou não no relato de uma pessoa.

Seguindo o raciocínio, o autor do artigo aponta que o comportamento não verbal pode ser mais importante que o verbal, destacando que o comportamento não verbal é responsável por mais da metade de toda a comunicação. Com essa informação, salienta que o suporte que o comportamento não verbal dará, confirmará a credibilidade de uma resposta, ou trará destaque para o desconforto nas atitudes e gestos indicando uma possível fraude e a necessidade de continuar perguntando. O comportamento do

entrevistador pode influenciar no comportamento do suspeito. Por fim, quanto mais inquieto o suspeito, mais revelador se torna seu comportamento.

Oliveira (2015), na continuação de seu raciocínio, cita o "Sistema de Codificação de Ação Facial", desenvolvido por Paul Ekman, o qual ensina como fazer o reconhecimento e marcar as Unidades de Ação, as quais representam a atividade muscular que por sua vez produzem modificações momentâneas na aparência facial da pessoa observada. Entre uma pessoa e outra a variação da aparência pode acontecer de formas diferentes, dependendo das características físicas, tais como estrutura óssea da face, as variações existentes na musculatura facial, a forma como a gordura é distribuída, as dobras existentes na pele etc. As sensações que cada emoção gera no corpo humano são padronizadas de forma única. Com a familiarização destas, pode-se ficar ciente, desde quando surgem, da resposta emocional, dessa forma há a possibilidade de ter alguma chance de escolha se deve conservar a emoção ou se é necessário efetuar uma interferência na forma como esta aparece.

O autor explana que a cada emoção representa sinais bem particulares, principalmente na fisionomia e na voz. Por isto, torna-se importante saber identificar as sete emoções universais, quais sejam: surpresa, felicidade, tristeza, raiva, medo, desprezo e nojo.

Para Fexeus (2015), os sinais que o indivíduo está mentindo são facilmente detectáveis. Se é possível detectar algum tipo de desarmonia no que é expresso, é possível pensar que há duas mensagens diferentes sendo enviadas pelo indivíduo. O autor diz que é importante procurar por sinais contraditórios, indícios inconscientes que repassam informação destoante da que está sendo emitida verbalmente. Os verdadeiros sentimentos e pensamentos são expressos de maneira difícil de controlar por meio dos sinais não verbais.

Ainda segundo Fexeus (2015), quando alguém mente ou tenta esconder os próprios pensamentos e sentimentos, haverá um "vazamento" em inúmeras áreas diferentes, porém alerta que há algumas pessoas que não exibem nenhuma espécie de "vazamentos" ao mentirem, logo deve-se ficar atento. Não deve ser interpretada a ausência de vazamentos como garantia de que a pessoa está falando a verdade. Outro ponto importante que o autor cita é que é importante tomar cuidado com os falsos positivos, uma pessoa pode parecer estar "vazando", mas pode estar falando a verdade. Nesses casos o autor ensina que deve-se prestar atenção em vários tipos de sinais diferentes antes de formar uma convicção sobre o comportamento de uma pessoa estar falando a verdade ou não.

Acrescendo do pensamento sobre o assunto, Fexeus (2015) chama a atenção para que além de prestar atenção em todos os sinais contraditórios seja observado também o contexto no qual a pessoa e a entrevista acontece, uma vez que os sinais podem estar sendo motivados por alguma situação que acabou de acontecer ou que a pessoa está pensando naquele momento, fatores diversos ao que o entrevistador acredita se tratar. Dessa forma, o contexto é mais um fator a ser analisado para saber se está influenciando no comportamento natural da pessoa.

Dentre os tipos de sinais e comportamentos, Fexeus (2015) elenca alguns: sinais contraditórios na linguagem corporal, sinais visíveis no rosto, qualificação (quando uma emoção facial é substituída por outra, modulação (quando a intensidade da expressão é alterada de propósito para enfraquece-la ou fortalece-la), falsificação (que se divide em simulação [quando uma emoção é exibida não se está sentindo nada], neutralização [quando o indivíduo tenta não revelar nada, porém sente alguma emoção] e mascaramento [quando tenta-se encobrir a emoção que se está sentindo com outra emoção]. O autor relata que a máscara mais utilizada pelas pessoas para ocultar as emoções é o sorriso. Outro ponto importante indicado pelo autor são as microexpressões faciais, contudo pela rapidez com que ocorrem são mais difíceis de detectar e exigem treinamento e prática para se conseguir fazer a leitura. Dentre outros pontos a se observar o autor cita as mãos, todo o resto do corpo, atos falhos gestuais (quando são realizadas pequenas ações sem sentido, devido ao nervosismo da pessoa, como abrir e fechar uma caneta, rasgar papéis em pedacinhos etc.), mudanças na voz, tom da voz, mudanças na fala, mudanças na linguagem, digressões e excentricidades (divagações em afirmações, que não levam a lugar nenhum ou dão muitas voltas em um assunto), repetição das mentiras, cortina de fumaça (uso de falácias e abstrações para confundir o ouvinte), criar distâncias usando-se de negações, criar distância com despersonalização (palavras que envolvam mais pessoas ou respostas vagas em algum sentido, como nunca, sempre, todo mundo, ninguém etc.), expressando reservas quando conta algo [“você pode até não acreditar, mas...”], sofisticação linguística. Enfim estas são as formas como o autor referencia como sinais que o indivíduo pode executar quando tenta mentir ou esconder algo.

Pease e Pease (2005) citam os oito gestos mais comuns associados à mentira, sendo: tapar a boca (o cérebro inconscientemente quer reprimir as palavras enganosas), tocar o nariz (pode ser um toque rápido ou algumas esfregadelas, o autor cita um estudo onde os cientistas comprovaram aumento da pressão arterial nos vasos sanguíneos do nariz quando uma mentira é contada, ocasionando formigamento e leve coceira), coceira no nariz (a pessoa sente a necessidade não só de tocar, mas de

coçar o nariz), esfregar os olhos (segundo o autor é o cérebro tentando bloquear coisas enganosas, duvidosas ou desagradáveis que a pessoa vê ou evitar olhar para o rosto da pessoa para quem se está mentindo), pegar na orelha (seria uma versão adulta do gesto que crianças fazem de tapar os ouvidos quando não querem ouvir algo, então se a pessoa escuta algo e responde pegando na orelha pode ser um indicador que ela está dizendo algo que ela mesmo não concorda, gestos variantes seriam coçar atrás da orelha, mover a ponta do dedo para dentro e para fora da orelha, ficar puxando o lóbulo e dobra a orelha para a frente de maneira a encobrir o duto auditivo), coçar o pescoço (normalmente coça-se com o dedo indicador a parte do pescoço que fica abaixo do lóbulo da orelha, indica normalmente contradição nas próprias palavras), afrouxar o colarinho (devido ao aumento da pressão causado pela mentira a pessoa costuma suar na região do pescoço, logo ela afrouxa o colarinho procurando ar fresco, se resfriar, se acalmar), dedo na boca (gesto evoluído do bebê quando quer a segurança da mãe, o adulto além de levar a mão e dedos à boca, pode procurar outros objetos, como cachimbos, cigarros, canetas, entre outros objetos).

Na FIG. 1 verifica-se um homem tocando ou coçando o nariz, normalmente devido à irrigação sanguínea aumentar na região do nariz um leve formigamento pode levar a pessoa a tocar ou coçar o nariz quando não concordar com o que é dito. E à direita vemos o homem coçando os olhos, demonstrando que quer fechar os olhos, não quer ver a pessoa para a qual se está mentindo.

FIGURA 1 – HOMEM TOCANDO/COÇANDO O NARIZ E HOMEM TOCANDO O OLHO.

Fonte: Pease e Pease (2005).

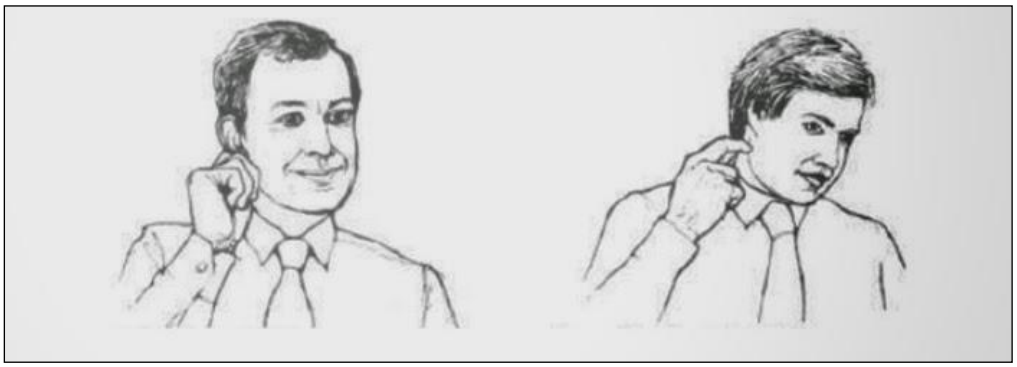
Na FIG. 2 verifica-se um homem procurando aliviar a pressão e o calor provocados pelo desconforto causado pela mentira, a qual eleva sua pressão sanguínea e provoca até mesmo sudorese.

FIGURA 2 – HOMEM AFROUXANDO O COLARINHO.

Fonte: Pease e Pease (2005).

Na FIG. 3 percebe-se um homem tocando o lóbulo da orelha, como se não quisesse ouvir o que está sendo dito e outro coçando o pescoço, devido ao desconforto causado pela mentira, sinais indicativos que não se concorda com o que está sendo dito.

FIGURA 3 – HOMEM TOCANDO O LÓBULO DA ORELHA E HOMEM COÇANDO O PESCOÇO.



Fonte: Pease e Pease (2005).

Na FIG. 4 verifica-se um homem tapando a boca com a mão, demonstrando que seu cérebro deseja reprimir aquelas palavras que estão sendo ditas por não concordar com aquilo.

FIGURA 4 – HOMEM TAPANDO A BOCA.

Fonte: Pease e Pease (2005).

Percebe-se dessa forma que a Técnica de Análise de Veracidade é uma técnica complexa e que exige treinamento e prática por parte dos Agentes de Inteligência que irão utilizar dela em suas missões, haja vista que são muitas variáveis que devem ser observadas, analisadas e confrontadas com o contexto no qual o entrevistado e entrevistador se inserem para que não haja a existência de falsos positivos ou falsos negativos em relação ao que o indivíduo entrevistado diz e seja possível alcançar a verdade nos fatos que são ditos.

CONSIDERAÇÕES FINAIS

Verifica-se a importância da utilização da Técnica de Análise de Veracidade nas Ações e Operações de Inteligência, uma vez que a informação por si só, sem que seja de alguma forma checada com relação à sua veracidade pode por toda uma Operação a perder.

Tendo em vista a forma rotineira como ocorrem os contatos verbais e não verbais dos Agentes de Inteligência com toda sorte de pessoas nas mais variadas situações (testemunhas, vítimas, suspeitos, entre outras) percebe-se que o desenvolvimento da habilidade em discernir o que é verdade do que está sendo relatado, assim como descobrir o que está sendo encoberto por mentiras, é extremamente relevante para o serviço operacional de inteligência, uma vez que a confirmação ou não de um dado por meio desta técnica pode dar rumo totalmente diferente à sequência de ações de uma Operação de Inteligência.

Evidente também que a Inteligência de Segurança Pública prescinde de ações especializadas, visando à identificação, o acompanhamento e a avaliação de ameaças reais ou potenciais, sempre orientadas para a produção e salvaguarda de conhecimentos necessários à decisão, seja no planejamento e à execução de uma política de segurança pública, ou até mesmo no nível operacional, como é o caso focado do presente artigo. Somente assim, terá condições de: prever, prevenir e reprimir atos criminosos com maior eficiência, tendo como base técnica especializada a utilização a Análise de Veracidade, a qual deve ser do conhecimento do profissional de ISP, especialmente o Agente de Inteligência.

Diante disto, destaca-se a relevância em investir em treinamento nesta área de conhecimento, principalmente para os Agentes de Inteligência que trabalham em campo, coletando o dado negado. Como campos vinculados, cita-se como exemplo as áreas de investigação, interrogatório, entrevista, programação neurolinguística.

