O Emprego das Fontes abertas no Âmbito da Atividade de Inteligência Policial

Sara Souza Leite
Departamento de Polícia Federal - Brasil

RESUMO

O presente trabalho discorre sobre o emprego das fontes abertas na atividade de inteligência policial. Nos últimos anos, houve um avanço considerado nos sistemas de comunicação e de tecnologia, o que causou uma mudança significativa no ambiente informacional. Todavia, os serviços de inteligência no Brasil não acompanharam esse movimento, mantendo um padrão que não atende mais a todas as demandas. Essa pesquisa demonstra que é imperiosa a reforma nas estruturas das comunidades de inteligência, a fim de investir e desenvolver uma área voltada para o serviço de *Open Source Intelligence* (*OSINT*). Trata-se de uma análise sobre os objetivos e as necessidades atuais decorrentes do serviço de inteligência policial, a função da *OSINT* na atividade de inteligência policial, o valor de uma fonte aberta, seus atributos e suas limitações, breve histórico da atividade de inteligência de fontes abertas nos EUA e como as fontes abertas poderiam ajudar na prevenção da corrupção.

Palavras-chave: Inteligência Policial. Fonte aberta. *Open Source Intelligence (OSINT).* Valor da *OSINT*. Limitações. Prevenção da corrupção.

1. Introdução

O cenário de corrupção e violência instalado e vivenciado pela sociedade brasileira tem comprovado a necessidade cada vez maior do aprimoramento das instituições policiais e em especial dos seus profissionais.

A evolução tecnológica ocorrida nos últimos anos possibilitou um aumento gigantesco de informações em domínio público. Permitiu, inclusive, o acesso e a expansão de forma rápida e prática. Em decorrência dessa modernização e da utilização massiva das tecnologias de informação e de comunicação, as fontes abertas tornaram-se um meio inesgotável de conhecimento.

Recebido em 01 de julho de 2014.
Aceito em 11 de novembro de 2014.
Brasília, v. 5, n. 1, p. 11-45, jan/jun 2014.
ISSN 2178-0013
ISSN Eletrônico 2318-6917

Hoje existe uma diversidade de dados disponíveis capazes de auxiliar a atividade de inteligência. Essas informações podem oferecer material relevante quando bem processadas e analisadas. Neste ambiente concentram-se informações provenientes de variadas fontes. A *OSINT* (*open source intelligence*) assume papel fundamental na coleta de dados. Através dela é possível obter documentos oficiais não restritos, acompanhar a dinâmica econômica, social e política de um país, monitorar as tendências da mídia e as produções técnico-científicas (BEST, 2008).

Muitas informações disponibilizadas na internet podem contribuir, inclusive, para prevenir e combater a corrupção. De maneira preventiva, exercendo um controle social sobre os atos dos administradores públicos. De forma educativa, difundindo as boas práticas na administração de bens e recursos públicos (MENDES; MORESI e SILVA, 2010, p. 5). De forma repressiva, compartilhando e difundindo com a polícia judiciária as denúncias graves oriundas de fontes abertas.

Na verdade, a difusão em meio eletrônico de diversas informações não é suficiente para coibir a prática de atos de aproveitamento ilícito por parte de indivíduos e organizações, necessitando do apoio de outros instrumentos de enfrentamento. Contudo, as fontes abertas são um meio importante que ajuda a mitigar os efeitos danosos da corrupção na sociedade, como se verá mais adiante.

As redes sociais ancoradas na internet possuem um papel de destaque entre as formas de comunicação existentes. Embora ocorram em múltiplas variedades, todas possuem o dado, a imagem e a informação como legados.

O fruto da coleta baseada em uma fonte aberta pode identificar qual a estratégia seguinte para execução de uma ação, para a obtenção do dado negado[1]. Além disso, pode complementar uma informação existente, direcionar e assessorar o tomador de decisão tanto em nível estratégico, como operacional e tático, contribuindo de forma substancial para a atividade de inteligência.

É preciso entender e saber empregar a *OSINT* no âmbito dos interesses do tomador de decisão e das operações de inteligência. Para isso, é necessário analisar o dado, a sua origem, confrontá-lo com outras informações já existentes, a fim de produzir material suficiente ao conhecimento.

1 Dado negado são informações não disponibilizadas ao público, ou seja, de acesso restrito ou protegido, incluindo-se, nesse último caso, as chamadas "informações classificadas".

Antes de adentrar no tema proposto sobre as fontes abertas, a seção 2 busca traçar parâmetros a respeito da função da inteligência policial. Em seguida, serão discutidos os conceitos e o desenvolvimento de uma atividade de inteligência baseada numa *OSINT*. Ainda na seção 3, foram inseridos dois tópicos, quais sejam, um que discute o valor de uma fonte aberta para a atividade de inteligência e o outro, um breve histórico sobre a evolução da *OSINT* nos Estados Unidos, como forma de compreender e analisar a sua gigantesca estrutura, amplitude e finalidades, além de enfatizar o seu valor e importância para os serviços de inteligência. Na seção 4, serão apresentadas as limitações existentes em se trabalhar com fontes abertas e, ao final, como a *OSINT* pode ser útil na prevenção da corrupção no Brasil.

O escopo do presente trabalho é expor a importância do emprego das fontes abertas para a atividade de inteligência policial, sobretudo em tempos atuais, onde cada vez mais se depende dos meios de comunicação, em especial a internet, para interagir, trabalhar, pesquisar e se comunicar.

2. Função da Inteligência Policial

Antes de adentrarmos no tema do emprego das fontes abertas, importante tecermos alguns parâmetros da atividade de inteligência policial.

A inteligência policial no Brasil remonta antes mesmo da inteligência clássica. Getúlio Vargas, em 1933, criou a Delegacia Especial de Segurança Política e Social (DESPS), transformada, em 1944, em Divisão de Polícia Política e Social (DPS). Da sua origem até 1964 este órgão atuou na vigilância e na repressão de adversários do regime vigente, repassando tal tarefa ao Serviço Nacional de Informações (SNI), no início do regime militar. Nesse período, a inteligência policial se desenvolveu sob a ótica política, de perseguição aos dissidentes do governo (BRITO, 2006).

Com o fim do regime militar em 1985 e com a promulgação da Constituição de 1988, as instituições policiais, incluindo o Departamento de Polícia Federal (DPF), passam por diversas mudanças relativas à área de inteligência. Neste processo, a atividade de inteligência policial, que antes era focada no interesse político, volta-se para o crime organizado, para o contraterrorismo e suas vertentes, como a lavagem de dinheiro, narcotráfico, sonegação fiscal (CEPIK, 2003).

Essa mudança de paradigma, todavia, manteve uma imprecisão dos limites de atuação dos órgãos como polícia e como analistas de inteligência, muitas vezes se mesclando.

A linha de atuação de um serviço de inteligência policial e da atividade de investigação criminal é muito tênue, mas não se confundem. Celso Ferro (2008, p. 9) apresenta um conceito de inteligência policial, onde fica clara a distinção entre a atividade de inteligência e a investigação policial:

> *[...] atividade que objetiva a obtenção, análise e produção de conhecimentos de interesse da segurança pública no território nacional, sobre fatos e situações de imediata ou potencial influência da criminalidade, atuação de organizações criminosas, controle de delitos sociais, assessorando as ações de polícia judiciária e ostensiva por intermédio da análise, compartilhamento e difusão de informações.*

O escopo da inteligência policial não é produzir provas, o que a difere de uma investigação policial. Contudo, na produção de conhecimentos voltados para a área criminal podem surgir fatos ou situações relacionados a supostos crimes. Dentro desse contexto, não existe óbice em compartilhar esse conhecimento com a unidade de polícia judiciária responsável para a sua devida apuração ou, havendo investigação ou processo em curso sobre os mesmos fatos, corroborar as provas até então produzidas.

Como bem ressaltou Denilson Feitosa Pacheco (2005, p. 3) sobre o assunto:

> *Quanto à validade das provas obtidas na busca (operação de inteligência), todas as "provas" obtidas pelas atividades de inteligência em geral e pelas operações de inteligência podem, em princípio, ser utilizadas na investigação criminal, desde que sujeitas às limitações de conteúdo e de forma estabelecidas pela lei processual penal. Essa possibilidade de utilização decorre do princípio da liberdade probatória do processo penal.*

De acordo com o Manual de Inteligência Policial (BRASIL, 2011, vol. 1, p. 6), inteligência policial é:

> *[...] a atividade de produção e proteção de conhecimentos, exercida por órgão policial, por meio do uso de metodologia própria e de técnicas acessórias, com a finalidade de apoiar o processo decisório deste órgão, quando atuando no nível de assessoramento, ou ainda, de subsidiar a produção de provas penais, quando for necessário o em-*

> *prego de suas técnicas e metodologias próprias, atuando, neste caso, no nível operacional.*

Já a Resolução nº1, de 15 de julho de 2009, que regulamenta o Subsistema de Inteligência de Segurança Pública (SISP), define que inteligência policial é, *in verbis*:

> *[...] o conjunto de ações que empregam técnicas especiais de investigação, visando a confirmar evidências, indícios e a obter conhecimentos sobre a atuação criminosa dissimulada e complexa, bem como a identificação de redes e organizações que atuem no crime, de forma a proporcionar um perfeito entendimento sobre a maneira de agir e operar, ramificações, tendências e alcance de condutas criminosas.*

Os diversos conceitos acima ilustrados mostram que o tema ainda é bastante controverso, ora voltado para a produção de provas, ora assumindo contornos de inteligência de segurança interna, voltada para ações de segurança pública[2].