REFERÊNCIAS

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF. Presidência da República, [2018]. Disponível em: <*http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm/*>. Acesso em 03/10/2019.

BRASIL. **Doutrina Nacional de Inteligência de Segurança Pública (DNISP)**. Coordenação-Geral de Inteligência. Secretaria Nacional de Segurança Pública - Ministério da Justiça. 2014.

CARDOSO JÚNIOR, Walter Félix. **Inteligência Empresarial Estratégica**. Tubarão. Ed. Unisul. 2005.

CEPIK, Marco A. C. **Espionagem e Democracia**. FGV. Rio de Janeiro. 2003.

FEXEUS, Henrik. **A Arte de Ler Mentes: Como Interpretar Gestos e Influenciar Pessoas Sem Que Elas Percebam**. Petrópolis, RJ. Vozes. 2013.

GONÇALVES, Joanisval Brito. **Atividade de Inteligência e Legislação Correlata**. Ed Impetus. Niterói. 2009.

LIMA, Rinaldo de Azevedo. **A Execução de Despesas de Caráter Sigiloso no Âmbito do Sistema de Inteligência da Polícia Militar de Minas Gerais. Belo Horizonte**. Monografia (Especialização em Segurança Pública). Academia de Polícia Militar de Minas Gerais. Fundação João Pinheiro. 2010.

BRASIL. **Doutrina Nacional de Inteligência e Segurança Pública.** Ministério da Justiça. Secretaria Nacional de Segurança Pública. Brasília. 2009.

OLIVEIRA, Wellington de. **Aplicando Técnicas de Entrevista e Interrogatório na Investigação-Método REID**. 2015. Disponível em: <*https://www.pc.ms.gov.br/artigos/aplicando-tecnicas-de-entrevista-e-interrogatorio-na-investigacao-metodo-reid/*>. Acesso em: 05/10/2019.

PACHECO, Denilson Feitoza. **Direito Processual Penal: Teoria, Crítica e Práxis**. 4ª ed. rev. e aum. Editora Impetus. Niterói. 2006.

PEASE, Allan; PEASE, Barbara. **Desvendando os Segredos da Linguagem Corporal**. Tradução Pedro Jorgensen Junior. Ed Sextante Rio de Janeiro. 2005.

PINTO, Maurício Viegas. **Análise de Veracidade: Diferentes Abordagens Doutrinárias no Âmbito da Inteligência de Segurança Pública**. Instituto Brasileiro de Análise de Veracidade. Disponível em <*https://www.ibrav.org.br/artigoanalisedeveracidade*>. Acesso em: 13/07/2020.

SILVA, Pedro Henrique de Aquino. **Atipicidade da Conduta do Agente de Inteligência da Polícia Militar Frente ao Crime de Usurpação de Função Pública**. In.: [Orgs.].

HAMADA, Hélio Hiroshi; MOREIRA, Renato Pires. **Teoria e Práticas de Inteligência de Segurança Pública**. Belo Horizonte: Editora D'Plácido, Série Inteligência, Estratégia e Defesa Social. 2019.

DADOS DOS AUTORES:

Renato Pires Moreira

Mestrando em Gestão & Organização do Conhecimento pela Escola de Ciência da Informação da Universidade Federal de Minas Gerais. Especialista em Inteligência de Estado e Inteligência de Segurança Pública pela Fundação Escola Superior do Ministério Público de Minas Gerais. Assistente de pesquisa voluntário da Linha de Pesquisa "Cenários Prospectivos para Defesa e Segurança - Metodologias, Tendências e Práticas", que compõe o grupo Design de Jogos, Processo Decisório e Cenários Prospectivos do Laboratório de Simulações e Cenários, Escola de Guerra Naval. Pesquisador no Núcleo de Pesquisas em Ciências Policiais e Segurança Pública atuando na linha de pesquisa Gestão Estratégica, Inteligência de Segurança Pública e Tecnologias Inovadoras. Currículo Lattes: http://lattes.cnpq.br/2355715189859936

Imer Alves de Brito Júnior

Bacharel em Ciências Militares com Ênfase em Defesa Social pela Academia de Polícia Militar de Minas Gerais, 2011. Curso de Inteligência Policial pelo Centro de Treinamento de Inteligência da Polícia Militar do Distrito Federal (2016). Especialista em Inteligência de Segurança Pública pelo Centro de Pós-Graduação da Academia de Polícia Militar de Minas Gerais (2019). Atuou como Professor na Escola de Inteligência da Polícia Militar (2016-2019). Graduando em Engenharia de Software pela Universidade Estácio de Sá (2020-2021).

Currículo Lattes: http://lattes.cnpq.br/7969857452274816

tenalves190@gmail.com

RISP
Revista de Inteligência de Segurança Pública
ISSN 2675-7168; 2675-7249

RELAÇÃO ENTRE FACÇÕES CRIMINOSAS E CRIMES CIBERNÉTICOS

Eliezer de Souza Batista Junior
Henrique de Queiroz Henriques
Rober Yamashita

RESUMO: O texto intitulado de relação entre facções criminosas e crimes cibernéticos almeja analisar a relação entre esses grupos marginalizados com as novas técnicas de crimes adotadas no ciberespaço no Brasil e a partir do ano de 2012. Para tanto, o artigo foi dividido em três partes principais. A primeira trata de conceitos básicos, provendo o leitor da visão de mundo dos autores. O segundo aborda sobre a classificação dos autores. O terceiro apresenta os crimes cibernéticos realizados por organizações criminosas no Brasil desde 2012. Para tanto, foram adotados os métodos qualitativo, dedutivo e com realidade aparente, sob o prisma da epistemologia do positivismo. Para tanto, as pesquisas foram baseadas em revisão documental, no qual se priorizaram artigos acadêmicos, livros, periódicos especializados e sites noticiários, nessa ordem. Os dados apontam que o crime organizado já começou a se utilizar de ferramentas digitais, mas que não chegou ao seu ápice. Há vários aspectos que necessitam de melhoria no cenário brasileiro, como legislação, prioridade e protocolos de segurança.

Palavras-Chave: Crimes Cibernéticos, Facções Criminosas e Crime Organizado no Brasil.

ABSTRACT: This paper entitled the relationship between criminal factions and cybercrime aims to analyze the relationship between these groups with the new crime techniques adopted in cyberspace in Brazil and from the year 2012. For this purpose, the article was divided into three main parts. The first deals with basic concepts, providing the reader with the authors' worldview. The second part reveals the cyber concepts classification considered by the authors. The third presents cybercrimes carried out by criminal organizations in Brazil since 2012. For this purpose, qualitative, deductive and apparent reality methods were adopted, under the prism of the epistemology of positivism. Therefore, the research literature were based on academic papers, books, specialized periodicals and news sites were prioritized, in that order. The data show that organized crime has already started using digital tools, but that it has not reached its peak. There are several aspects that need improvement in the Brazilian scenario, such as legislation, priority and safety protocols.

Keywords: Cyber Crimes, Criminal Factions and Brazil.

INTRODUÇÃO.

O tema segurança pública é um assunto que modifica através dos tempos, especialmente considerando as mudanças sociais e políticas. Nos anos 60, a segurança e até mesmo a defesa estavam focadas no plano físico. Com a invenção da ARPANET e sua extensão do tipo *spin-off* para a sociedade

civil, um novo espaço foi criado: o virtual (COHEN-ALMAGOR, 2011, pp. 46-56). Esse espaço, tido como "livre" foi aproveitado por vários profissionais de forma a automatizar e coletar dados, bem como, melhorar a performance de *business* em rede.

Da mesma forma que pessoas que atuam na legalidade souberam usufruir dos benefícios desse novo domínio, outras que atuam na ilegalidade também se utilizaram dessa nova possibilidade. Conforme preconiza Morgenthau (2003), "não há vácuo de poder", de forma que criminosos conseguiram aproveitar os buracos deixados pela liberdade na Internet.

O espaço cibernético foi utilizado emulando crimes normais do espaço físico. Dessa forma, houve apenas uma adaptação do que é realizado na realidade à vida virtual. Vários grupos se tornaram especializados nesses tipos de crimes, em que há destaque para os grupos *hackers*. Entretanto, em vários países, há uma preocupação grande em relação às facções criminosas que chegam a impor barreiras à soberania estatal em alguns países. No Brasil, a maioria dos acadêmicos não acreditam em tal situação atualmente, mas concordam que é um problema que deve ser combatido a fim de evitar a sua proliferação em áreas que possam atentar contra o bem-estar da sociedade brasileira como um todo.

As leis no Brasil são muito recentes, em termos cibernéticos (MARQUES, 2018). Boa parte dos juristas defendem que os protocolos estabelecidos no código penal já servem para abarcar os crimes cibernéticos. O exemplo de países mundo afora mostra que há necessidade de leis específicas e, nesse sentido, desde 2012 com a lei "Carolina Dieckmann", os crimes cibernéticos começaram a ficar mais detalhados.

O problema que este artigo tentará responder é: "qual a relação das facções criminosas com a utilização do espaço cibernético para cometer crimes dessa natureza no Brasil após o ano de 2012?". Dessa forma, o objetivo a ser alcançado é o de analisar as ações de crimes cibernéticos cometidos por facções criminosas brasileiras a partir do ano de 2012.

Utilizar-se-á a metodologia qualitativa, utilizando-se fontes bibliográficas acadêmicas, livros, periódicos especializados e sites, nessa prioridade. Também usará a dedução, pois o referido artigo não se propõe a propor novas teorias. A realidade aparente será utilizada porque não há possibilidades de se saber todos os dados referentes a ataques cibernéticos. Dessa forma, os bancos de dados utilizados serão considerados como verídicos.

1 DESENVOLVIMENTO.

Este capítulo estará dividido em 3 (três) seções: histórico e definições básicas, atores envolvidos e crimes cibernéticos cometidos por facções criminosas brasileiras.

1.1 Histórico e definições básicas.

A *Internet* modificou o comportamento da sociedade mundial, de forma que cada vez mais as pessoas se tornam dependente desse tipo de tecnologia (CASTELLS, 2002). A pandemia ocasionada pelo vírus Sars-Cov-2 aumentou tal dependência, pois havia a necessidade de realizar e manter o isolamento social por conta do alto índice de transmissão (OLIVEIRA, 2020). Alguns autores defendem que a sociedade não vive mais na Era Contemporânea, mas na Era da Informação (ALMEIDA, 2007).

A cibernética é um termo originário da palavra grega *kubernétikê* que pode ser traduzida como "a arte de pilotar". Em 1948, Wiener se utilizou dessa palavra para dar um outro sentido: o de controle e de comunicação entre animais, homens e máquinas, visando o desenvolvimento do campo militar (WIENER, 1998). Esse conceito foi estendido para a sociedade em tempos mais tarde (KIM, 2004).

Durante a guerra fria, com a preocupação de tornar as comunicações resilientes a ataques nucleares vindos da ex-URSS, o EUA desenvolveu uma rede com três nós que intercambiavam informações. Essa rede (chamada de ARPANET) foi aumentando até abarcar todo o território americano. Após verificar que o conceito poderia ser utilizado pela sociedade civil, houve o transbordamento e aumento a nível mundial, criando-se o que se conhece como Internet ou rede mundial de computadores.

O espaço ocupado por essa estrutura é denominado ciberespaço ou espaço cibernético e pode ser conceituado como "domínio global no ambiente informacional do qual a característica única e distintiva é enquadrada pelo uso do espectro eletrônico e eletromagnético para criar, armazenar, trocar e explorar informações via redes interdependentes e interconectadas usando tecnologias de informação e comunicação" (KUEHL, 2009).

As principais características da Internet são: (1) domínio global, no qual as fronteiras são colocadas em segundo plano; (2) distintiva e única, pois fenômenos ocorrem no espaço eletrônico e eletromagnético, podendo trazer efeitos no físico; (3) conectividade, interconectando estruturas

existentes (KUEBL, 2017); (4) reúne ambiente físico (infraestruturas e computadores) e lógico (configurações de redes) (RATTRAY, 2001); e (5) possibilidade de anonimização (KALLBERG & COOK, 2017).