Denilson Feitosa Pacheco (2010, p. 5) afirma que:

> *Há um grande esforço para se adequar (melhor se diria: complementar) a inteligência dita de estado (ou seja, relativa à segurança nacional, isto é, do Estado e da sociedade como um todo) à área de segurança pública. A inteligência de segurança pública ou inteligência criminal é um conceito em construção.*
>
> *Nessa linha de adjetivação do termo inteligência, poderíamos ainda subdividir a inteligência de segurança pública (ou inteligência criminal) em inteligência policial, para a inteligência desenvolvida no âmbito das Polícias, e inteligência prisional (ou, mais restritivamente, inteligência penitenciária), para a desenvolvida no âmbito dos estabelecimentos prisionais.*

2 **Inteligência de Segurança** (*security intelligence*), também denominada **Inteligência Interna ou Doméstica**, está relacionada com as ameaças internas que comprometem a segurança do Estado, de suas instituições e da sociedade, como subversão, espionagem, violência politicamente motivada por instabilidade econômica, política e social (GONÇALVES, 2010, p. 43).
Inteligência de Segurança Pública pode ser definida como: [...] *o exercício permanente e sistemático de ações especializadas para a identificação, acompanhamento e avaliação de ameaças reais ou potenciais na esfera de Segurança Pública, basicamente orientadas para produção e salvaguarda de conhecimentos necessários para subsidiar os governos federal e estaduais a tomada de decisões, para o planejamento e à execução de uma política de Segurança Pública e das ações para prever, prevenir, neutralizar e reprimir atos criminosos de qualquer natureza ou atentatórios à ordem pública.* (DNISP, 2009, p. 10). O Decreto 3695/2000, que instituiu o subsistema de inteligência de segurança Pública (SISP), dispõe em seu art.2º, parágrafo 3º, que os órgãos integrantes do SISP têm por missão: *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.*

A inteligência aplicada aos serviços de polícia judiciária e segurança pública, em geral, deve se preocupar com a prevenção do crime, através de estudos que identifiquem o *modus operandi* das principais organizações criminosas, os comandos hierárquicos, mapeamento de rotas e locais, principais focos de criminalidade, novas tendências e estatísticas (GOMES, 2009). Subsidiariamente, podem assessorar uma investigação policial e vice-versa. A inteligência policial deve se preocupar, portanto, em produzir conhecimento de interesse de atividade policial.

Dentro dessa linha de raciocínio, inteligência policial é a atividade de produção e proteção de conhecimentos voltados para a atividade policial, dentre as quais sobre fatos e situações de imediata ou potencial influência na criminalidade, *modus operandi* das organizações criminosas, assessorando as ações de polícia judiciária, com o intuito de prevenir e maximizar os resultados no combate ao crime e instrumentalizar os gestores na tomada de decisão.

Ela deve se preocupar também com o bom êxito das atividades fim da polícia judiciária, ou seja, implementar estudos baseados na eficácia do inquérito policial e nos resultados advindos dos processos criminais. Gerir de forma adequada o bem público significa trabalhar para o melhor resultado.

A atividade de inteligência, de modo geral, preocupa-se em produzir conhecimento. Esse conhecimento é derivado de informações, informe, fato ou dado que foi selecionado, avaliado, interpretado e, então, expresso de tal forma que evidencie sua importância para determinado problema (PLATT, 1962). A inteligência policial evoluiu por um lado, mas deixou uma aresta no processamento e na análise da informação.

Como bem expôs Vladimir Brito (2006, p. 138):

> *Ao contrário das organizações de Estado, ou da I. C. (*Inteligência Competitiva*)*[3]*, as instituições responsáveis pela inteligência policial no Brasil tendem a subutilizar o momento do processamento e análise de informações, deixando de maximizar sua ação, uma vez que uma parcela significativa do que é coletado tende a não ser aproveitado.*
>
> *Com a proliferação de recursos de tecnologia da informação, além das várias disciplinas de coleta permitidas ao Estado, tende-se a ob-*

3 Expressão em grifo acrescentada pela autora

> *ter um volume significativo de dados, contudo os mesmos não são processados adequadamente e consequentemente não chegam sequer a serem analisados e inseridos em um contexto mais amplo.*

As investigações policiais e os processos criminais são de extrema relevância para o serviço de inteligência policial na medida em que são capazes de produzir dados (número de operações, investigados e presos, perfil, rota financeira da organização, *modus operandi*) que vão auxiliar na produção do conhecimento estratégico voltado para o estudo e a prevenção do crime. Essas informações, contudo, muitas vezes acabam sendo desperdiçadas e não aproveitadas pelos órgãos de inteligência.

A utilização de um grande volume de dados e informações não caracteriza a atividade de inteligência. Essas informações devem ser trabalhadas de forma adequada para possibilitar um estudo de padrão criminal, bem como tendências futuras. Deve existir um ambiente propício para a real utilização dessas informações, como forma de maximizar os resultados no combate ao crime e instrumentalizar os gestores na tomada de decisões, como já dito.

Nesse ambiente, inclui-se a formação de parcerias, inclusive com o setor privado. Com o advento de novas tecnologias e com a disponibilidade de uma infinidade de informações, oriundas especialmente da internet, grandes empresas multinacionais dependem, cada vez mais, da inteligência competitiva para tomar decisões e proteger seu legado. O resultado é um número crescente do setor comercial privado em investimentos e desenvolvimento de ferramentas de *OSINT* (BEST, 2008).

Vladimir Brito (2006, p. 39) contextualiza bem este exemplo, voltado para a inteligência policial:

> *Considerando-se que as empresas privadas historicamente têm uma série de restrições ao acesso e obtenção de informação, que as instituições de inteligência estatal não possuem, estas primeiras desenvolveram instrumentos para maximizar a utilização das informações disponíveis, geralmente obtidas a partir de fontes abertas ao público, que não precisam de autorização legal para sua utilização. Neste sentido a referida Inteligência Competitiva – I. C. pode representar novas experiências que podem ser utilizadas pelas instituições de combate ao crime, a exemplo do uso de fontes abertas, ou seja, fontes cujo acesso não sofre restrição legal, sendo o acesso franqueado a sociedade.*

Como se constata, é necessário investir no processamento e análise das informações, interagir com os diversos órgãos de inteligência, organizações e empresas privadas, especialmente aquelas que possuem sistemas de tecnologia mais avançados nessa área. É preciso maximizar o uso das fontes abertas, criar padrões e procedimentos próprios como forma de organizar e gerir o conhecimento produzido, adotando modelos que se adequem às necessidades funcionais de cada instituição.

Fregapani (2003, p. 166) afirma que:

> *Todas as instituições relacionadas com segurança, inclusive os serviços de Inteligência, ao se reorganizarem, procuram responder algumas perguntas: 1- Quais são as prioridades da nossa missão? 2- Como poderemos cumprir as nossas missões? 3- Quais os óbices e as ameaças ao cumprimento de nossas missões? 4- Que modificações devem ser feitas nos procedimentos, nos meios e na estrutura para sermos bem sucedidos nas missões?*

Em suma, é preciso rever o papel da inteligência policial atual, seu desempenho, suas metas e seus limites. É preciso aprimorar os sistemas de inteligência de forma a potencializar a produção do conhecimento e desenvolver formas adequadas e seguras de gestão das informações, visando cumprir com eficiência os objetivos propostos.

3. Inteligência de Fontes abertas

Inteligência é, em uma definição ampla, "toda informação coletada, organizada ou analisada para atender as demandas de um tomador de decisões qualquer" (CEPIK, 2003, p. 29).

Sherman Kent apresenta uma definição clássica, descrevendo inteligência sob três aspectos (MORESI *et al.*, 2010, p. 5):

- *como produto: é a representação do resultado do processo de produção de conhecimento, atendendo a demanda do tomador de decisão, tornando o resultado obtido por meio do processo de inteligência, um produto de inteligência;*
- *como organização: apresenta as estruturas funcionais, que tem como missão crítica a obtenção de informações e a produção de conhecimento de inteligência, podendo ser caracterizados como os operadores da inteligência;*

- *como atividade ou processo: refere-se aos caminhos pelos quais certos tipos de informação são requeridos, coletados, obtidos, analisados e difundidos. Determinação dos procedimentos para a obtenção de determinados dados, em especial aqueles protegidos.*

Quando se fala em inteligência de fontes abertas devemos pensar na informação ou dado que foi coletado, selecionado, analisado e expresso de tal forma que evidencie a sua importância para determinado problema (PLATT, 1962). O conceito de *OSINT*, portanto, não se confunde com o de fontes abertas.

Marco A. C. Cepik (2003, p. 51) define *OSINT* como a análise baseada na:

> *[...] 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).

A produção do conhecimento, de forma geral, envolve o chamado "ciclo ou processo da inteligência" que, tradicionalmente, consiste num processo de repetição ancorado em cinco etapas básicas (JOHNSTON, 2005, p. 46):

- *Planejamento e direção: abrange a gestão de todo o esforço do processo e envolve, em particular, a determinação dos requisitos de escolha baseados nas solicitações dos clientes.*
- *Coleta: refere-se à coleta de dados brutos com o intuito de atender à demanda pretendida. Esses dados podem ser obtidos de fontes abertas e/ou secretas.*
- *Processamento: refere-se à conversão dos dados brutos em um formato em que os analistas possam usar.*
- *Análise e produção: descreve o processo de avaliação de dados de confiabilidade, validade e relevância, integrando-os e analisando-os, convertendo o produto deste esforço em um*

> *todo significativo, que inclui avaliações de eventos e implicações das informações recolhidas.*
>
> - *Disseminação: é a difusão do conhecimento produzido ao seu público-alvo.*

Frisa-se que não existe um consenso geral e uniforme na doutrina de quantas etapas são necessárias para execução do ciclo da inteligência. Cepik enumera até dez etapas, enquanto Lowenthal assinala sete fases do processo de inteligência (GONÇALVES, 2010, p. 67). Todavia, o objetivo do presente trabalho não é explicitar os diferentes ciclos, mas apenas expor um processo básico que é desenvolvido na produção do conhecimento e que deve ser adaptado conforme as finalidades de cada setor e das suas demandas.

O conceito de *OSINT* trabalha com a coleta de informações, passando por todo ciclo da inteligência e o resultado será o produto de um raciocínio elaborado e contextualizado a respeito de um fato ou ação (MENDES; MORESI e SILVA, 2010). O produto de uma *OSINT* geralmente é divulgado a um público seleto, a fim de abordar uma questão específica.

Informações disponibilizadas publicamente não possuem nenhum valor como produto de inteligência se não é filtrada, analisada, processada e validada. Os analistas de inteligência devem ser treinados para descobrir fontes adequadas de informações. Em seguida, devem discriminar quais dados são relevantes para uso dentro da demanda requerida (MINAS, 2010).

Pode ocorrer, contudo, em alguns casos, que o ciclo de produção do conhecimento seja quebrado em virtude de informações relevantes coletadas, especialmente de uso diplomático ou militar imediato. Neste caso, as informações irão direto ao usuário final, sem passar pela etapa de análise e produção (CEPIK, 2003), sob pena de ferir o princípio da oportunidade. Trata-se, todavia, de uma exceção à regra, em face das peculiaridades existentes próprias das fontes abertas.

Dentre o rol de informações que podem ser coletadas pelas fontes abertas, Lowenthal (MORESI *et al*., 2010, p. 7) enumera:

> *a) Mídia: jornais, revistas, rádio, televisão e informação baseada em computador;*
>
> *b) Dados públicos: relatórios do governo, orçamentos públicos,*

> *dados demográficos, audiências públicas, debates legislativos, conferências de imprensa, discursos, avisos de segurança marítima e aeronáutica, estatísticas;*
>
> *c) Profissional e acadêmica: conferências, simpósios, congressos, associações profissionais, trabalhos acadêmicos e especialistas temáticos;*

Brito (2006, p. 152-153) acrescenta, ainda:

> *d) "Literatura cinzenta": informações com distribuição limitada, tais como pesquisas científicas e tecnológicas, trabalho acadêmicos, dentre outros materiais.*
>
> *e) Observação de terceiros: coleta de informações a partir de pilotos de avião amadores, monitores e observadores de comunicações de rádio, turistas e aventureiros, dentre outros;*
>
> *f) Comunidades baseadas na Web e conteúdo gerado por usuários individuais: redes sociais, sites de compartilhamento de vídeo, wikis, blogs e folksonomias;*
>
> *g) Informações geoespaciais: imagens de satélite, mapas, atlas, dentre outros.*

Além da mídia tradicional disponibilizada em fontes abertas, a internet permitiu também a expansão nas áreas de IMINT (inteligência de imagens) e SIGINT (inteligência de sinais) com versões abertas de variados programas e dados (MERCADO, 2007).

As facilidades advindas do progresso tecnológico, também impuseram a necessidade de qualificar a informação, sob pena de sobrecarregar o decisor, desviando a atenção do foco pretendido (MENDES e MORESI, 2012). Dentro dessa linha de raciocínio, para melhor compreensão dos conceitos, *OSINT* não se confunde com ***Open Source Data*** (*OSD*) e *Open Source Information* (*OSIF*). Estes dois últimos constituem matéria prima na formação da *OSINT*.

OSD é um dado sem edição, que não foi processado. Ele se encontra no seu estado bruto e são denominadas fontes primárias. Pode ser uma fotografia, uma carta pessoal, uma gravação. Estes dados brutos precisam se submeter a uma elaboração a fim de alcançar o próximo nível, a *OSIF*. Assim, quando esses dados são analisados, editados e publicados transformam-se em informação disponível. Todas essas fontes secundárias constituem a *OSIF* (NATO, 2002, p. 2-3).

É importante traçar objetivos e prioridades para não se perder nesse oceano de fontes abertas. Cada nação possui situações, objetivos e ameaças diferentes. Célio Fregapani (2003, p. 167) cita, por exemplo, os Estados Unidos, "tendo como objetivo manter a hegemonia mundial, certamente sentem como ameaças aos seus objetivos nacionais o terrorismo, a proliferação nuclear, a carência de certas matérias-primas e a concorrência comercial."

No caso da atividade de inteligência policial, as fontes abertas devem fornecer material necessário capaz de produzir conhecimento de interesse de atividade policial, ou seja, sobre questões voltadas para a criminalidade, estatísticas, contrainteligência, contraespionagem, medidas de prevenção e combate ao crime, como já mencionado no primeiro capítulo.

Um dos pontos cruciais da *OSINT* é o analista. Ele deve ser um especialista, com profundo conhecimento do problema que está sendo abordado. Coletores e analistas devem ser capazes de reduzir os déficits analíticos causados por tentativas de desinformação[4] ou pela má qualidade do dado. Além disso, uma notícia de jornal, por exemplo, pode ser interpretada de diversas formas por um analista da CIA, da Agência Brasileira de Inteligência (ABIN) ou do *Mossad*, dependendo de suas prioridades, de seus interesses e de seus parâmetros (AFONSO, 2006).

Diversos documentos da CIA, por exemplo, afirmaram erroneamente que o Iraque possuía armas de destruição em massa. Em verdade, os analistas acreditaram que os dados de armas do Iraque tinham sido confirmados por várias fontes, quando na verdade ele tinha vindo de uma única fonte, mas descrito de várias maneiras (PINCUS, 2004).

As comunidades de inteligência no Brasil devem se preocupar, ainda, em capacitar os analistas em línguas estrangeiras ou cooptar servidores já habilitados. As novas diretrizes da inteligência atual – prevenção e repressão ao crime organizado, contraterrorismo – exige do analista conhecimento abrangente. Stephen C. Mercado (2007, p. 5) revela que saber línguas estrangeiras é a chave de exploração da *OSINT.* Além disso, a maioria dos programas e *softwares* disponíveis para se trabalhar com *OSINT* não possui versão em português, sendo o padrão em inglês.

4 Desinformação: conceito no capítulo 3 – OSINT e suas Limitações.

O volume crescente de dados disponíveis exige o uso de ferramentas de *software* avançadas que permitem aos analistas lidarem com o excesso de informação (BEST, 2008). Um simples dado não faz sentido dentro de um contexto mais amplo. É preciso que haja a junção dessas informações para a identificação de fatores e tendências que, de forma isolada, passariam despercebidos. Nas palavras de Cláudia Coutinho (2011): "o que faltam não são dados, mas a visualização inteligente deles."

A obtenção do conhecimento através de uma fonte aberta exige, como se vê, implementação de sistemas e investimento em tecnologia, estrutura adequada e mão de obra qualificada para exercer essa função.

Por conseguinte, de nada adianta ter o maior e mais eficiente aparato em tecnologia, os melhores analistas, se os serviços de inteligência não se interagirem, nem se comunicarem. O atentado de 11 de setembro é o melhor exemplo disso. Os Estados Unidos colhiam dados através de seus sistemas eletrônicos e telefonia interurbana de tudo que continha palavras chaves como *bomba, terrorismo, martírio, atentado* e outras. Eram tantos dados que os analistas não conseguiam processar tudo em tempo hábil e oportuno. A escola de pilotagem onde os futuros suicidas treinaram havia informado à CIA, que produziu um memorando interno alertando para o grande número de islâmicos freqüentando estes cursos. O *Federal Bureau of Investigation* (*FBI*) possuía outras informações e o Departamento de Imigração também. Bin Laden, três semanas antes, anunciou que ele e seus partidários fariam um ataque sem precedentes nos EUA devido ao apoio que o governo americano dava a Israel. A CIA sabia disso e o FBI também. Tudo era tão compartimentado que uma agência não sabia dos dados das outras. Elas não se comunicavam e não alertaram as companhias aéreas das eventuais ameaças (FREGAPANI, 2003).

Nesse novo modelo proposto (da produção do conhecimento através de uma área especializada em *OSINT*) é preciso se ater que, para o seu perfeito equilíbrio, é primordial uma gestão eficiente do conhecimento, a difusão e a interação entre os diversos órgãos. Nesse aspecto, Rodrigo Carneiro Gomes (2009, p. 128-129) ilustra bem a questão:

> *Há bancos de dados institucionais da Polícia Civil, Polícia Rodoviária Federal, Polícia Militar, Exército, Marinha, Aeronáutica, Abin, Detran, bancos de dados policiais das delegacias especializadas em lavagem de dinheiro, imigração ilegal, assalto a banco e, ainda, os não-policiais como os da Receita Federal, Dataprev/INSS,*

> *CNIS,* ***mas os setores responsáveis pelo gerenciamento dos dados respectivos não interagem, o que gera uma enorme quantidade de dados perdidos e pouco trabalhados.*** *[...]*
>
> *O ex-Secretário de Segurança de Guarulhos, a fim de reafirmar o seu posicionamento, invoca o exemplo paulista: "A Polícia Militar tem seu grupamento de inteligência, com status de batalhão, que é a P2, e cada batalhão tem sua própria unidade de P2. Na Polícia Civil existe o Dipol (Departamento de Inteligência Policial). No Departamento de Narcóticos (Denarc) também existe uma divisão de inteligência, da mesma forma que no Deic, departamento que deveria enfrentar o crime organizado, mas cuida basicamente de crimes contra o patrimônio. Com freqüência, os departamentos de polícia do interior também têm seus setores de inteligência.* ***Mesmo assim, cada vez que ocorre uma rebelião nos presídios ou um ataque contra a polícia, os órgãos policiais são pegos desprevenidos. Ou seja, existem muitos órgãos e pouca inteligência.****" (grifo nosso)*

Resumidamente, como dito alhures, são requisitos básicos para uma atividade de inteligência baseada em fontes abertas:

- **Mineração e cruzamento de dados através de** *softwares* **específicos** – a mineração de dados é o termo coletivo usado para dezena de técnicas que retiram informações de grande volume de dados e as transformam em algo significativo. Hoje existem diversos *softwares* de *data mining* (mineração de dados) disponíveis gratuitamente no mercado.