Na rede mundial de computadores há diversas ações cibernéticas que podem ser classificados em três formas: ataque, crime e guerra cibernética. O ataque cibernético é um ataque de tecnologia da informação no espaço cibernético direcionado contra um ou vários outros sistemas de tecnologia da informação que objetivam dano na segurança da informação que podem ser comprometidos individual ou coletivamente (FAGA, 2017). A Guerra cibernética é um tipo de guerra conduzida a partir de computadores e redes que os conectam, travada por Estados ou seus representantes contra outros Estados (SHELDON, 2016). Dessa forma, pode-se dizer que a guerra é um subconjunto do ataque cibernético. O crime cibernético é uma especificação de crime que é facilitado ou comprometido usando redes computacionais ou dispositivos informacionais (FAGA, 2017). Nesse sentido, há utilização de meios computacionais e viola uma disposição penal tipificada por leis do Estado brasileiro. Há uma grande área comum entre os crimes e os ataques. Entretanto, aqueles que se utilizam de imagens, como pornografia, não são ataques, mas puramente crimes (HATHAWAY, CROOTOF e LEVITZ, 2012).

Há de se ressaltar que os conceitos aqui apresentados mostram uma visão de mundo acadêmica. Muitas instituições no Brasil e no mundo não reconhecem tais conceitos como corretos. Fazem seus próprios protocolos e realizam suas ações neles baseados. Tal situação ocorre com as polícias brasileiras, pois não há um órgão gerencial capaz de estabelecer regras para todas as entidades que trabalham com o tema segurança cibernética a nível estatal. A consequência é uma base de dados não homogênea, o que dificulta a análise dos dados para comparações temporais e regionalizadas.

O cenário dos crimes cibernéticos é caótico no Brasil. Periódicos especializados classificam o Brasil como a quinta fonte de ataques cibernéticos no mundo (PIVA, 2021). No diagnóstico realizado pela Estratégia Nacional de Segurança Cibernética em 2017, verificou-se que houve prejuízo de cerca de 22 bilhões de dólares no mercado brasileiro (BRASIL, 2020). O relatório da *Internet Organised Crime Threat Assessment* (IOCTA) de 2018 atribui a falta de legislação adequada a esses ataques (EUROPOL, 2018).

1.2 Atores.

No ambiente virtual, as pessoas podem desenvolver diversos tipos de atividades, sejam recreativas ou mesmo de trabalho, mas também podem ser vítimas de criminosos especializados, ou até por pessoas que aprendem na própria *internet* como aplicar golpes, ou roubar dados. Dessa forma, criminosos tem migrado de crimes comuns como assaltos para os crimes tecnológicos, principalmente por conta da baixa exposição e pelas penas mais brandas da legislação brasileira (BARRETO, 2016).

Nesse sentido, encontram-se três tipos básicos de atuadores no ciberespaço que podem ser considerados potenciais atores de crimes cibernéticos. Os chamados hackers, pessoas recrutadas e que agem de forma autônoma (chamados por alguns de "lobos solitários"). Os atores do ciberespaço são os mais variados, sendo necessário distingui-los. Em linhas gerais, os Hackers se dividem em dois grupos: os *white hats*, aqueles que possuem conhecimentos de segurança e redes, usando seus conhecimentos para proteção e defesa de sistemas de pessoas e empresas; e os *black hats*, os quais utilizam dos mesmos conhecimentos para práticas criminosas (BARRETO, 2016).

Pessoas recrutadas são aquelas que por suas capacidades na área cibernética, informática, redes e outros podem ser cooptadas para realizar atividades ilícitas para o crime organizado, seja por meio de pagamento ou por coação. Mentes brilhantes podem ser cooptadas no próprio ciberespaço, já que o mundo de jogos é vasto e aberto em toda internet. Nesse caso, jovens conhecedores e reconhecidamente hábeis na internet e em cibernética podem ser recrutados pelas organizações criminosas ou até mesmo nações (KLIMBURG, 2011).

Os chamados "lobos solitários" são pessoas que por motivações diversas e/ou ideológicos, na maioria das vezes radicais, que são criados para defender causas pessoais ou visões de mundo. Nesse sentido atuam no ciberespaço de forma a refletir suas crenças sociológicas e psíquicas como frustrações a ambições pessoais. Estes podem atuar para fomentar causas individuais ou mesmo projetos de poder inspirados a partir de grandes redes e grupos terroristas, tudo isso voluntariamente. Com isso, prontificam-se a fazer de tudo pela causa adotada, em um determinado local e circunstância (PIRES, 2016).

Há vários grupos criminosos organizados de Norte à Sul do país, sendo os principais exemplos: Primeiro Comando da Capital (PCC), Comando Vermelho (CV), Amigos dos Amigos (ADA), Terceiro

Comando Puro (TCP), Primeiro Comando Mineiro (PCM), Paz, Liberdade e Direito (PLD), Comando Norte/Nordeste e Família do Norte (FN) (BITTAR, 2019).

As facções criminosas no Brasil remontam da década de 70. Desde o início, essas facções se especializaram em crimes, sendo que a sustentação econômica advém principalmente do tráfico de drogas. Adicionam-se também outras atividades como roubos, sequestros e assaltos (HARTMANN, 2011).

1.3 Crimes cibernéticos praticados por facções criminosas.

Com a chegada da Era da Informação, houve a necessidade do crime organizado se reinventar para auferir mais lucro. Para tanto, crimes foram inovados dentro do ambiente cibernético. Nesse ínterim, surgem os crimes cibernéticos que são caracterizados por atividade criminosa que tem como alvo ou faz uso de um computador, uma rede de computadores ou dispositivo conectado em rede, infringindo algum dispositivo tipificado em uma lei. Isso mostra que essa derivação de crime não é praticada somente por hackers, mas também por pessoas ou organizações (KASPERSKY, 2019).

O ciberespaço é definido como um novo domínio das relações de poder, onde atores diversos estão integrados ao meio técnico-científico-informacional, o que faz surgir desafios e ameaças diferentes dos domínios tradicionais. As barreiras à entrada no ciberespaço diminuem a cada dia. Com dispositivos de fácil acesso e baixo custo, torna-se cada vez mais difícil de se identificar de onde partiu um ataque, podendo qualquer pessoa mal-intencionada executar ações em meio a um ambiente desafiador e incerto, já que não possui fronteiras geográficas, e praticamente, anônimas. Os atores dessas ações podem ser desde adolescentes até organizações criminosas (COLARIK, 2015).

Ainda que a criminologia não tenha se aprofundado no estudo dos delitos em grupo, entende-se que a associação para o mal é comum na delinquência, sendo as facções criminosas um fenômeno de aproximação de pessoas de forma gregária. Dessa feita, formam organizações sociais delinquentes, com intuito comum de praticar crimes, tendo como motivador um grupo de influência organizado e hierarquizado (SHIMIZU, 2011).

Outra característica importante de se ressaltar é que as facções criminosas são enquadradas no chamado crime organizado que possui uma estrutura capaz de articular ordens e estabelecer objetivos concretos a serem atingidos por seus membros. Assim, impõem respeito às normas autoridades de seus

líderes, calculando previamente os riscos de cada operação na busca de resultados (DOS SANTOS BIGOLI, 2014)

Uma das formas de implementação da informatização foi modificar a forma de venda de ilícitos, na qual traficantes passaram a vender de forma online, por meio da *deep* e *dark web*, sendo incluído o serviço de entrega até usuário final. Essa modificação no modo de venda talvez seja responsável pelo maior *boom* econômico das organizações narco criminosas, pois conseguiram atingir maior público e, portanto, maximizou lucros (LACERDA, 2018).

Usando os lucros da venda de drogas, as principais facções brasileiras revertem esse dinheiro para compra de armas com fins da autoproteção do grupo criminoso e ampliação da sua área de venda (CORDEIRO, 2019). A *deep e dark web* também facilitaram o tráfico internacional ilegal de armas (COX, 2017).

Os crimes não ficaram apenas na parte de vendas. Alastrou-se, tornando-se uma base para operações contra alvos. Um exemplo ocorreu quando houve monitoramento de agentes de segurança que trabalhavam no presídio federal de Catanduvas–PR. A consequência foi a morte de Melissa de Almeida Araújo em uma emboscada, supostamente, por ser a responsável pela transferência do traficante Marcola para o presídio federal em Rondônia. As investigações concluíram de que Melissa foi seguida por membros da facção PCC, utilizando as redes sociais da ex-psicóloga (COSTA, 2017).

Investigações oficiais apontam que o PCC possui técnicas avançadas de investigação social com pesquisas aprofundadas em redes sociais, como Facebook, Snapchat, Instagram, Twitter e fontes oficiais, utilizando-se de cadastros e dados publicados em páginas oficiais nos mais diversos órgãos públicos. De posse dessas informações, realizam ameaças contra agentes e trabalhadores, como magistrados, promotores, repórteres e servidores de segurança pública (PAZ, 2019).

A utilização das redes sociais também serve para divulgação e promoção de atividades, contribuindo com a projeção do poder e disseminação do medo na sociedade. Os criminosos usam imagens de suas ações, exibem armas e escolhem suas próximas vítimas. Um exemplo ocorreu com Luyan Roges, quando seu assassinato foi gravado, postado em uma rede social e enviado aos familiares. Esse crime teria sido executado após julgamento e ordem dos “Tribunais do Crime” (ARAUJO, 2019).

Com a maior adoção de comunicações pelo meio digital, a polícia tem interceptado conversas e ordens emanadas por facções. Entretanto, esse é um trabalho difícil, pois quando a justiça solicita informações para as empresas detentoras de serviços de comunicações, esbarram em recusas fundamentadas na privacidade do cliente. Tal situação leva a intermediação do poder judiciário que pode ou não continuar com o procedimento investigatório (THOMAS, 2016).

Outro crime comum por parte de integrantes do crime organizado é a clonagem de cartões de crédito. As técnicas são variadas, podendo se levar a cabo com a instalação de uma simples câmera com a finalidade de filmar os dados do cartão até a instalação de *chips* em leitores (LAVORENTI E SILVA, 2000).

Há pessoas que não se envolvem diretamente com o crime organizado (chamados de simpatizantes pela causa), mas que têm realizado um ciberativismo para legalização de ilícitos (SILVA e ROSA, 2019), corroborando com a percepção de poder das facções no ciberespaço. Há registros de que essas pessoas estejam levando discussões para legalização das drogas, tendo como um dos argumentos o poderio das facções, tentando levar terror à sociedade.

O crime organizado também passou a vislumbrar as criptomoedas como fonte de recursos, principalmente nas situações de sequestros. Existem relatos de exigências de pagamentos de resgate utilizando *bitcoins*, o que dificulta a atuação das delegacias especializadas (PAGNAN, 2017). Outra forma foi verificada pelo uso de mineradoras de *bitcoins*. Dessa forma, os criminosos usando o lucro advindo de ativos virtuais podem comercializar armas. Esse procedimento é dificilmente rastreado pelos órgãos responsáveis, por conta pouca gama de dados de rastreabilidade nas transações comerciais utilizando-se as criptomoedas (BARBOSA, 2019).

Outro ponto que dificulta o processo investigatório é que, infelizmente, os registros de crimes cibernéticos arquivados nas polícias especializadas pouca padronização. Não há unificação dos procedimentos relativos às investigações dos crimes cibernéticos e, dessa forma, cada delegacia possui um *modus operandi* próprio. A criação de delegacias, núcleos técnicos e grupos especializados, com treinamento e capacitação periciais poderiam mitigar essa vulnerabilidade (MPF, 2016).

O sistema PIX desenvolvido pelo Banco Central para facilitar transações bancárias (BRASIL, 2021) também tem representado mais um canal de vulnerabilidade cibernética. Criado para acompanhar

tendência mundial, o sistema possui brechas de segurança física. Quadrilhas especializadas em sequestros relâmpagos pedem resgate utilizando-se essa plataforma. Como a transferência é praticamente instantânea, os bandidos se aproveitam de contas laranjas para poder receber o dinheiro e, após sacado, é muito difícil de achar os mandantes (GUGELMIN, 2021).

CONCLUSÃO.

O ambiente incerto, ambíguo, complexo e vulnerável em que o Brasil faz parte apresenta problemas inéditos. Como apresentado nesse artigo, o próprio crime organizado, ou não organizado, adaptou-se as novas formas de transações comerciais para criar novos golpes e estelionatos.

O uso do espaço cibernético para prática de crimes traz novos desafios para os agentes de segurança pública, para os legisladores e para os países como um todo. O anonimato nas ações criminosas envolvendo o campo informacional, em específico o cibernético, dificulta ações mais concretas contra criminosos digitais.

Ademais, há a necessidade de criar leis mais enérgicas em termos de punição quando se trata de crimes no espaço cibernético. Por se tratar de tema relativamente novo, muitas discussões precisam avançar nesse campo. Somente uma legislação mais rígida e capacidade de vigilância e pronta resposta vão permitir um combate mais efetivo contra esses criminosos.

Por se falar em capacidade de vigilância e ações contra os criminosos, os órgãos governamentais responsáveis nas mais diversas esferas precisam unificar esforços no combate ao crime organizado. A interação no aprimoramento técnico profissional, bem como o compartilhamento de informações, principalmente de banco de dados, pode ajudar a superar o óbice no combate aos crimes cibernéticos. Verificou-se também que os protocolos de ferramentas extremamente flexíveis dificultam a implantação de níveis de segurança com maior robustez. No caso do Pix, há necessidade de inserir tais características protocolares, como a adoção de cadastramento prévio e regras mais duras sobre transferência de altos valores (dependente do perfil de cada usuário).

Constata-se que há basicamente três tipos de atuadores no ciberespaço: os chamados "*hackers*", pessoas recrutadas e "lobos solitários". Qualquer um desses três atores podem ser responsáveis por crimes cibernéticos. Nesse sentido, o objetivo desse artigo foi verificar a relação entre facções criminosas e crimes cometidos no espaço cibernético.

Verifica-se que as facções criminosas brasileiras já se inseriram na "Era da Informação". Pode-se dizer que, aparentemente, ainda estão em um estágio inicial, visto que utilizam tecnologias que estão disponíveis a todo o público. Entretanto, caso haja investimentos massivos, esses grupos podem representar grave ameaça contra a democracia e ao Estado de Direito, uma vez que podem direcionar suas ações às infraestruturas estratégicas e causar estragos substanciais à sociedade brasileira.

Dessa forma, há uma aparente relação das facções criminosas, desde 2012 no Brasil, principalmente no recrutamento de pessoas com conhecimentos na área de informática. Como visto, essas pessoas recrutadas podem ser até mesmo jovens e menores de idade que estudam procedimentos, técnicas e golpes para ampliar o leque de atuação das facções criminosas visando o aumento do lucro e financiamento de outros crimes. Infelizmente, a legislação brasileira não se flexibilizou a ponto de aproveitar as pessoas que trabalham para os crimes cibernéticos de forma a serem aproveitadas em ações legais, em apoio às polícias, conforme ocorre no EUA e em outros países.

É certo que além das pessoas recrutadas pelo crime organizado, há atuação de "lobos solitários" e *hackers* mal-intencionados. Novamente voltamos a questão da dificuldade em atribuir autoria para um crime digital cometido no espaço cibernético. Para mitigar esses óbices, cresce de importância o trabalho de inteligência e o compartilhamento de informações entre os atores que combatem diuturnamente a perversidade dos crimes cibernéticos.

Por fim, verifica-se que o avanço tecnológico trouxe muita comodidade ao mundo moderno. A situação atual com a Pandemia do COVID-19 aumentou ainda mais o uso de ferramentas no espaço cibernético e em consequência as transações comerciais e financeiras rapidamente adaptaram-se a nova realidade. O cidadão passou a ficar mais exposto e suscetível a crimes cibernéticos, crescendo de importância a conscientização da sociedade quanto aos procedimentos de segurança e correto uso dos dispositivos eletrônicos disponíveis.

REFERÊNCIAS

AGUIAR, Andrey J. **Qual é a Diferença entre Dark Web e Deep Web?** Disponível em: <*https://www.tecmundo.com.br/internet/128029-diferenca-entre-dark-web-deep-web.htm*>. Acessado em 10 de abril de 2020.

ALMEIDA, D. J. **Globalização: A Sociedade em Rede**. 2019. Disponível em <*https://docplayer.com.br/24218555-Globalizacao-a-sociedade-em-rede.html*>. Acesso em 30 de setembro de 2020.

ARAUJO, Ismael. **Facções Usam Internet na Divulgação de seus Crimes.** Disponível em: <*https://imirante.com/oestadoma/noticias/2019/07/13/faccoes-usam-a-internet-na-divulgacao-de-seus-crimes/*>. Acessado em 03 de abril de 2020.

BARBOSA, Soraia. **PM de São Paulo Apreende Mineradora Usada Pelo PCC.** Disponível em: <*https://guiadobitcoin.com.br/noticias/pm-sao-paulo-apreende-mineradora-pcc/*>. Acesso em 21 de fevereiro de 2020.

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética: À Luz do Marco Civil da Internet**. Brasport. 2016.

BARROS, Evelin. **Saiba a Diferença entre Surface Web, Dark Web e Deep Web, e Entenda o Lado Obscuro da Internet.** Disponível em <*https://blog.maxieduca.com.br/saiba-a-diferenca-entre-surface-web-dark-web-e-deep-web-e-entenda-o-lado-obscuro-da-internet/*>. Acessado em 10 de abril de 2020.

BITTAR, Paula. **Especial Presídios - A História das Facções Criminosas Brasileiras.** 2019. Disponível em <*https://www.camara.leg.br/radio/programas/271725-especial-presidios---a-historia-das-faccoes-criminosas-brasileiras--05--50-->. Acessado em 21 de fevereiro de 2020.

BRASIL. **Decreto nº 10.222 de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília. 2020.

BRASIL. Banco Central. **O Que É Pix?** 2021. Disponível em: <*https://www.bcb.gov.br/estabilidadefinanceira/pix*>. Acessado em 7 de julho de 2021.

CASTELLS, M. (2002). **A Era da Informação**: **Economia, Sociedade e Cultura** (6 ed.). (R. V. Majer, Ed.) Rio de Janeiro: Paz e Terra S/A.

COHEN-ALMAGOR, R. **Internet History**. International Journal of Technoethics, pp 45-64. Abril-Junho de 2011.

CORDEIRO, Tiago. **Como Facções como PCC e Comando Vermelho Controlam o Contrabando no Brasil.** Disponível em: <*https://www.gazetadopovo.com.br/republica/como-faccoes-como-pcc-e-comando-vermelho-controlam-o-contrabando-no-brasil/*>. Acessado em 10 de abril de 2020.

COSTA, Flávio. **Monitoramento, Emboscada e Tiros no Rosto: Como o PCC Matou Psicóloga de Prisão Federal.** Disponível em: <*https://noticias.uol.com.br/cotidiano/ultimas-noticias/2017/07/24/monitoramento-emboscada-e-tiros-no-rosto-como-o-pcc-matou-psicologa-de-prisao-federal.htm*>. Acessado em 21 de fevereiro de 2020.

COX, Joseph. **Traficantes da Deep Web Contrabandeavam Armas Dentro de DVDs e Karaokês**. Disponível em: <*https://www.vice.com/pt_br/article/payy5g/traficantes-da-deep-web-contrabandeavam-armas-dentro-de-dvds-e-karaokes*>. Acessado em 10 de abril de 2020.

EUROPOL, European Union Agency For Law Enforcement Cooperation. ***Internet Organised Crime Threat Assessment (IOCTA) 2018***. Disponível em: <*https://www.europol.europa.eu/activitiesservices/main-reports/internet-organised-crime-threat-assessment-iocta-2018*> Acesso em junho de 2019.

FAGA, H. P. (2017). **The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century**. A Journal of Vytautas Magnus University, p 1-34. DOI: 10.1515/bjlp-2017-0001

GUGELMIN, Felipe. **Sequestros-Relâmpago Crescem com a Adoção de Pagamentos Via Pix.** 2021. Disponível em: <*https://canaltech.com.br/seguranca/sequestros-relampago-crescem-com-a-adocao-de-pagamentos-via-pix-189022/*>. Acessado em 6 de julho de 2021.

HARTMANN, Julio Cesar Facina. **Crime Organizado no Brasil.** Assis, 2011. p 58. Trabalho monográfico apresentado ao curso de Direito do IMESA (Instituto Municipal de Ensino Superior de Assis). Disponível em: <*https://cepein.femanet.com.br/BDigital/arqTccs/0611230215.pdf*>. Acessado em 28 de fevereiro de 2020.

HATHAWAY, O. A., CROOTOF, R., & LEVITZ, P. e. (2012). **The Law of Cyber-Attack**. California Law Review, 817-886.

KALLBERG, J., & COOK, T. S. (2017). **Four Cyber Tenets That Undermine Conventional Strategies.** The Unfitness of Traditional Military Thinking in Cyber, 8126-8130.

KASPERSKY. **O Que é Crime Cibernético? Tipos de Crimes Cibernéticos**. 2019. Disponível em: <*https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime*>. Acessado em 30 de abril de 2020.

KIM, J. H. (jan/jun de 2004). **Cibernética, Ciborgues e Ciberespaço**: **Notas Sobre as Origens da Cibernética e sua Reinvenção Cultural**. Horizontes Antropológicos, 21, 199-219.

KLIMBURG, A. (2011). **Mobilising Cyber Power**. **Survival: Global Politics and Strategy,** 53(1), 41-60.

KUEBL, D. T. (2017). **From Cyberspce to Cyberpower**: **Defining the Problem. Cyberpower and National Security**, p 24-42.

LACERDA, Ricardo. **O Portal de Drogas da Deep Web.** Disponível em: <*https://super.abril.com.br/comportamento/o-portal-de-drogas-da-deep-web/*>. Acessado em 10 de abril de 2020.

LAVORENTI, Wilson; e SILVA, José Geraldo. **Crime Organizado na Atualidade.** Edição Bookseller. Campinas, São Paulo. 2000.

MARQUES, R. S. **O Ambiente Cibernético e o Direito Internacional dos Conflitos Armados: Uma Proposta de Adequação Doutrinária**. Doutrina Militar Terrestre. 2018.

MENEGHETI, Francis Kanashiro. **Origem e Fundamentos dos Tribunais do Crime.** Disponível em: <*http://www.anpad.org.br/diversos/down_zips/68/2013_EnANPAD_EOR792.pdf*>. Acessado em 10 de abril de 2020.

MILHOMENS, Lucas. **Entendendo o Ciberativismos em Terra na Nova Esfera Pública Interconectada.** Dissertação (Mestrado em Comunicação) do Programa de Pós-graduação em Comunicação. Universidade Federal da Paraíba, João Pessoa. 2009.

MORGENTHAU, H. J. **A Política Entre as Nações: A Luta Pelo Poder e Pela Paz**. (K. W. THOMPSON, Trad.) São Paulo. Universidade de Brasília. 2003.

MPF. **Atuação do Ministério Público Federal: Combate aos Crimes Cibernéticos.** Disponível em: <*https://www.cnmp.mp.br/portal/images/Palestras/Atua%C3%A7%C3%A3o_do_MP_no_combate_aos_crimes_cibern%C3%A9ticosINFANCIA_E_JUVENTUDE.pdf*>. Acessado em 11 de abril de 2020.

OLIVEIRA, T. M. (Maio de 2020). **Manifestações e Aglomerações em Períodos de Pandemia por Covid-19**. Interamerican Journal of Medicine and Health, 2020;3:e202003025.

PAGNAN, Rogério. **Bandidos Pedem 'Dinheiro Digital' para Libertar Refém de Seqüestro.** Disponível em: <*https://www1.folha.uol.com.br/cotidiano/2017/05/1880569-bandidos-pedem-dinheiro-digital-para-libertar-refem-de-sequestro.shtml*>. Acessado em 10 de abril de 2020.