- **Servidores qualificados** – a vantagem competitiva entre os serviços de inteligência não está centralizada somente na informação, mas na capacidade dos analistas de produzirem um conhecimento com alto valor agregado e que atenda plenamente as demandas do usuário.

- **Gestão eficiente do conhecimento** – as informações devem ser trabalhadas de forma adequada para possibilitar o seu acesso e pronto uso, visando o estudo de padrões, perfis e tendências criminais, que vão culminar em ações e políticas de combate ao crime.

- **Difusão oportuna** – é importante atentar para a adequação do processo de produção do conhecimento e a sua difusão em tempo oportuno.

- **Interação entre os diversos órgãos e sistemas** – quanto mais os órgãos de inteligência se interagirem e seus sistemas se comunicarem, melhor serão os resultados voltados para a diminuição da criminalidade.

- **Troca de conhecimento com acadêmicos e setores privados** – é preciso conhecer, discutir e debater sobre novas tecnologias voltadas para a área de *OSINT*. Além disso, é importante saber aproveitar de forma mais eficiente as ferramentas já disponíveis, em benefício da atividade de inteligência policial.

Nesta nova era, é imprescindível o desenvolvimento da atividade de inteligência baseada em *OSINT* como forma de enfrentar os desafios modernos. Isto não significa que a atividade de inteligência obtida através do dado negado ou de técnicas especiais de investigação[5] será relegada. Na verdade, ambas se complementam e tornam o produto final da inteligência mais claro e preciso quanto às necessidades de seu cliente.

3.1 O VALOR DAS FONTES ABERTAS

A revolução na tecnologia da informação tornou as fontes abertas mais acessíveis, onipresentes e valiosas. Podem-se coletar importantes dados com maior facilidade e menor custo do que nunca. A *OSINT*, hoje, é parte essencial da atividade de inteligência e contribuinte indispensável para o conhecimento produzido devido a sua compatibilidade com seu ambiente global (MINAS, 2010).

Percebe-se, todavia, que ainda existe uma visão equivocada de que uma informação adquirida por meios "secretos" é mais importante ou "valiosa" do que aquela obtida por fontes abertas ou disponíveis (MERCADO, 2004). O ex-Presidente Nixon uma vez menosprezou a CIA, em palavras que captam o erro comum (MERCADO, 2004, p. 1): "Para que eles servem? Eles tem mais de 40.000 mil pessoas que ficam lendo jornais?"

É importante saber que a fonte aberta assume papel relevante na atividade de inteligência. Por se tratarem de dados disponíveis, não quer dizer que não possuam credibilidade. Ao contrário. Muitos desses dados atualmente ser-

5 De acordo com Antônio Sintra, *o conceito de técnicas especiais de investigação criminal, engloba a actividade policial dissimulada, de natureza confidencial, ou até secreta, que é desenvolvida com a finalidade de obter fluxos de informação tratada (intelligence) respeitante a actividades de pessoas suspeitas e/ou de recolher material probatório resultante de sua participação em práticas delituosas, a nível individual e/ou no seio de grupos criminosos organizados, com destaque para as condutas que integram as definições legais de terrorismo, criminalidade violenta, especialmente violenta e altamente organizada, mediante recurso a adequados meios humanos e/ou técnicos* (SINTRA, 2010, p.70). As técnicas especiais de investigação abrangem, dentre outras, a infiltração policial, a entrega vigiada ou controlada, a interceptação, a captação ambiental e de sinais, a exploração de local e o uso de recompensas (LEITE, 2012, p. 13).

vem para complementar outras informações, trazendo subsídios a produção do conhecimento. A fonte aberta também pode ser determinante na tomada de decisões, no monitoramento econômico, social e político de um país.

Stephen Mercado (2004) faz uma análise interessante entre uma fonte aberta e uma informação restrita ou protegida. Ele enumera alguns atributos em se trabalhar com uma fonte aberta, quais sejam:

- **Velocidade**: inúmeras situações e fatos importantes são primeiramente divulgados pelos meios de comunicação e pela mídia, muitas vezes fazendo o seu acompanhamento em tempo real, *on-line*. Exemplo recente ocorreu quando se noticiou que o condenado pelo processo denominado como mensalão, José Dirceu, pleiteava autorização ao Juiz da Vara de Execução Penal para trabalhar no Hotel Saint Peter, em Brasília. Jornalistas, no dia seguinte, já haviam levantado todo o histórico da empresa e já se encontravam no Panamá para entrevistar o suposto laranja. Segundo divulgado na mídia, a *Truston International*, sócia majoritária do Hotel Saint Peter, fica sediada no Panamá e é presidida por um laranja, José Eugenio Silva Ritter. Ainda segundo o "Jornal Nacional", da TV Globo, ele mora num bairro pobre da cidade, trabalha há 30 anos como auxiliar de escritório numa empresa de advocacia e, no papel, é dono de mais mil empresas (O GLOBO, 2013).

- **Quantidade**: existem muitos mais jornalistas, blogueiros, estudiosos, especialistas do que analistas de inteligência e policiais em investigações. Além disso, eles contam com muito mais autonomia e recursos para executarem determinadas ações do que a própria polícia (veja-se o próprio exemplo dado acima). Como já dito, a integração e a troca de informações com organizações, acadêmicos e empresas privadas, nos dias de hoje, são imprescindíveis à atividade de inteligência.

- **Qualidade e clareza**: dependendo da origem, é possível auferir imediatamente a autenticidade de uma informação adquirida por uma fonte aberta. Se confrontada com outros dados então, gera certeza no analista que produz o conhecimento, tornando-se um documento de grande valia. Por outro lado, um documento classificado que foi produzido, por exemplo, com base numa denúncia anônima, num informante ou colaborador eventual, ou mesmo com base em estimativas, muitas vezes não terá seu grau de confiança prontamente atestado.

- **Facilidade de uso**: trabalhar com uma fonte aberta é ter seu acesso para pronto uso. Assim, ela não depende de credencial de segurança, programas de criptografia, cuidados de segurança na difusão e na compartimentação. Todos podem ter acesso. Não se confunda, pois, fonte aberta com fonte gratuita. Nem toda fonte aberta é gratuita. Fonte aberta é aquela disponível para qualquer cidadão, ainda que mediante pagamento para aquisição e uso.

- **Baixo custo**: em sua grande maioria, as fontes abertas desoneram o Estado de forma substancial. A obtenção de dados pela internet é rápida, fácil e de baixíssimo custo. Leonardo Singer Afonso (2006, p. 54) destaca que:

> *[...] Robert Steele [...], depois de examinar as demandas feitas à Inteligência do Corpo de Fuzileiros Navais dos Estados Unidos num determinado espaço de tempo, chegou à conclusão de que mais de 80% delas poderiam ser atendidas por meio de fontes abertas, de maneira dinâmica e a baixo custo, se comparado ao orçamento destinado àquelas demandas supridas por onerosas operações de campo.*

Em 2013, por exemplo, a polícia suíça apreendeu 1,2 toneladas de maconha com a ajuda do Google Earth, um *software* de imagens. A investigação resultou na prisão de 17 pessoas e na localização da plantação, que estava camuflada em uma plantação de cereais (BARRETO, WENDT; 2013, p.74). Chris Crego foi preso em meados de outubro de 2009 em Nova York, por assalto. Ele se declarou culpado, mas em seguida fugiu daquele estado. Em 2010, foi encontrado e recapturado em seu local de trabalho em Terre Haute, Indiana, depois de ter publicado detalhes, inclusive seu horário de trabalho, em suas páginas no *Facebook* e no *MySpace* (JACOBSSON, 2010).

O uso de *OSINT* pode resultar não somente em economia monetária, mas também em menor risco para os agentes e analistas do que a utilização de métodos considerados intrusivos como, por exemplo, as técnicas especiais de investigação.

As fontes abertas propiciam um leque enorme de informações de domínio público que não devem ser menosprezadas pelas comunidades de inteligência. Se bem trabalhadas, por profissionais experientes, podem trazer enormes avanços para enfrentar os atuais desafios da área de inteligência como o desenvolvimento das organizações criminosas, do terrorismo e da contraespionagem.

3.2 BREVE HISTÓRICO DO EMPREGO DE OSINT NOS EUA

Como forma de enfatizar o valor das fontes abertas para a atividade de inteligência, este tópico procura descrever, de forma sucinta, a evolução do serviço de OSINT nos Estados Unidos, procurando compreender e analisar a sua gigantesca estrutura, amplitude e seus principais objetivos.

No final de 1930, na Universidade de Princeton, nos Estados Unidos, foram desenvolvidos trabalhos de monitoramento de rádio de ondas curtas estrangeiras. Posteriormente, em 1941, o governo americano criou o *Foreign Broadcast Information Service (FBIS)*, com o intuito de acompanhar as publicações e as transmissões de rádio, durante a Segunda Guerra Mundial (MERCADO, 2007).

Este monitoramento tinha como escopo influenciar a opinião pública e, assim, a política dos Estados Unidos em relação à guerra. O *FBIS* também realizava a análise das transmissões de rádio e das publicações para descobrir eventuais mudanças de conteúdo que poderiam implicar mudanças nas intenções japonesas (RIDDEL, 1992).

Com o final da II Guerra Mundial, o FBIS foi ameaçado de extinção, o que provocou uma enxurrada de críticas, inclusive pela imprensa. Assim, com a aprovação da Lei de Segurança Nacional em 1947, este serviço foi incorporado à CIA, recém fundada.

O *FBIS* cresceu em resposta a Guerra Fria e dos interesses de todo o mundo nos Estados Unidos. Na verdade, a exploração de fontes abertas pelo FBIS constituiu uma parte importante de toda a inteligência sobre a União Soviética, a China e outros adversários (MERCADO, 2007).

Marco Cepik (2003, p. 51-52) descreve um pouco do que era coletado pelo *FBIS*:

> *Por exemplo, sabe-se que durante a Guerra Fria um programa em conjunto da CIA e da US Air Force resumia e/ou traduzia inteiramente a maioria das publicações tecnocientíficas da União Soviética. Já em 1956, isso significava o resumo/tradução do conteúdo de 328 periódicos científicos e cerca de 3 mil livros e monografias por ano. [...]*

> *De acordo com declarações do então deputy director of central intelligence, em 1992 o serviço de vigilância de mídia estrangeira da CIA (o* Foreign Broadcast Information Service – FBIS*) monitorava 790 horas semanais de programação de TV em 50 países e 29 línguas diferentes.*

O *FBIS* contava com 19 pontos de coleta em todo o mundo em localidades diversas como Assunção, Bangcoc, Cidade do Panamá, Hong Kong, Londres, Seul e Viena (CEPIK, 2003).

Estes escritórios de campo eram formados por nacionais, americanos e estrangeiros e geralmente funcionavam em uma embaixada, consulado ou em alguma área militar. A sede, localizada em Reston, adquiria e examinava cerca de 3 mil jornais e periódicos em quase 60 línguas regularmente, conforme discurso do vice-Diretor do *FBIS*, J. Niles Riddel, em 1992. Os analistas selecionavam o que era de interesse do Governo dos EUA e enviavam a quase 700 tradutores independentes contratados. Caso algum conteúdo demonstrasse ser sensível ao tempo, era traduzido instantaneamente na própria sede para uma rápida disseminação (RIDDEL, 1992).

Em 1974, os relatórios diários do *FBIS* foram disponibilizados ao setor privado, através de assinaturas pagas, contribuindo para maior participação da sociedade nas questões de interesse comercial e político dos Estados Unidos (RIDDEL, 1992).

Em 2005, o *FBIS* deixou de existir sob a égide da CIA e passou a fazer parte da estrutura do *Director of National Intelligence* (*DNI*) com novo nome, *Open Source Center* (*OSC*). Essa mudança ocorreu em razão da necessidade de reestruturação e modernização da comunidade de inteligência do país que estava em descrédito, devido ao atentado de 11 de setembro e por fornecer documentos questionáveis de que o Iraque possuía armas de destruição em massa (AFONSO, 2006).

O Diretor Geral da CIA acumula a função de agente executivo do *DNI* na gestão do *OSC*. O *OSC* tem a tarefa de melhorar a disponibilidade de fontes abertas para oficiais de inteligência e outros funcionários do governo.

O *OSC* coleta, traduz, produz e divulga informações provenientes de fontes abertas que atendam às necessidades dos decisores políticos, militares, policiais e analistas de inteligência em todo o Governo dos EUA. Ele elabora mais de 2.300 produtos por dia, incluindo traduções, transcrições,

análises, relatórios, compilações de vídeo e inteligência geoespacial para atender necessidades de curto e longo prazo. Seus produtos abrangem questões que vão desde temas políticos, militares, econômicos, ciência e tecnologia, assim como contraterrorismo, não proliferação de armas, combate ao narcotráfico e outros temas de segurança interna (CIA, 2009).

Parte desse material é disponibilizado para os oficiais de inteligência e funcionários do Governo americano a partir do endereço eletrônico: www.opensource.gov (BRITO, 2011, p.151-152).

Até 31 de dezembro de 2013, o *OSC* fornecia material para o *National Technical Information Service (NTIS)*, através do feed de notícias on-line World News Connection, que eram disponibilizadas ao setor privado. Contudo, esse serviço foi extinto. O Porta-voz da CIA, Christopher White, explicou que o *feed* de fontes abertas de informações do *NTIS* tornou-se desatualizado e necessitaria de alto custo para atualizá-lo (AFTERGOOD, 2014).

Além do *OSC*, existem, ainda, outras unidades setoriais especializadas em fontes abertas, que atuam junto ao Departamento de Defesa e ao Departamento de Estado (MERCADO, 2004).

Este breve histórico do uso de fontes abertas pela comunidade de inteligência dos EUA serve para ilustrar, pelo menos em parte, a sua importância para a atividade de inteligência (seja ela de Estado, policial, competitiva), além de expressar o quanto as comunidades de inteligência no Brasil deveriam evoluir nesse sentido.

4. *OSINT* e suas Limitações

Os desafios enfrentados por uma inteligência baseada em fontes abertas são muitos. O crescimento fenomenal da quantidade de dados, informações e opiniões publicadas veio acompanhado do uso mal intencionado da internet, de fraudes *on-line*, conteúdos ilegais, perseguição virtual e utilização e disseminação de idéias extremistas e terroristas (BEST, 2008).

Clive Best (2008) afirma que até 1998 existiam cerca de 15 *links* terroristas em *websites*, sendo que até 2008 este número era mais de 4500. Tudo isso gera novos desafios para as agências de segurança, de criação e aplicação das leis.

Trabalhar com *OSINT* não é tarefa fácil. Ela possui várias limitações. Uma delas é que um analista dificilmente vai encontrar informações atuais que possuem algum grau de sigilo em domínio público. O enorme número de vazamentos divulgados pela mídia não possuem valor expressivo dentro de um universo de documentos classificados, embora sejam extremamente úteis quando se tornam de uso comum.

Por conseguinte, a *OSINT* nunca substituirá outras formas de obtenção de informações, como o dado negado, por exemplo. Além disso, a validação ou a complementação de uma fonte ou dado poderá necessitar do acionamento de agentes de campo (AFONSO, 2006) ou do cruzamento de variadas fontes de informações.

Nas sociedades consideradas de regime fechado, a análise dos meios de comunicação tem provado ser de grande valor, segundo Mercado (2004) e Burke (2007). A Coréia do Norte, por exemplo, possui apenas dois jornais em circulação: um do partido comunista e o outro administrado pelo Governo. Esses dois jornais são instrumentos de doutrinação em massa e servem de referência para os analistas determinarem as motivações e prioridades do Governo. Isso possibilita uma maior cobertura das informações, fato que não ocorre nos países democráticos, por possuírem uma multiplicidade e uma diversidade de dados disponíveis.

A internet fez com que os dados derivados de uma fonte aberta fossem mais práticos e úteis, tornando-se, por outro lado, mais difícil de gerir. Ademais, a quantidade de informações disponíveis e a diversidade de formatos desses dados criam obstáculos na produção do conhecimento (POUCHARD, 2009).

Nesse diapasão, um dos maiores problemas enfrentados com a criação de um setor especializado em *OSINT* é adequar a quantidade de informação bruta coletada com o processo de produção e difusão do conhecimento em tempo hábil. Até mesmo com software sofisticado, pode acontecer do analista da *OSINT*, devido ao volume do fluxo de dados, perder uma informação importante. É preciso saber identificar o que é relevante, filtrar e processar todas as informações e extrair um conhecimento (LOWENTHAL, 2003).

Não custa lembrar que o maior mérito da atividade de inteligência é obter superioridade informacional, ou seja, capacidade de fornecer ao decisor, em tempo hábil e oportuno, conhecimentos suficientes, claros e conci-

sos, que trarão vantagem estratégica e competitiva, minando os adversários e as ameaças existentes.

Possuir uma grande quantidade de informações derivadas de fontes abertas não vai necessariamente lhe dar uma grande quantidade de conhecimento, pois a maioria das informações recebidas não serão de interesse do receptor. Assim, é preciso saber filtrar muito bem os dados coletados antes de repassá-los para outros analistas. As facilidades advindas do progresso impuseram a necessidade de qualificar a informação, sob pena de sobrecarregar o decisor, desviando a atenção sobre o foco pretendido e perturbando o nível decisório correspondente (MENDES; MORESI, 2012, p. 47).