PAZ, Dayene. **Durante Ofensiva em Presídio, Chefe do PCC Debocha e Ameaça Polícia.** Disponível em: <*https://www.midiamax.com.br/policia/2019/operacaoo-impetus-pcc-debocha-em-rede-social-um-dia-da-caca-outro-do-cacador*>. Acessado em 10 de abril de 2020.

PIA, Artur. **Brasil Fica na 5ª Posição no Ranking de Ataques Cibernéticos no Mundo.** 2020. Disponível em: <*https://revistaoeste.com/tecnologia/brasil-fica-na-5a-posicao-no-ranking-de-ataques-ciberneticos-no-mundo/*>. Acessado em 3 de agosto de 2021.

PIRES, Nuno Lemos. **Do Terrorismo Transnacional ao Choque de Valores**. Nação e Defesa. 2016.

RATTRAY, G. **Strategic Warfare in Cyberspace**. Washington. MIT Press. 2001.

SCHIAVON, Guto. **Mineração de Bitcoin: Entenda Como Funciona.** Disponível em: <*https://cointimes.com.br/mineracao-de-bitcoin-entenda-como-funciona/*>. Acessado em 10 de abril de 2020.

SERPA, D. A. L. **Pix é o Nome do Sistema de Pagamentos Instantâneos do Banco Central.** 2020. Disponível em: <*https://www.inovarti.com.br/pix-e-o-nome-do-sistema-de-pagamentos-instantaneos-do-banco-central/*>. Acessado em 03 de abril de 2021.

SHELDON, J. B. **Cyberwar**. 2016. Disponível em: <*https://www.britannica.com/topic/cyberwar*>. Acesso em 30 de setembro de 2020.

SHIMIZU, Bruno. **Solidariedade e Gregarismo nas Facções Criminosas: Um Estudo Criminológico à Luz da Psicologia das Massas**. 2011. Tese de Doutorado. Universidade de São Paulo.

SILVA, J. C. P.; ROSA, L. C. dos S. **Uma Análise Sobre as Associações de Usuários de Drogas das Regiões Sudeste e Centro-Oeste a Partir do Ciberativismo.** Congresso Brasileiro de Ciência e Sociedade. Centro Universitário Santo Agostino, Teresina – PI. 2019. Disponível em: <*https://proceedings.science/proceedings/100107/_papers/110639/download/fulltext_file1*>. Acessado em 26 de maio de 2021.

THOMAS, Jennifer Ann**. Redes Marginais: O Submundo do Facebook, do WhatsApp e do Youtube.** Disponível em: <*https://veja.abril.com.br/tecnologia/redes-marginais-o-submundo-do-facebook-do-whatsapp-e-do-youtube/*>. Acessado em 03 de abril de 2020.

WIENER, N. **Cibernética**: **O El Control y Comunicación en Animales y Máquinas**. 1998. Disponível em <*https://www.metodista.br/revistas/revistas-metodista/index.php/CSO/article/download/856/907#:~:text=Aqui%20%C3%A9%20preciso%20destacar%20que,e%20n%C3%A3o%20somente%20de%20comunica%C3%A7%C3%A3o.&text=Nesse%20sentido%2C%20a%20comunica%C3%A7%C3%A3o%20an%C3%B*>. Acesso em 19 de abril de 2021.

DADOS DOS AUTORES:

Eliezer de Souza Batista Junior

Doutorando em Ciências Militares pela Escola de Comando e Estado-Maior do Exército (Instituto Meira Mattos). Mestre em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais. Pós-Graduado em Ciência de Dados e Big Data Analytics, Análise de Malware, Guerra Eletrônica e Guerra Cibernética. Bacharel em Sistemas de Informações e Ciências Militares. É oficial do Exército no posto de Major.

Henrique de Queiroz Henriques

Mestrando em Ciências Militares pela Escola de Comando e Estado-Maior do Exército (Instituto Meira Mattos). Pós-Graduado em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais.

Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras. É oficial do Exército Brasileiro no posto de Tenente-Coronel.

Rober Yamashita

Doutor, PhD em Business Administration pela Asia e University, Kuala Lumpur, Malásia (2020). Graduado em Ciências Militares pela Academia Militar das Agulhas Negras (2004). Especialização em Guerra Eletrônica pelo Centro de Instrução de Guerra Eletrônica (2005). Especialização em Criptografia e Segurança de Redes pela Universidade Federal Fluminense (2007). Especialização em Mestre D´Armas pela Escola de Educação Física do Exército (2007). Graduação em Administração pela Universidade do Sul de Santa Catarina (2011). Mestrado em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (2012). Curso de Comando e Estado-Maior do Exército (ECEME) biênio 2019/2020. É oficial do Exército no posto de Major.

RISP
Revista de Inteligência de Segurança Pública
ISSN 2675-7168; 2675-7249

INTELIGÊNCIA DE SEGURANÇA PÚBLICA E INVESTIGAÇÃO CRIMINAL: APRENDER AS DIFERENÇAS PARA DESENVOLVER A CULTURA DE INTELIGÊNCIA NO ÂMBITO DA SEPOL/RJ

Robson da Costa Ferreira da Silva

RESUMO: Este ensaio aborda a problemática da falta de cultura de Inteligência no âmbito da Secretaria de Estado de Polícia Civil do Rio de Janeiro. O objetivo deste estudo é, a partir da diferenciação feita da Atividade de Inteligência e Atividade Investigatória, propor soluções para o incremento da Atividade de Inteligência na estrutura da SEPOL, principalmente no âmbito das Delegacias de Polícia. A metodologia adotada comportou uma pesquisa bibliográfica e documental, visando buscar referenciais teóricos e fazer um diagnóstico da SEPOL, além da experiência do autor como Delegado de Polícia Civil do Estado do Rio de Janeiro e mais especificamente como profissional da área de inteligência. O campo de estudo delimitou-se a diferenciação das atividades, de inteligência e investigatória, ao sistema de inteligência da SEPOL e às Delegacias de Polícia nesse contexto. Os principais tópicos são: Inteligência de Segurança Pública e Investigação Criminal: pontos convergentes e divergentes e o Sistema de Inteligência da Secretaria de Estado de Polícia Civil (SISEPOL). A conclusão indica a falta de cultura de Inteligência no âmbito da SEPOL, mais especificamente nas Delegacias de Polícia, o que gera uma baixíssima produtividade na busca, análise e disseminação de conhecimentos em todo Sistema de Inteligência da instituição. Aponta como soluções a lotação de um Analista de Inteligência em cada Delegacia de Polícia e o incremento do ensino da matéria Inteligência na formação acadêmica dos futuros gestores.

Palavras-Chave: Inteligência de Segurança Pública no Estado do Rio de Janeiro. Efetividade do SISEPOL.

ABSTRACT: This essay addresses the problem of the lack of a culture of intelligence within the scope of the State Secretariat of Civil Police of Rio de Janeiro. The objective of this study is, based on the differentiation made between the Intelligence Activity and Investigative Activity, to propose solutions to increase the Intelligence Activity in the structure of SEPOL, mainly within the scope of the Police Stations. The methodology adopted involved a bibliographic and documentary research, aiming to seek theoretical references and make a diagnosis of SEPOL, in addition to the author's experience as Civil Police Delegate of the State of Rio de Janeiro and more specifically as an intelligence professional. The field of study defined the differentiation of activities, from intelligence and investigative, to the intelligence system of SEPOL and to the police stations in this context. The main topics are: Public Security Intelligence and Criminal Investigation: converging and diverging points and the Intelligence System of the State Secretariat of Civil Police (SISEPOL). The conclusion indicates the lack of a culture of intelligence within the scope of SEPOL, more specifically in the police stations, which generates a very low productivity in the search, analysis and dissemination of knowledge throughout the institution's Intelligence System. It points out as solutions the capacity of an Intelligence Analyst

in each Police Station and the increase of the teaching of the Intelligence subject in the academic formation of the future managers.

Keywords: Public Security Intelligence in the State of Rio de Janeiro. Effectiveness of SISEPOL.

INTRODUÇÃO.

O presente artigo tem por escopo aclarar a distinção entre Inteligência de Segurança Pública e Investigação Criminal, de forma que a atividade de inteligência seja desenvolvida com eficiência no âmbito da SEPOL/RJ (Secretaria de Polícia Civil do Estado do Rio de Janeiro), principalmente no fluxo de informações que tenha por origem as Delegacias de Polícia, base do organograma da instituição. O fato da atividade de inteligência de segurança pública e a atividade investigatória criminal possuírem alguns pontos de intersecção, aliado ao desconhecimento do que seja a atividade de inteligência, sua finalidade e importância, acarreta uma baixíssima produtividade das Delegacias de Polícia, no que se refere a remessa de dados, informações e conhecimentos de inteligência.

Para tanto, será feita uma classificação da atividade de inteligência e suas espécies, dentre as quais a Inteligência de Segurança Pública (ISP), que será conceituada com vistas a melhor diferenciá-la da investigação criminal. Com o mesmo objetivo, será trabalhado o tema da investigação criminal. Numa fase seguinte serão apresentadas as principais diferenças, semelhanças e pontos de intersecção entre ambas atividades, suas finalidades e importâncias. Também será demonstrado o funcionamento do Sistema de Inteligência da Secretaria de Estado da Polícia Civil do Estado do Rio de Janeiro (SISEPOL), mas especificamente no que se refere ao papel das Delegacias de Polícia.

Trataremos também das causas e consequências desse fenômeno e proporemos algumas mudanças práticas, de baixo custo e de fácil execução, que entendemos ser suficientes para minorá-lo.

Como metodologia utilizada, além da base teórica retirada da legislação pertinente, periódicos, literatura especializada e de artigos científicos, será apresentada a quantidade do fluxo de informações de inteligência recebidas pela Subsecretaria de Inteligência da SEPOL/RJ (SSINTE), órgão central não só da SEPOL mas de todo Sistema de Inteligência de Segurança Pública do Estado do Rio de Janeiro (SISPERJ), com o objetivo de contrastar quantitativamente o fluxo total recebido e o fluxo recebido apenas das Delegacias de Polícia do Estado do Rio de Janeiro. Será também apresentada análise da

grade curricular dos últimos cursos de formação para Delegado de Polícia Civil do Estado do Rio de Janeiro, como forma de demonstrar quantitativamente como se dá o ensino de Inteligência na formação dos policiais da SEPOL/RJ, mais especificamente seus gestores.

1. INTELIGÊNCIA DE SEGURANÇA PÚBLICA.

Para distinguir, num primeiro momento é preciso jogar luzes sobre ambas as realidades de forma individual e pormenorizada. Começaremos pela ISP.

Segundo o artigo 1º, § 2º, I da Lei n.º 9.883/1999 que instituiu o SISBIN, inteligência é:

> "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."

O conceito é repetido por toda a legislação subjacente.

Trata-se da produção de conhecimento elaborado, cuja matéria-prima é obtida por fontes abertas ou não, tendente a assessorar o tomador de decisões em seu processo decisório. O sigilo é um componente essencial da atividade e pode estar inserido nos dados obtidos e/ou na análise feita. Toda atividade que envolva planejamento e tomada de decisão, que dependa de um dado negado ou uma análise secreta, pode ser escopo da atividade de inteligência. (GONÇALVES, 2017).

Segundo a Doutrina de Inteligência de Segurança Pública do Estado do Rio de Janeiro - DISPERJ/2015 (Documento Reservado), que padroniza e sistematiza os procedimentos de ISP no Estado do Rio de Janeiro:

> A atividade de Inteligência de Segurança Pública (ISP) - nos seus dois ramos, Inteligência e Contrainteligência - é o exercício permanente e sistemático de ações especializadas para identificar, avaliar e acompanhar ameaças reais ou potenciais na esfera de Segurança Pública, basicamente orientadas para produção e salvaguarda de conhecimentos necessários para subsidiar os tomadores de decisão, para o planejamento e execução de uma política de Segurança Pública e das ações para prever, prevenir, neutralizar e reprimir atos criminosos de qualquer natureza que atentem à ordem pública, à incolumidade das pessoas e do patrimônio.

Nota-se pelo contraste dos conceitos colacionados acima, que a relação se dá entre gênero (Inteligência) e espécie (ISP). Cabe ressaltar também a menção feita pelo último texto legal a um duplo objetivo desejado pela ISP: assessorar no nível estratégico, ou seja, no planejamento e execução de

políticas de Segurança Pública, bem como no nível tático-operacional, que também engloba a atividade investigatória criminal. Esta relação entre a atividade de ISP e a investigatória, será melhor explicitada em tópico próprio.

Os autores, tantos os clássicos, quanto os modernos, dentro e fora do Brasil, apresentam modelos de classificação distintos relativos à atividade de inteligência.

Uma apropriada classificação, condizente com os desafios atuais e com a ampliação do campo de aplicação da atividade de inteligência é de suma importância como forma de determinar-se o alcance e a abrangência da ISP. Essencialmente e em resumo, será evidenciada uma compreensão exata do que seja e onde se insere a ISP como instrumento de obtenção de ganhos contra o crime, notadamente o mais organizado.

Através de uma classificação própria, procuraremos demonstrar que a Inteligência de Segurança Pública é modalidade de inteligência tão nobre como qualquer outra e que é instrumento eficaz de assessoramento às políticas e ações nesta seara.

As distinções em vários ramos são acidentais, não modificam a essência da atividade, apenas as distinguem, ainda que sob o mesmo eixo. Inteligência é o gênero do qual derivam várias espécies conforme a categorização observada. Inteligência de Segurança Pública é espécie do gênero Inteligência, embora por vezes essa terminologia venha sendo empregada de forma genérica e equivocada. Não raro, sua importância e alcance são diminuídos por conta desses equívocos.

Segundo Mingardi (2007), a Inteligência Criminal, numa análise que consideramos equivocada, "é considerada uma espécie de "prima pobre" da Inteligência de Estado e "prima distante" da Inteligência Militar, que é a atividade mais antiga do ramo." O menosprezo se dá como se o assunto tratado (segurança pública) fosse menos relevante, ou pela confusão comum entre ISP e investigação criminal.

Propomos uma classificação disposta em 05 (cinco) categorias distintas: quanto ao ente; quanto ao ambiente; quanto à abrangência; quanto ao destinatário e quanto ao seu objeto.

Com relação ao ente, a Inteligência é classificada em pública e privada, conforme a natureza jurídica de quem a produz. A Inteligência clássica nasceu com o Estado Moderno, como forma de

buscar dados para assessorar o Chefe de Governo e/ou Estado na tomada de decisões. Com o passar dos tempos as corporações viram a necessidade de aplicar no âmbito empresarial a metodologia do conhecimento para, estrategicamente, fazer frente aos desafios inerentes à sua atividade.

No que concerne ao ambiente cinde-se em externa e interna, conforme a localização do dado a ser buscado ou coletado.

Quanto à abrangência, a Atividade de Inteligência se divide, conforme classificação da Escola Superior de Guerra, entre Inteligência Global, Regional e Setorial. Global é aquela que diz respeito aos interesses da nação como um todo em relação às outras nações, regional, aquela de interesse de determinada região e setorial aquela que concerne à determinado setor ou atividade.

No que diz respeito ao seu destinatário, a divisão se dá entre Inteligência político-estratégica e tático-operacional, conforme a posição em que se encontra o decisor, destinatário do produto da Inteligência. Político-estratégica é aquela de interesse do dirigente da nação ou de Estado-Membro, bem como dos respectivos primeiros escalões. Dirigem-se ao assessoramento na formulação de políticas públicas ou nas decisões estratégicas. Tático-operacional é aquela direcionada aos órgãos de execução das políticas e ações a serem implementadas.

Por fim, quanto ao seu objeto, divide-se em 04 (quatro) grandes grupos: Inteligência de Estado, Militar, de Segurança Pública e Administrativo-Fiscal.

Inteligência de Estado é aquela de alto nível, relativa ao interesse nacional frente aos demais entes da comunidade internacional. Busca o conhecimento sobre Estados estrangeiros, visando um planejamento estratégico (no sentido de se atingir um ponto desejado no futuro) da Nação.

Inteligência Militar é a que visa, em tempo de paz ou de guerra, conhecer o poder militar e a fisiografia de Estados que sejam inimigos declarados ou potenciais.

O conceito de Inteligência de Segurança Pública já foi colacionado acima por ocasião da apresentação do texto da DISPERJ.

Por fim, Inteligência Administrativo-Fiscal é que aquela cujo conhecimento busca o assessoramento nas atividades em que o Estado exerce seu Poder de Polícia Administrativo, Poder Fiscalizatório ou Correcional. Não tem por escopo produzir conhecimento sobre Segurança Pública,

porém, não raro, esbarra de forma colateral neste tema. São exemplos dessa modalidade de Inteligência, a Inteligência Tributária, Penitenciária, Ambiental e Previdenciária. Por tangenciarem, por vezes, a temática da Segurança Pública, podem, e devem ser incluídas em qualquer sistema que se destine à atividade de Inteligência de Segurança Pública.

Conforme a classificação por nós elaborada, a Inteligência de Segurança Pública é: pública; externa ou interna; global, regional ou setorial; política-estratégica ou tático-operacional. Ou seja, a Inteligência não fica restrita pelo assunto que ela aborda, torna-se Inteligência pelos seus requisitos essenciais e não perde essa qualidade por aspectos acidentais, como por exemplo, o nível hierárquico do decisor, tema de referência, dentre outros.

2 INVESTIGAÇÃO CRIMINAL.

A atividade investigatória, em linhas gerais, consiste em transformar, ainda que no mundo das ideias, uma situação indeterminada em uma situação determinada, a ponto de situá-la conforme as distinções e relações que a constituem, unificando o todo a partir da situação originariamente encontrada. Esta é a lição do filósofo John Dewey (1938, p. 58).

Esta atividade pode envolver movimentos ou fatos dentro do mundo das coisas, como também operações mentais, como juízos, raciocínios ou pensamentos, ou ainda ambos (DUTRA, 2005, p. 167).

É a atividade de descobrir, utilizando-se de métodos físicos, mentais, lógicos, éticos ou jurídicos possíveis, uma realidade que ainda não foi descortinada. Ou ainda, é trazer à tona ao mundo visível ou intelectualmente aferível, uma realidade até então ignorada.

A investigação criminal, como espécie desse gênero que é a investigação científica, não foge dos aspectos essenciais de sua matriz, diferindo-se por especificidades próprias.

Eliomar da Silva Pereira define a investigação criminal, confrontando esta atividade com a atividade genérica de investigação científica. Diz o autor que é a

> "Atividade pragmática e zetética por essência, é uma pesquisa, ou conjunto de pesquisas, administradas estrategicamente, que, tendo por base critérios de verdade e método limitados juridicamente por direitos e garantias fundamentais, está dirigida a obter provas acerca da existência de um crime, bem como indícios de sua autoria, tendo por fim justificar um processo penal, ou a sua não instauração, se for o caso, tudo instrumentalizado sob uma forma jurídica estabelecida por lei."

Difere a investigação criminal das demais espécies principalmente por seu objeto e por seus objetivos. Seu objeto de análise é o crime e o criminoso e seus objetivos são a descoberta e a reconstituição da verdade dos fatos e o apontamento da autoria.

A investigação criminal se materializa, precipuamente, através do Inquérito Policial, previsto no artigo 4º e seguintes do Código de Processo Penal. Segundo Lima (2017; p. 105):

> "... consiste em um conjunto de diligências realizadas pela polícia investigativa objetivando a identificação das fontes de prova e a colheita de elementos de informação quanto à autoria e materialidade da infração penal, a fim de possibilitar que o titular da ação penal possa ingressar em juízo."

Bom frisar que, por trabalhar na expectativa da restrição da liberdade, fica a investigação criminal a todo tempo submetida ao regramento constitucional e infraconstitucional, além do controle externo do Ministério Público.

3 INTELIGÊNCIA DE SEGURANÇA PÚBLICA E INVESTIGAÇÃO CRIMINAL: PONTOS CONVERGENTES E DIVERGENTES.

As confusões feitas pelo público em geral, mas, principalmente pela imprensa, políticos e profissionais da Segurança Pública em relação à ISP e à Investigação Criminal, têm sido a principal causa de restrições e equívocos quanto ao âmbito de aplicabilidade desta modalidade de Inteligência.

Um erro comum é utilizar o termo "inteligência" fora de seu sentido técnico, ou seja, de método sistematizado e permanente de produção de conhecimento. É verdade que a estratégia de focar o combate à criminalidade no embate violento tem sido pouco eficaz e não permite o desmantelamento de organizações criminosas, apenas resulta em mortes e poucas prisões em flagrante. Dessa forma, o termo "inteligência" vem sendo empregado sistematicamente em contraposição à essa política de enfrentamento violento, como sinônimo de investigação criminal silenciosa. Não raro, quando morre um terceiro, vítima de confronto entre policiais e criminosos, a imprensa e a sociedade civil cobram, e os governantes prometem sempre, um maior investimento em "inteligência", em clara referência ao emprego semântico equivocado ao qual fizemos menção.

Passamos agora a analisar as características de ambas as atividades como forma de contrastá-las.

3.1 Objeto.

Ambas as atividades, de ISP e a investigatória criminal, têm por objeto a análise do crime e do criminoso. Nisso reside a coincidência entre ambas, o que não implica, como amplamente explorado acima, uma mesma identidade ou ainda, que uma atividade possa constituir-se em substituta da outra.

3.2 Objetivos.

A ISP tem por objetivo produzir conhecimentos e informações para subsidiar o planejamento e execução de políticas de segurança pública (nível político-estratégico) bem como ações para prever, prevenir, neutralizar e reprimir atos criminosos de qualquer natureza (nível tático-operacional). No nível tático-operacional se inserem tanto as ações de polícia preventiva quanto as ações de polícia repressiva, estas últimas consubstanciadas por intermédio de investigações criminais, em regra.

Note-se aqui não uma coincidência quanto ao objetivo, mas um importante ponto de contato entre objetivos de ambas as atividades. A ISP pode vir a ser produzida para subsidiar a investigação criminal, trazendo elementos para que o Delegado de Polícia possa melhor direcionar suas investigações. Ao ponto que a investigação criminal também subsidia (ou ao menos deveria subsidiar) a ISP com os dados produzidos e colhidos no âmbito do Inquérito Policial, ainda que este seja um objetivo acessório, mas não menos importante.

O conhecimento produzido pela ISP para subsidiar a investigação tem caráter informativo e acessório, não deve ser inserido como diligência investigatória, sob pena de invalidar toda uma investigação e futura ação penal[12]. O objetivo da ISP, quando é destinada a subsidiar a investigação, é servir de conhecimento ao tomador de decisões (Delegado de Polícia) para orientar sua investigação. É instrumental, não sucedâneo.

O objetivo principal da investigação criminal é reunir indícios de autoria e provas de materialidade do crime, como forma de embasar eventual ação penal. Porém, no primeiro atendimento prestado aos comunicantes do crime, na confecção do Registro de Ocorrência, na qualificação e oitiva

[12] No HC 147.837/RJ, o Ministro Gilmar Mendes (STF) reconheceu a ilegalidade do uso das evidências obtidas por meio da técnica de infiltração de agente de inteligência, como se provas fossem em investigação policial.

dos envolvidos, na produção de provas periciais, dentre outras diligências investigatórias, importantes dados são colhidos para o bom êxito daquela investigação em particular, mas que também servem, em igual nível de importância, para que se previnam novas infrações penais, para que sejam elaboradas políticas públicas globais de prevenção, para que se possa impedir ou minorar a prática de delitos correlatos, para que se possam solucionar outros crimes ou que sejam usados no planejamento estratégico ou orçamentário das instituições policiais. É neste ponto que a investigação criminal subsidia a inteligência.

Assim, tanto a ISP, quanto a investigação criminal têm por um de seus objetivos o suporte mútuo.

3.3 Ações e Técnicas.

Ambas atividades se utilizam de técnicas em comum para busca, coleta e processamento de dados utilizados como matéria-prima de suas atividades. São exemplos dessas técnicas: a entrevista ou termo de declarações, a vigilância, a entrada, a infiltração, a gravação ambiental, o uso de softwares de análise de vínculo, dentre outras.