Por conseguinte, saber gerir de forma adequada o conhecimento é um enorme desafio das comunidades de inteligência. Vladimir Brito (2006, p. 146) assevera que:

> *Considerando-se o grande volume de dados, a questão de como geri-los torna-se essencial, uma vez que estes tendem a aumentar exponencialmente. Cabe notar que a capacidade das organizações de inteligência em produzir boas análises, sobretudo de longo prazo, relaciona-se diretamente a qualidade da coleção disponível. No momento em que inexistam coleções organizadas, inexistem informações acessíveis, e, portanto, objetivamente é o mesmo que não se possuir a referida informação.*

Além disso, um analista deve ser criterioso na produção do conhecimento, uma vez que nem tudo que é publicado é verdadeiro ou confiável. Não há controle sobre a produção de uma fonte aberta. Assim, uma informação pode ter caráter, na verdade, de:

- **Desinformação** - realizada para, intencionalmente, confundir alvos (pessoas ou organizações), a fim de induzir esses alvos a cometerem erros de apreciação, levando-os a executar um comportamento pré-determinado (DNISP, 2009. p. 34);

- **Contrainformação** - ação ou estratégia para impedir ao inimigo ou a uma entidade o acesso a uma informação verdadeira, notadamente com divulgação de informações falsas (Dicionário PRIBERAM, 2008-2013);

- **Propaganda** - é a manipulação das informações com uso de recursos persuasivos (folhetos, TV, rádio, outdoor, redes sociais, *blogs*, mídias) e

visa produzir um comportamento em benefício de quem está promovendo, informando, traduzindo ou anunciando. A propaganda é possuidora de poder de convencimento e busca influenciar indivíduos sociáveis nos seus atos ideológicos (FERRO JÚNIOR, 2011).

Na verdade, as informações retiradas de fontes abertas nunca devem ser analisadas, a priori, como verdades absolutas, sob pena do analista incorrer em erro. Elas devem ser confrontadas com outras fontes a fim de ser utilizadas na atividade de inteligência (BARRETO; WENDT, 2013).

Washington Platt (1962, p. 66), em 1962, já mencionava o Princípio da Exploração das Fontes, qual seja:

> *O Princípio da Exploração das Fontes requer o perfeito acionamento de todas as fontes que possam jogar alguma luz sobre a Informação.*
>
> *Quais são as possibilidades e limitações prováveis de cada fonte? Até que ponto confirmam ou se contradizem? Quanto mais variadas as fontes, maior a possibilidade de efetivas verificações cruzadas. Fontes variadas ampliam as bases do documento, aprofundam a perspectiva e diminuem a possibilidade de erros sérios.*

Os órgãos de inteligência ainda lidam com outro grande entrave que reside na tradução de um dado estrangeiro para o idioma nacional. Softwares de tradução nos dão uma noção do texto, mas ignoram linguagens coloquiais, gírias, costumes locais, entre outros. Investir em analistas que dominam outras línguas, poliglotas, é essencial para este tipo de atividade (MERCADO, 2007).

Do ponto de vista da segurança, a internet deve ser vista como uma via de mão dupla. Potenciais adversários podem utilizar a internet para obter informações e não há controle direto sobre o que é postado por terceiros, como já dito (BURKE, 2007). Além disso, ela se baseia em informações que são fragmentárias e abertas a várias interpretações.

A função deste capítulo não é esgotar todas as restrições existentes em relação à *OSINT*, mas apenas explicitar alguns problemas advindos deste ramo de atividade. Essas limitações não servem, todavia, para desprestigiar a fonte aberta. Ao contrário, serve para aprofundar o conhecimento do analista que deverá saber filtrar melhor os dados que julgar úteis para a atividade desenvolvida.

5. Como a *OSINT* Pode Ajudar a Prevenir a Corrupção

A corrupção afeta o sentido de igualdade e da justiça social, prejudica a confiança dos cidadãos, deslegitima as instituições e gera danos sociais (FIESP, 2010, p. 30). Aquele que atua em decorrência das facilidades proporcionadas pela sua função, predador dos cofres públicos, da moral administrativa, prejudica toda a coletividade, fator que impede o progresso e o crescimento da Nação.

O custo médio da corrupção no Brasil é estimado entre 1,38% a 2,3% do PIB, isto é, de R$ 50,8 bilhões a R$ 84,5 bilhões (correspondente ao ano de 2010), conforme índice de percepção da corrupção, recentemente elaborado pela Federação das Indústrias do Estado de São Paulo (FIESP, 2011, p. 6).

A prevenção da corrupção no Brasil assume, pois, papel de destaque nesse cenário atual e é um grande desafio a ser enfrentado pelas comunidades de inteligência. Dentro desse contexto, a *OSINT* deve ser utilizada como recurso fundamental no planejamento e na obtenção de informação relevante, fornecendo alertas e identificando eventuais irregularidades no gasto público.

Com a criação de diversos portais públicos é possível acompanhar os programas de governo, a destinação e os gastos públicos via internet. O site Comprasnet, por exemplo, permite acompanhar as informações referentes às licitações e contratações promovidas pelo Governo Federal. No Portal da Transparência é possível acompanhar a execução financeira dos programas de governo, em âmbito federal, e informações sobre os recursos públicos federais e suas destinações. O Portal Siga Brasil permite que qualquer indivíduo tenha acesso amplo a diversas bases de dados sobre planos e orçamentos públicos federais (MORESI *et al.*, 2010).

O site do Banco do Brasil disponibiliza informações sobre repasses de recursos aos governos federal, estadual e municipal, permitindo um acompanhamento do que é repassado a cada gestor. O Banco Nacional do Desenvolvimento (BNDES) também possui uma opção de consulta a projetos realizados pela Administração Direta Pública e o Banco, possibilitando que qualquer pessoa fiscalize essas operações (BARRETO e WENDT, 2013).

Qualquer interessado em manter convênio com o Governo Federal, desde setembro de 2008, é obrigado a se cadastrar no Sistema de Convênios do Governo Federal (SINCOV), ferramenta disponível no Portal dos Convênios, permitindo aos órgãos o gerenciamento *on-line* de todos os contratos (SILVA JÚNIOR, 2011).

Pelo Portal da Transparência também é possível realizar uma consulta das empresas que foram fornecedoras do Governo Federal, por ramo de atividade econômica. Estes portais públicos, dentre outros, são fontes abertas confiáveis para a coleta de informações para diversas finalidades. É possível obter informações sobre gastos públicos com o objetivo de manter um controle sob eles, tanto quanto para produzir informações úteis para a Inteligência Competitiva (MORESI *et al.*, 2010).

Todos esses portais citados possuem os dados e as informações. Todavia, para se atingir o objetivo proposto, qual seja, prevenir a corrupção por meio de *OSINT*, é necessário o uso de ferramentas que possam coletar grandes volumes de dados e fazer o cruzamento dessas informações. Nesse momento, o trabalho do analista é fundamental para detectar eventuais distorções e, ainda, para traçar estratégias que possam minar essas disfunções.

Outra vertente a ser considerada é o papel da imprensa na divulgação de crimes, especialmente os de "colarinho branco"[6]. As redes de televisão, assim como revistas, portais de notícias na web estão sempre publicando matérias relacionadas à corrupção, envolvendo autoridades, políticos e funcionários públicos. Esses dados, quando confrontados, servem de suporte para iniciar uma investigação ou mesmo para auxiliar as operações em andamento.

As redes sociais, sob as suas diversas formas, também possuem importante função na prevenção da corrupção. Elas influenciam parcelas significativas da sociedade e contribuem para o controle social sobre os recursos públicos, ora difundindo boas práticas na condução de recursos, ora denun-

6 A expressão "*white collar crimes*" foi usada pela primeira vez em 1940, por Edwin Sutherland, durante um discurso na American Sociological Association. O termo surgiu em decorrência das práticas criminosas realizadas por agentes de elevado status econômico e social, que no exercício de suas atividades profissionais, locupletam-se como forma de obter ganhos indevidos para si ou para a corporação. Disponível em: <http://pt.wikipedia.org/wiki/Crime_do_colarinho_branco> Acesso em 20/01/2012.
No Brasil, a expressão crime de "colarinho branco" é, muitas vezes, utilizada para os crimes tributários, financeiros, econômicos, contra a administração pública, em especial aqueles ligados a prática de corrupção e desvio de dinheiro público. (LEITE; 2012, p. 30)

ciando abusos (MORESI *et al.*, 2010). Além disso, possuem alto valor agregado, ou seja, informações e dados pessoais como imagens, círculo social, valores ideológicos, contatos.

O monitoramento através das redes sociais também pode ser importante para acompanhamento de pessoas envolvidas em denúncias de corrupção. Saber como pensam, suas tendências sociais e políticas, podem ajudar na análise e no cruzamento de dados quando confrontados com outros tipos de informações. Além disso, novas tecnologias, disponíveis especialmente via internet, são capazes de otimizar e conduzir de forma prática, através de baixo custo, o trabalho do analista ou do investigador. Diversas ferramentas podem ser adquiridas gratuitamente viabilizando o processo de cruzamento e análise de dados[7].

Dentro do tema proposto, a Universidade Católica de Brasília (UCB), em parceria com a Controladoria Geral da União (CGU), elaboraram um projeto de pesquisa muito interessante denominado "Operações de Informação para apoiar a prevenção à fraude" (MENDES; MORESI, 2012). Para fins didáticos, será apresentado um resumo do que foi proposto e dos resultados obtidos.

Os objetivos específicos da pesquisa eram, dentre outros, identificar, caracterizar e qualificar as fontes abertas no ciclo da inteligência; analisar a aplicação de conceitos doutrinários de operações de informação na prevenção à fraude e à corrupção; estudar as alternativas tecnológicas para análise de grandes volumes de dados; propor as bases doutrinárias para a aplicação de Inteligência de Fontes Abertas para a CGU.

Para alcançar esses objetivos, foram contratados doze bolsistas de graduação da área de Computação e Informática e treze bolsistas de Mestrado, que ficaram sob a orientação seis professores doutores (MENDES; MORESI, 2012, p. 48).