Nesse aspecto, um ponto importante a ser ressaltado é que a Investigação Criminal tem compromisso com a prova, enquanto a Inteligência de Segurança Pública tem compromisso com a convicção do analista (SCARPELLI, 2012).

Dessa feita, as restrições à coleta e busca de dados no âmbito da investigação criminal são muito maiores do que na atividade de inteligência. Naquela há limitações legais severas quanto à busca da verdade, sob pena de anulação, tendo em vista que está sempre sob perspectiva o direito à liberdade de alguém. Enquanto que na ISP, como o compromisso é com a convicção do analista essas limitações são menores e circunscritas de forma absoluta aos direitos e garantias fundamentais, como a inviolabilidade do domicílio e das comunicações telefônicas.

4 O SISTEMA DE INTELIGÊNCIA DA SECRETARIA DE ESTADO DA POLÍCIA CIVIL DO RIO DE JANEIRO (SISEPOL).

Um sistema é um conjunto de indivíduos que interagem entre si, tendentes a consecução de um ou mais objetivos comuns. Nesse sentido foi pensado o SISEPOL, para coordenar e integrar as

unidades da SEPOL no que concerne à atividade de inteligência, tendo por órgão central a Subsecretaria de Inteligência.

Segundo a Resolução SEPOL n.º 114 de 09 de março de 2020 (Anexo 1), todas as unidades da SEPOL estão aptas a fazer parte do SISEPOL desde que esta unidade se estruture para tanto e o Secretário de Estado de Polícia Civil transforme essa unidade em Agência de Inteligência (AI) por ato específico próprio. Até o momento a mencionada resolução não foi posta em prática por carecer de regulamentação.

Hoje, apenas as unidades da ponta (Delegacias de Polícia) e a Corregedoria Geral de Polícia funcionam como AI e estão formalmente aptas a fazer parte do Sistema. A Corregedoria, inclusive está posicionada como Agência Especial autônoma dentro da estrutura do SISPERJ, do qual a SSINTE também é órgão central.

4.1 O papel das delegacias de polícia na estrutura do SISEPOL.

As Delegacias de Polícia compõem a base da estrutura da SEPOL. Realizam a atividade-fim da Polícia Judiciária, ou seja, a atividade investigatória. É a face visível, é quem mantém a relação da instituição com os destinatários do serviço.

Hoje nós temos no Estado do Rio de Janeiro 186 (cento e oitenta e seis) Delegacias, espalhadas por 82 (oitenta e dois) municípios diferentes, sendo que nosso Estado possui 92 (noventa e dois) municípios.

Segundo a Resolução n.º 1001 de 30 de agosto de 2016 (Anexo 2), elaborada pela extinta Secretaria de Estado de Segurança Pública (SESEG), as Delegacias de Polícia são formatadas da seguinte forma: 1) um grupo de gestão técnico-operacional formado pelos Delegados Titulares, Assistentes e Adjuntos e 2) uma equipe de Apoio e Execução formada por um Grupo de Investigação de Plantão (GIP), um Grupo de Investigação Complementar (GIC), uma Seção de Inteligência Policia (SIP), uma Seção de Suporte Operacional (SESOP) e um Agente de Pessoal.

No primeiro grupo se encontram os gestores da unidade, as Autoridades Policiais, enquanto no segundo estão seus agentes, os executores. Dentre os grupos de agentes, temos os plantonistas (GIP), são os que dão o atendimento inicial e, conforme o caso, elaboram o Registro de Ocorrência ou auxiliam

na lavratura do Auto de Prisão em Flagrante. No GIC estão os agentes que dão sequencia à investigação. Na SIP estão os agentes responsáveis, dentre outras funções, pela atividade de inteligência. Na SESOP são feitos os trâmites administrativos da unidade, enquanto que o Agente de Pessoal trata dos assuntos inerentes aos recursos humanos.

4.2 A Seção de Inteligência Policial (SIP).

A SIP, como dito acima, é a responsável direta pela atividade de inteligência no âmbito das Delegacias de Polícia. É quem torna essa unidade uma Agência de Inteligência. Segundo o artigo 9º da Resolução SESEG n.º 1001/2016, são 16 (dezesseis) as suas atribuições, as quais transcreveremos abaixo textualmente. Cabe à SIP:

> I - executar a atividade de inteligência policial;
> II - executar atividade de identificação biométrica, datiloscópica e fotográfica, classificação, processamento e arquivamento de informações relativas aos investigados ou indiciados em investigações preliminares ou Inquéritos Policiais, assim como as medidas necessárias ao procedimento correlato em se tratando de adolescentes infratores;
> III - providenciar o pedido de anotação criminal quando determinado pelo Delegado de Polícia;
> IV - solicitar folha de antecedentes penais ao órgão oficial de identificação, informando o referido órgão dos detalhes do indiciamento, além de instruir os autos com os dados relativos aos antecedentes porventura existentes, quando determinado pelo Delegado de Polícia;
> V - receber, em caso de prisão em flagrante, a fiança arbitrada pelo Delegado de Polícia, a qual deverá ser imediatamente lançada no livro de fianças e repassada à SESOP para recolhimento aos cofres públicos por meio de guia oficial, desde que tais procedimentos não estejam sob a responsabilidade do núcleo de apoio cartorário;
> VI - acautelar e escriturar livro de fianças e seus respectivos valores, desde que tais procedimentos não estejam sob a responsabilidade do núcleo de apoio cartorário;
> VII - acautelar e manter atualizados os arquivos relativos às guias de pessoa presa ou apreendida, mandados de prisão, alvará de soltura, álbuns fotográficos e retratos falados;
> VIII - expedir pelo sistema informatizado e arquivar em pasta própria, as guias de pessoas presas ou apreendidas, mediante o devido recibo;
> IX - zelar pela inviolabilidade dos dados e informações registradas na SIP, somente fornecendo-as a pessoas ou órgãos legalmente autorizados, após ou por determinação do Delegado de Polícia;
> X - arquivar fotografia e retrato falado digitalizado no sistema, referente a pessoa ou local vinculado a infração penal, para imediata consulta em álbuns;
> XI - realizar consultas a órgãos do serviço público referentes a antecedentes penais do investigado ou indiciado, para fins de atualização do respectivo prontuário;
> XII - elaborar análise criminal ou estatística de ocorrências policiais, conforme determinação do Delegado de Polícia;
> XIII - analisar dados e informações de inteligência policial coletados nas investigações ou em outras fontes para fins de cadastro, relativos a fatos de interesse policial, investigados ou indiciados, bem como modalidades de delitos praticados em locais sensíveis da circunscrição;
> XIV - analisar preliminarmente informações relativas a patrimônio incompatível atribuído a servidores da UPAJ, conforme determinação do Delegado Titular;
> XV - inserir de imediato em sistema próprio, ocorrências relativas a veículos;
> XVI - manter as senhas de acesso aos principais sistemas sempre ativas e atualizadas.

Dessas 16 (dezesseis) atribuições, 10 (dez) são típicas da atividade de inteligência, as demais podem ser exercidas por outros profissionais. Devido à falta de cultura de Inteligência no âmbito da SEPOL, historicamente, os analistas da SIP, de uma maneira geral, sempre exerceram as atribuições que lhes eram cobradas pelos gestores, aquelas das quais dependia o andamento ordinário da unidade e que não possuem, via de regra, relação com a produção sistematizada de conhecimento.

Nos dias de hoje a situação se agravou. Não obstante o excesso de atribuições trazidas pela Resolução n.º 1001/2016, atualmente, poucas unidades dispõem de um servidor com dedicação exclusiva à SIP. Devido à carência de servidores, os analistas de inteligência da SIP exercem suas funções também em outros setores da Delegacia, a despeito da vedação expressa no artigo 5º da Portaria PCERJ n.º 775 de 05 de outubro de 2016 (Anexo 3). Para tanto, foram atribuídas senhas mistas (GIP/SIP; GIC/SIP; SESOP/SIP) para atuação no sistema operacional da SEPOL. Na verdade, a função de analista de SIP está praticamente extinta, o que há são servidores lotados em outras seções que fazem algumas funções da SIP quando estas são pré-requisito procedimental necessário para o regular andamento das investigações. Cabe aqui ressaltar que, nenhuma dessas funções podem ser qualificadas como atividade de inteligência no sentido estrito. Como exemplo temos a solicitação da folha de antecedentes penais do indiciado, o recebimento da fiança e a expedição da guia de preso.

CONCLUSÃO.

Com o desenvolvimento do presente artigo pudemos compreender a falta de cultura de Inteligência no âmbito da SEPOL, mais especificamente nas Delegacias de Polícia, o que gera uma baixíssima produtividade na busca, análise e disseminação de conhecimentos em todo seu Sistema de Inteligência. Para uma instituição que tem a informação como umas de suas principais matérias-primas, esse fato é muito preocupante, embora a solução esteja longe de ser complicada.

A atividade de inteligência é desconhecida da maior parte dos integrantes da instituição, que a confundem com a atividade de investigação, atividade-fim e principal produto da SEPOL. Além da confusão mencionada, existe o desconhecimento da finalidade e importância da atividade de inteligência.

O Policial (me refiro aqui indistintamente a todos os cargos), de uma forma geral, não tem a compreensão de que os dados produzidos em determinada investigação são úteis não só para aquele

caso específico, mas também para outros e ainda serve como auxílio para o planejamento macro de atribuição da administração superior.

As 186 (cento e oitenta e seis) Delegacias espalhadas por quase todos os bairros da Capital e em mais 81 (oitenta e um) outros Municípios oferecem uma capilaridade enorme e um consequente potencial na busca de informações de inteligência. Potencial este que não pode ser desperdiçado, principalmente num cenário onde estão presentes a insegurança generalizada, a violência e o crime organizado. Soma-se a isso o fato de que nosso Estado se encontra em dificuldades financeiras, onde recursos humanos e materiais são bastante escassos e precisam ser otimizados.

A SIP, seção voltada precipuamente para atividade de inteligência no âmbito das Delegacias de Polícia, de fato, de uma maneira geral, nunca foi utilizada para exercer seu papel, pelo total desconhecimento dos gestores do que seja a atividade de inteligência, sua utilidade e abrangência. Soma-se a isso, o grave problema de escassez de pessoal, que transformou os servidores da SIP em verdadeiros "faz-tudo".

Para se ter uma ideia de quão baixo é o fluxo de inteligência que parte das Delegacias para a SSINTE que é o órgão central do Sistema, em 2020 do total de 11.951 (onze mil novecentos e cinquenta e um) documentos de inteligência recebidos pela SSINTE, somente 395 (trezentos e noventa e cinco) foram oriundos das Delegacias de Polícia, ou seja, apenas 3,30 % (três vírgula trinta por cento) dos documentos que movimentam o órgão central de todo o Sistema de Inteligência, não só da SEPOL, mas de toda a Inteligência de Segurança Pública do Estado do Rio de Janeiro, partiram de uma Delegacia de Polícia (Documento Reservado).

Vale ressaltar que muitos desses documentos oriundos de Delegacias, ou foram confeccionados por Delegacias dirigidas por gestores que já possuíam conhecimento na área de Inteligência ou foram emitidos a pedido da própria SSINTE.

Ambas as atividades, de inteligência e investigatória, operadas de forma associada, são capazes de gerar enormes benefícios, principalmente no combate à criminalidade organizada.

Não podemos olvidar de que a mudança cultural se inicia pela formação tanto de quem já se encontra nos quadros da SEPOL, como dos recém chegados. Não obstante os esforços envidados nos últimos anos na melhoria do ensino policial, o ensino da Inteligência ainda não encontrou o devido

espaço na grade curricular da Academia de Polícia. Das últimas 04 (quatro) turmas de Delegados de Polícia que a ACADEPOL formou, somente uma teve aulas de ISP (Anexo 4).

A implementação de algumas medidas, relativamente simples, pode conduzir a SEPOL a um nível bem mais alto no que diz respeito à atividade de inteligência.

Uma primeira medida a ser tomada seria a designação de um policial com formação em Inteligência para compor a SIP de cada Delegacia de Polícia, mas direcionado única e exclusivamente às 10 (dez) atividades típicas de inteligência, conforme descrito no artigo 9º da Resolução SESEG n.º 1001/2016, conquanto outro servidor possa ser incumbido das demais atividades descritas no mesmo artigo.