A arquitetura do projeto dividiu-se em três camadas (MENDES; MORESI, 2012, p. 48):

> - **infraestrutura de Tecnologia da Informação** – *procurou desenvolver uma plataforma tecnológica que permitia o processamento de grandes volumes de informação de forma distribuída;*

7 Dentre alguns *softwares* e programas disponíveis gratuitamente, pode-se citar: *Maltego, NodeXL, yED Graph Editor, Weka, Touchgraph, Pajek, Gephi, Many Eyes, Maxmind.*

> - **produção de informação** – *estudar soluções de software para aplicação na análise de grandes volumes de dados (quantitativos e qualitativos) empregando técnicas de mineração de dados e de textos, coleta e processamento automático de informação e recuperação de informação não estruturada;*
>
> - **operações de informação** – *desenvolvimento de doutrina apropriando do conceito de Inteligência, Contrainteligência e Comunicação Organizacional para aplicação no contexto da prevenção à fraude e corrupção.*

Dentre os resultados obtidos ao longo das pesquisas desenvolvidas estão (MENDES; MORESI, 2012, p. 49-50):

> *- definição de vários indicadores para extração de informações do DW-Compras, por meio de técnicas de mineração de dados, realizada por meio da ferramenta WEKA. Os resultados obtidos permitiram a identificação de indícios de comportamentos irregulares ou entidades, supostamente, beneficiadas;*
>
> *- a confirmação da possibilidade da utilização do Diário Oficial da União (DOU) como fonte aberta de conhecimento para a busca de indícios de irregularidades nas aquisições do Governo Federal Brasileiro, a criação de casos de uso e alertas para a busca de irregularidades, além da exploração de novas possibilidades para a descoberta de conhecimento em fontes abertas de informação. Entretanto, o experimento realizado com* software *de* ECM *(*Electronic Content Management*) revelou que este tipo de ferramenta é limitada para atender necessidades de recuperação de informação;*
>
> *- um método para análise geoespacial e predição de irregularidades em procedimentos médicos no Sistema Único de Saúde (SUS). O estudo às bases de dados abertas do SUS buscou identificar informações dispersas entre várias tabelas distintas, que, quando avaliadas, conjugadas e interpretadas, permitam revelar evidências de indícios de irregularidades de fraudes;*
>
> *- o uso da propaganda em redes sociais como instrumento de Contrainteligência (CI) aplicada à prevenção da corrupção. Foi realizado experimento no* Twitter *onde foram publicadas informações, de forma planejada, e monitorada a repercussão e a propagação delas na rede;*
>
> *- uma ferramenta de coleta e interação no* Twitter*, que tem a finalidade de extrair e publicar informações na rede social. A ferramenta foi desenvolvida para atender os seguintes objetivos: coletar informações relevantes a partir de fontes identificadas, especificamente usuários do* Twitter*; armazenar as informações obtidas em uma base de dados consistente que permita acesso aos dados e interface de buscas para possibilitar a criação de ferramentas de análise e ma-*

> *nipulação das informações; fornecer interface gráfica via web para visualização dos dados contidos na base, permitindo pesquisas por usuários; permitir a inserção de mensagens no* Twitter *por meio de um ou mais perfis previamente definidos; fornecer aferição de impacto das mensagens inseridas pela ferramenta em tempo real;*
>
> *- o desenvolvimento de protótipo de indexação de* blogs *para realizar a busca, a leitura e o armazenamento de postagens consideradas relevantes. O sistema inicia a captura de postagens em* blogs *a partir de uma lista de URLs de blogs fornecida pelo usuário no momento em que o mecanismo de indexação é ativado. Então, ele inicia o armazenamento das postagens encontradas nesses* blogs *e segue em frente, continuando o rastreamento partindo para outros blogs recomendados naqueles fornecidos na lista inicial, e assim por diante. Dessa forma, é realizada a carga em um banco de dados com as informações relevantes e relacionadas entre si, sendo possível realizar diversas medições e análises;*
>
> *- uma proposta de arquitetura de coleta e disponibilização de informações públicas sobre compras governamentais, que contemple as funcionalidades de coleta, tratamento e disponibilização das informações sobre contratações da Administração Pública Federal, disponíveis por meio do Acesso Livre ao* site *Comprasnet. O protótipo desenvolvido possui as seguintes funcionalidades:* download *automático das informações presentes do Comprasnet; estruturação, por meio de* parsing*, das informações coletadas; armazenamento em banco de dados relacional; interface para consulta das informações armazenadas.*

Conforme se constata, a evolução da tecnologia e dos sistemas de comunicação impuseram uma nova realidade aos órgãos de inteligência. Esses experimentos mostraram que o uso adequado da *OSINT* pode ser de grande valia na prevenção e no combate à fraude e à corrupção. Além disso, demonstrou-se que a informação, se bem manuseada e trabalhada, exerce um importante domínio que pode influenciar pessoas, grupos ou organizações.

Em suma, os portais públicos são fontes confiáveis de informações. As redes sociais são fontes valiosas. Todavia, para tornar essas informações produto de interesse da atividade de inteligência policial é necessário o emprego de *softwares* adequados para realizar pesquisas, capturar e confrontar esses dados com grande velocidade. Todo esse processo de coleta pode resultar numa base de dados customizada, fruto de um conjunto de informações que se pretende analisar. Prevenir a corrupção é um dos objetivos da inteligência policial. Resta traçar, entre outros meios, um planejamento estratégico baseada numa *OSINT* que atenda essa demanda de forma eficiente e prática.

6. Considerações Finais

A explosão informacional intensificada no final do século XX, derivada especialmente da internet, trouxe novos desafios à atividade de inteligência. Um deles, sem dúvida, é a utilização da *OSINT* como forma de produzir conhecimento com alto valor agregado e menor custo e risco.

Verifica-se que a manipulação e o tratamento da informação derivada de uma fonte aberta são contribuintes para a produção de conhecimento com alto valor agregado, trazendo vantagem estratégica e competitiva. Trabalhar com fontes abertas é condição sine qua non para enfrentar os tempos modernos.

Por conseguinte, a prevenção e o combate ao crime dependem de esforços coletivos. Desenvolver e implementar uma área voltada para *OSINT* é apenas uma parte de um todo. Robert David Steele (2006) afirma que, nessa nova era, todos, incluindo qualquer terrorista, tem a opção de usar fontes abertas de informação que são iguais ou superiores às fontes secretas. Inteligência de fonte aberta aproveita o que todo mundo vê e sabe. Muda as regras do jogo.

Além disso, é de suma importância a troca de informações entre os serviços de inteligência. Não adianta possuir o maior e mais eficiente aparato em tecnologia, os melhores analistas, se não há gestão adequada do conhecimento, interação entre os sistemas e os órgãos de inteligência. É preciso se ater que uma inteligência voltada para a utilização de fontes abertas demora um tempo para atingir maturação.

Diante do exposto, pode-se observar que, ao destacar a importância do emprego das fontes abertas para a atividade de inteligência policial, existem vários requisitos que necessitam de integração e equilíbrio para tornarem seus efeitos tangíveis. Do contrário, continuaremos a ter muitos órgãos e pouca inteligência.

Sara Souza Leite

Agente de Polícia Federal. Atua há mais de 8 anos na Diretoria de Inteligência Policial, em Brasília/DF, do Departamento de Polícia Federal. Bacharel em Direito pela Faculdade Milton Campos/MG. Especialista em Inteligência Policial pela Escola Superior de Polícia da Academia Nacional de Polícia. Especialista em Direito Penal e Processo Penal pela Faculdade Gama Filho.

E-mail: sara.ssl@dpf.gov.br

ABSTRACT

The Employment of Open Source in the Framework of Activity of Police Intelligence

This work discusses the use of open sources in the activity of police intelligence. In recent years, there has been considered a breakthrough in communication and technology systems, which caused a significant change in the information environment. Brazil´s intelligence service did not follow this trend, causing the inability to meet all demands. This research shows that in order to invest and develop an area designated as Open Source Intelligence (OSINT), a reform in the structure of intelligence communities is imperative. This is an analysis of police intelligence actual objectives and necessities resulting from police activity, the function of the OSINT in the police intelligence, the value of open sources, its attributes and limitations, brief overview of OSINT in the EUA and how open sources could help prevent corruption.

Keywords: Police Intelligence. Open source. Open Source Intelligence (OSINT). Value of OSINT. Limitations. Prevention of corruption.

7. Referências

AFONSO, L. S. Fontes abertas e Inteligência de Estado. **Revista Brasileira de Inteligência**. Brasília: Abin, v. 2, n. 2, abr, 2006, p. 49-62. Disponível em: <http://www.abin.gov.br/modules/mastop_publish/?tac=Fontes_abertas_e_Intelig%EAncia_de_Estado>. Acesso em: 12 fev. 2014.

AFTERGOOD, S.. **CIA Cuts Off Public Access to Its Translated News Reports**. January 8, 2014. Disponível em: <http://blogs.fas.org/secrecy/2014/01/fbis-wnc/>. Acesso em: 10 fev. 2014.

BARRETO, A. G.; WENDT, E.. **Inteligência Digital**. Rio de Janeiro: Brasport, 2013.

BEST, C.. **Open Source Intelligence. Joint Research Centre**. 2008. Disponível em: <http://media.eurekalert.org/aaasnewsroom/2008/FIL_000000000010/071119_MMDSS-chapter_CB.pdf>. Acesso em: 01 mar. 2014.

BRASIL. Departamento de Polícia Federal (DPF). **Manual de Inteligência Policial**. Vol.1. 2011.

BRITO, V. de P.. **O Papel Informacional dos Serviços Secretos**. Dissertação apresentada ao Programa de Pós-Graduação para obtenção do título de mestre em Ciência da Informação. UFMG. Belo Horizonte: 2011.

_____. **Novos Paradigmas para a Inteligência Policial**. Manaus: 2006. Especialização em inteligência competitiva. Projeto final – Universidade Federal do Amazonas.

BURKE, C.. **Freeing knowledge, telling secrets:** Open source intelligence and development. 2007. CEWCES Research Papers. Paper 11. Disponível em: <http://epublications.bond.edu.au/cewces_papers/11>. Acesso em: 07 fev. 2014.

CENTRAL INTELLIGENCE AGENCY (CIA). Library. Publications. [...] **Centers in the CIA**. Publicado em 10 de setembro de 2009. <https://www.cia.gov/library/publications/additional-publications/the-work-of-a-nation/cia-director-and-principles/centers-in-the-cia.html>. Acesso em: 23 mar. 2014.

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

COUTINHO, C.. **MANY EYES**: revolução tecnológica, compartilhamento e universalização de informações. 2011. Disponível em: <http://claudiaccoutinho.wordpress.com/2011/09/24/many-eyes-revoluo-tecnolgica-compartilhamento-e-universalizao-de-informaes/> Acesso em: 30 jun.2014.

Dicionário Priberam da Língua Portuguesa, 2008-2013, Disponível em: <http://www.priberam.pt/dlpo/contra-informa%C3%A7%C3%A3o> Acesso em: 28 mar. 2014.

Federação das Indústrias do Estado de São Paulo (FIESP). Departamento de Competitividade e Tecnologia - DECOMTEC. **Relatório Corrupção**: custos econômicos e propostas de combate. 2010.

_____. **Índice de percepção da corrupção**. 2011.

FERRO JÚNIOR, C. M.. **A Inteligência e a Gestão da Informação Policial**. Brasília: Fortium, 2008.

_____. **Propaganda e Contrapropaganda**. Publicado em 22 de julho de 2011. Disponível em: <http://gestaopolicial.blogspot.com.

br/2011/07/propaganda-e-contrapropaganda.html> Acesso em: 20 mar. 2014.

FREGAPANI, C.. **Segredos da Espionagem** – a influência dos serviços secretos nas decisões estratégicas. Brasília: Thesaurus, 2003.

GOMES, R. C.. Prevenir o crime organizado: Inteligência policial, democracia e difusão do conhecimento. **Revista Brasileira de Segurança Pública e Cidadania**. Brasília: vol. 2, n. 2, jul-dez, 2009.

GONÇALVES, J. B.. **Atividade de Inteligência e Legislação Correlata**. Série Inteligência, Segurança e Direito. Niterói: Impetus, 2010.

JACOBSSON, S.. **PC World**. Cinco Criminosos Presos com Auxílio das Redes Sociais. Publicada em 22 de março de 2010. Disponível em: <http://pcworld.com.br/noticias/2010/03/22/cinco-criminosos-presos-com-o-auxilio-de-redes-sociais/> Acesso em: 20 jul.2014.

JOHNSTON, R.. **Analytic Culture in the US Intelligence Community** – an Ethnographic Study. Washington: The Center of the Study of Intelligence, 2005. Disponível em: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/analytic_culture_report.pdf> Acesso em 20 mar. 2014.

LEITE, S. S.. T**écnicas Especiais de Investigação**. Monografia apresentada como requisito parcial para conclusão do curso de Especialização em Direito Penal e Processual Penal. Brasília: Universidade Gama Filho. 2012.

LOWENTHAL, M.. **Intelligence**: From Secrets to Policy. Washington: CQ Press, 2003.

MENDES, G. L. de O.; MORESI, E. A. D.; SILVA, W. V.. E**studo sobre Portais Públicos como Fontes Confiáveis para Inteligência de Fontes Abertas**. VII Convibra Administração – Congresso Virtual Brasileiro de Administração. 2010. Disponível em: <http://www.convibra.org/2010.asp?ev=71&p=&lang=en>. Acesso em: 24 mar. 2014.

MENDES, G. L. de O.; MORESI, E. A. D.; Operações de Informação: um estudo sobre o desenvolvimento de doutrina aplicada à

prevenção à fraude. **Sistemas, Cibernética e Informática**. Brasília: vol. 9, n. 1, 2012.

MERCADO, S. C. Reexamining the Distinction between Open Source Information and Secrets. Studies In Intelligence: **Journal of the American Intelligence Professional**. Washington: v. 49, n. 2, 2004.

MERCADO, S. C. **Sailing The Sea of OSINT In The Information Age** – a venerable souce in a new era. Publicado em 14 de abril de 2007. Disponível em: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article05.html> Acesso em: 20 jan. 2014.

MINAS, H.. Can the Open Source Intelligence Emerge as an Indispensable Discipline for the Intelligence Community nn the 21st Century? – **Research Publication n. 139**. JANUARY, 2010. Disponível em: <https://docs.google.com/viewer?a=v&q=cache:kc8EuFjUwb0J:kms1.isn.ethz.ch/serviceengine/Files/ISN/111330/ipublicationdocument_singledocument/e42b441e-4bf3-45f7-9523-0875c61cb094/en/rieas139.pdf+CAN+THE+OPEN+SOURCE+INTELLIGENCE+EMERGE+AS+AN+INDISPENSABLE+DISCIPLINE+FOR+THE+INTELLIGENCE+COMMUNITY+IN+THE+21st+CENTURY&hl=pl&gl=pl&pid=bl&srcid=ADGEESiHLpoJNvsza1t5zYpDwFy_bho2Nb703trPSyctq1nj0swm9hpolNg6zC02EsqaYkgh86vwVOSo-NlgTms3mbPZK_7LSA6SOg4FRTRNYYnF34x4T7AS09Qn_Zqypr7T816OeAaw&sig=AHIEtbSqV71260rCpoZVMtSOauBGV--sQA>. Acesso em: 20 jan. 2014.

MINISTÉRIO DA JUSTIÇA (MJ). Secretaria Nacional de Segurança Pública. **Doutrina Nacional de Inteligência de Segurança Pública** (DNISP). Brasília. 2009.

MINISTÉRIO DA JUSTIÇA (MJ). **Resolução nº 1**, de 15 de julho de 2009, que regulamenta o Subsistema de Inteligência de Segurança Pública – SISP.

MORESI, E. A. D.; JUNIOR, O. S. da S.; *et al.* **Inteligência de Fontes Abertas:** um estudo sobre o emprego das redes sociais na prevenção à corrupção. VII Convibra Administração – Congresso Virtual Brasileiro de Administração. 2010.

Disponível em: <http://www.convibra.org/2010.asp?ev=71&p=&lang=en>. Acesso em: 24 mar. 2014.

NORTH ATLANTIC TREATY ORGANIZATION (NATO). **Open Source Handbook**. Vol.1, 2001. Disponível em: <http://www.oss.net>. Acesso em: 25 jan. 2014.

O GLOBO. **Empresa dona de hotel que ofereceu emprego a Dirceu tem laranja entre dirigentes**. Publicado em 03 de dezembro de 2013 - Disponível em: <http://oglobo.globo.com/pais/empresa-dona-de-hotel-que-ofereceu-emprego-dirceu-tem-laranja-entre-dirigentes-10960598>. Acesso em: 25 fev. 2014.

PACHECO, D. F.. **Atividades de inteligência e processo penal**. In: IV JORNADA JURÍDICA DA JUSTIÇA MILITAR DA UNIÃO – AUDITORIA DA 4ª CJM, 30 set. 2005, Juiz de Fora/MG. Disponível em: <http://www.advogado.adv.br/direitomilitar/ano2005/denilsonfeitozapacheco/atividadedeinteligencia.htm>. Acesso em: 20 jan. 2014.

PINCUS, W.. CIA Alters Policy After Iraq Lapses. **The Washington Post**, 12 February 2004: A1.

PLATT, W.. **A Produção de Informações Estratégicas**. Inc. editôres. 2ªed. 1962.

POUCHARD, L. C.; DOBSON, J. M.; TRIEN, J. P.. **A Framework for the Systematic Collection of Open Source Intelligence**. Oak Ridge National Laboratory. Stanford, California, USA, 2009. Disponível em: <http://www.csm.ornl.gov/~7lp/publis/tpa09_submission_16_final.pdf>. Acesso em: 12 fev. 2014.

RIDDEL, J. N.. **Remarks in First International Symposium**, National Security And National Competitiveness: Open Source Solutions. Publicado em 2 de dezembro de 1992. Disponível em: <https://www.fas.org/irp/fbis/riddel.html>. Acesso em: 15 fev. 2014.

SILVA JÚNIOR, O. S.. **Inteligência em Fontes Abertas:** Um Estudo sobre o Emprego de Mídias Sociais na Identificação de Irregularidas no Serviço Público Federal. Dissertação de Mestrado. Universidade Católica de Brasília. 2011.

SINTRA, A.. Técnicas Especiais de Investigação. Factor de segurança. **Investigação Criminal**. Revista Semestral de Investigação Criminal, Ciências Criminais e Forenses. Lisboa: nº 1, 2010.

STEELE, Robert David. **Open Source Intelligence.** Journal Article. Publicado em 19 de abril de 2006. Disponível em: <http://www.forbes.com/2006/04/15/open-source-intelligence_cx_rs_06slate_0418steele.html>. Acesso em: 01 abr. 2014.