Restaria a este Analista de Inteligência a incumbência de entrevistar pessoas, avaliar locais, reunir dados da Delegacia que possam ser úteis a outras esferas e produzir documentos de inteligência. Ficaria subordinado hierarquicamente ao seu Delegado Titular, enquanto que tecnicamente estaria subordinado à SSINTE, como já prescreve o parágrafo único do artigo 9º da Resolução SESEG n.º 1001/2016.

Para facilitar o fluxo entre os canais de inteligência, esses profissionais teriam acesso ao Sistema Apolo, sistema este utilizado pela SSINTE para o armazenamento e fluxo de dados e documentos de inteligência.

Não sendo possível num primeiro momento a lotação de um Analista de Inteligência em cada Delegacia, devido à escassez de servidores, ao menos poderiam ser lotados em cada Central de Flagrantes (Delegacias responsáveis pela avaliação e lavratura dos Autos de Prisão em Flagrante de determinada área) da Capital e da Baixada, bem como nas Delegacias consideradas de porte grande e extra grande de todo o Estado, como descrito Anexo 1 do Decreto Estadual n.º 43.624/2012.

Outra medida seria a inserção obrigatória da matéria Inteligência na grade curricular de formação dos Delegados de Polícia, gestores da instituição. Tal medida iria favorecer o incremento da cultura de inteligência, de forma a gerar um fluxo eficaz de dados e informações relevantes, seguras e oportunas aos tomadores de decisão da SEPOL presentes em todos os níveis. Não menos importante seria a formação dos agentes na matéria, mas no nível de especialização, àqueles que verdadeiramente possuem aptidão para dedicar-se à atividade de inteligência.

Como repetido algumas vezes neste trabalho, a Atividade de Inteligência não é um fim em si mesma, é atividade acessória que busca conferir efetividade, eficácia e eficiência ao organismo no qual ela é desenvolvida, para que os gestores tomem as melhores decisões possíveis dentro de seu campo de atuação. Após todo o diagnóstico aqui feito e as soluções apresentadas o que se espera é uma maior elucidação dos crimes complexos e um melhor enfrentamento às organizações criminosas, com a consequente geração de um ambiente de paz que favoreça um ambiente social e econômico saudável e frutuoso.

REFERÊNCIAS:

BRASIL. **Lei n.º 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**. Diário Oficial da União, Brasília, DF, 8 dez. 1999. Disponível em *<http://www.planalto.gov.br/ccivil_03/LEIS/L9883.htm>*. Acesso em: 20 abril de 2021.

RIO DE JANEIRO. **Decreto n.º 43.624 de 31 de maio de 2012. Aprova os Critérios de Distribuição de Efetivo das Polícias Civil e Militar do Estado do Rio de Janeiro, e dá outras providências**. Diário Oficial do Estado do Rio de Janeiro, Rio de Janeiro, RJ, 01 jun. 2012. Disponível em *<https://www.jusbrasil.com.br/diarios/37548974/doerj-poder-executivo-01-06-2012-pg-1>*. Acesso em: 20 abr. 2021.

SANTOS, Célio Jacinto dos. **Investigação Criminal e Inteligência: Qual a Relação?** Revista Brasileira de Ciências Policiais Brasília. v. 2, n. 1. jan/jun. 2011.

DEWEY, John. **Experiência e Natureza: Lógica: a Teoria da Investigação; Vida e Educação; Teoria da Vida Mora**l, São Paulo: Abril Cultural, Coleção Os Pensadores. 1980.

DUTRA, Luiz Henrique de Araújo. **Oposições Filosóficas: a Epistemologia e suas Polêmicas**, Florianópolis: Editora da UFSC. 2005.

PEREIRA, Eliomar da Silva. **Investigação Criminal: Uma Abordagem Jurídico-Científica**, Revista Brasileira de Ciências Policiais Brasília. v. 1, n. 1. jan/jun. 2010.

ANDRADE, Felipe Scarpelli. **Inteligência Policial: Efeitos das Distorções no Entendimento e na Aplicação**. Revista Brasileira de Ciências Policiais Brasília, v. 3, n. 2. jul/dez. 2012.

MINGARDI, Guaracy. **O Trabalho da Inteligência no Controle do Crime Organizado. Estudos Avançados**, v. 21, n. 61, p. 51-69, 1 dez. 2007. Disponível em: <*http://www.revistas.usp.br/eav/issue/view/750*>. Acesso em 24 maio de 2019.

LIMA, Renato Brasileiro de. **Manual de Processo Penal**: volume único. 5. ed. Salvador: JusPodivm. 2017.

GONÇALVES, Joanisval Brito. **Atividade de Inteligência e Legislação Correlata**. 5. Ed. Niterói: Impetus. 2017.

Andrade, Felipe Scarpelli. **Inteligência Policial: Efeitos das Distorções no Entendimento e na Aplicação**. Revista Brasileira de Ciências Policiais. Brasília, v. 3, n. 2. jul/dez. 2012.

CEPIK, Marco A. C. **Espionagem e Democracia: Agilidade e Transparência como Dilemas na Institucionalização dos Serviços de Inteligência**. Rio de Janeiro, Editora FGV. 2003.

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

PLATT, Washington. **A Produção de Informações Estratégicas**. Rio de Janeiro. Biblioteca do Exército, Livraria Agir Editora. 1974.

WOLOSZYN, André Luís. **Ameaças e Deságios à Segurança Humana no Séc. XXI: de Gangues, Narcotráfico, Bioterrorismo, Ataques Cibernéticos às Armas de Destruição em Massa**. 2. ed. Rio de Janeiro: Biblioteca do Exército. 2013.

DADOS DO AUTOR:

Robson da Costa Ferreira da Silva

É Especialista em Administração Pública pela Fundação Getúlio Vargas, Especialista em Gestão Estratégica, Processos e Projetos Integrados na Área de Segurança Pública pela COPPEAD/UFRJ, Especialista em Inteligência Estratégica pela Escola Superior de Guerra (ESG), Bacharel em Direito pela Universidade Católica de Petrópolis, Delegado de Polícia da Secretaria de Polícia Civil do Estado do Rio de Janeiro.

RISP
Revista de Inteligência de Segurança Pública
ISSN 2675-7168; 2675-7249

A RISP

A **Revista de Inteligência de Segurança Pública - RISP** (*ISSN 2675-7168; 2675-7249*) é uma publicação continuada, da Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro - ESISPERJ, idealizada como um ambiente de acesso ao conhecimento de forma oficial, objetiva e transparente e que visa divulgar manuais e estudos científicos, pesquisas atuais, alem das melhores e mais escorreitas práticas, contribuindo assim para a desmistificação do tema. A RISP é, destarte, voltada para a comunidade acadêmico-científica, profissionais do setor e mesmo a qualquer pessoa que tenha interesse em aprofundar conhecimentos na área de Inteligência, notadamente vinculados às questões da Segurança Pública.

MISSÃO

Qualificar os profissionais da Comunidade de Inteligência e manter atualizada a Doutrina de ISP, por meio da pesquisa e produção de conhecimento, visando potencializar a capacidade de atuação estatal na área finalística da Segurança Pública.

VISÃO

Ser referência em ensino, doutrina, pesquisa e extensão em ISP para a comunidade de inteligência.

VALORES

Produção de conhecimento em ISP; Valorização do ambiente democrático; Fortalecimento de rede; Integração; Profissionalização técnica; Respeito à diversidade; Interoperabilidade; Excelência científica e tecnológica.

RISP
Revista de Inteligência de Segurança Pública
ISSN 2675-7168; 2675-7249

Diretrizes para Autores

Os textos enviados devem ser produções intelectuais inéditas dos respectivos autores, devendo cuidar para que não haja inserção de conteúdo publicado sem menção da fonte, de modo a não ferir a política editorial adotada pela ESISPERJ e a ética científica.

Os textos devem ter como escopo a atividade de inteligência, com foco na atividade de Inteligência de Segurança Pública, podendo tomar como objeto todas as dimensões e aspectos inerentes à ISP.

O envio dos textos deve realizado para o e-mail: **risp.esisperj@gmail.com**, em *Word* dentro do prazo informado. No mesmo e-mail, deve ser encaminhado o Termo de Cessão de Direitos Autorais assinado e salvo em formato <.pdf>, além do arquivo contendo elementos pré-textuais. Visando facilitar esse processo, todos os modelos destes e outros documentos podem ser obtidos na página da ESISPERJ.

CONDIÇÕES GERAIS PARA SUBMISSÃO DE TEXTOS:

- A contribuição deve ser original e inédita, e não estar sendo avaliada para publicação por outra revista.
- As URLs para as referências devem ser informadas sempre que possível.
- O texto deve ser formatado de acordo com o modelo disponibilizado na página da ESISPERJ.
- O texto deve seguir os padrões de estilo e requisitos bibliográficos descritos e adotados pelo padrão vigente da ABNT.

Resenhas de livros também serão aceitas para publicação, observando-se as diretrizes previstas no tópico seguinte.

Diretrizes para Resenha

A resenha deve ser escrita para livros com até dois (2) anos de lançamento e que tenham como foco a atividade de inteligência, em especial, à ISP (Inteligência de Segurança Pública). Podendo ser escrita para livros em outros idiomas, resguardando-se a devida tradução para o Português (BR).

Os autores que tiverem sua proposição aprovada devem declarar que cedem os direitos autorais à Revista de Inteligência de Segurança Pública (RISP), podendo esta incluir o trabalho publicado em bases de dados públicas e privadas, no Brasil e no exterior. Devem ainda declarar que são o os únicos responsáveis pelo conteúdo do texto e que o mesmo não contem nada que possa ser considerado ilegal ou difamatório de terceiros.

As submissões em desacordo com as Instruções aos Autores não serão admitidas para avaliação e seus propositores serão devidamente comunicados.

CONDIÇÕES PARA SUBMISSÃO:

Como parte do processo de submissão, os autores são obrigados a verificar a conformidade da submissão em relação a todos os itens listados a seguir. As submissões que não estiverem de acordo com as normas serão recusadas e/ou devolvidas aos autores para adequação.

1. A contribuição deve ser original e inédita, e não estar sendo avaliada para publicação por outra revista; caso contrário, deve-se justificar em “Comentários ao Editor”.

2. O arquivo da submissão deverá estar nos formatos Microsoft Word, OpenOffice ou RTF, não podendo ultrapassar o limite de 2MB.

3. O texto deve usar espaço simples e fonte de 12-pontos, alem de itálico em vez de sublinhado (exceto em endereços URL). Figuras e tabelas deverão ser descritas e inseridas no decorrer do texto e não ao término do documento na forma de anexos.

4. O texto deverá seguir os padrões de estilo e requisitos bibliográficos descritos em Diretrizes para Autores, na página *online* sobre a Revista.

5. Ao menos um dos autores deve possui a titulação de doutor.

6. Em caso de submissão a uma seção com avaliação por pares (ex.: artigos), verifique se as instruções disponíveis em 'Assegurando a Avaliação Cega por Pares' foram corretamente seguidas.

DECLARAÇÃO DE DIREITO AUTORAL

Autores que publicam nesta revista concordam com os seguintes termos:

1) Autores mantêm os direitos autorais e concedem à revista o direito de primeira publicação, com o trabalho simultaneamente licenciado sob a Licença *Creative Commons Attribution* que permite o compartilhamento do trabalho com reconhecimento da autoria e publicação inicial nesta revista.

2) Autores têm autorização para assumir contratos adicionais separadamente, para distribuição não-exclusiva da versão do trabalho publicada nesta revista (ex.: publicar em repositório institucional ou como capítulo de livro), com reconhecimento de autoria e publicação inicial nesta revista.

3) Autores têm permissão e são estimulados a publicar e distribuir seu trabalho *online* (ex.: em repositórios institucionais ou na sua página pessoal) a qualquer ponto antes ou durante o processo editorial, já que isso pode gerar alterações produtivas, bem como aumentar o impacto e a citação do trabalho publicado.

Juntem-se a nós!