INTELIGÊNCIA DE FONTES ABERTAS (OSINT) COMO INSTRUMENTO ESTRATÉGICO PARA ANÁLISE, DECISÃO E SEGURANÇA PÚBLICA

Renato Pires Moreira[*]
Luiz Augusto Vieira de Oliveira[**]
Luiz Carlos Ferreira[***]

RESUMO: A Inteligência de Fontes Abertas (*OSINT*) tornou-se um dos pilares da atividade de inteligência contemporânea, especialmente em um cenário marcado pela hiperconectividade, pela velocidade da informação e pelo crescimento exponencial de dados públicos. Este artigo apresenta uma análise abrangente sobre os fundamentos, metodologias e aplicações da *OSINT*, examinando modelos clássicos do ciclo de inteligência e comparando-os com a abordagem doutrinária brasileira. Discute-se a categorização das fontes abertas, os critérios de avaliação da confiabilidade informacional e o papel das ferramentas tecnológicas na produção do conhecimento estratégico. O estudo enfatiza a importância da análise crítica, da triangulação informacional e das competências cognitivas do analista, destacando a aplicação da *OSINT* no enfrentamento de crimes complexos, como o tráfico de bens culturais. Conclui-se que a *OSINT* constitui um recurso indispensável à modernização da inteligência, ao aprimoramento da tomada de decisão e ao fortalecimento das políticas de segurança pública.

Palavras-chave: inteligência; *OSINT*; análise de inteligência; segurança pública; decisão estratégica.

DOI: https://doi.org/10.36776/ribsp.v9i23.345

Recebido em 28 de novembro de 2025.	Aprovado em 2 de abril de 2026.

[*] Polícia Militar de Minas Gerais (PMMG). Orcid: https://orcid.org/0000-0002-4592-750X CV Lattes: http://lattes.cnpq.br/2355715189859936 .
** Polícia Militar do Estado do Rio de Janeiro (PMERJ). Orcid: https://orcid.org/0000-0002-4515-624X . CV Lsttes: http://lattes.cnpq.br/2521804130249993
*** Laboratório de Simulação de Cenários da Escola de Guerra Naval. Orcid: https://orcid.org/0009-0008-2875-6623 . CV Lattes: http://lattes.cnpq.br/6742185166567411

OPEN SOURCE INTELLIGENCE (OSINT) AS A STRATEGIC INSTRUMENT FOR ANALYSIS, DECISION-MAKING, AND PUBLIC SECURITY

ABSTRACT: Open Source Intelligence (*OSINT*) has emerged as one of the core components of contemporary intelligence activities, particularly in an environment defined by hyperconnectivity, rapid information flows, and the exponential growth of publicly available data. This article provides a comprehensive analysis of the foundations, methodologies, and practical applications of *OSINT*, examining classical intelligence cycle models and comparing them to the Brazilian doctrinal approach. It discusses the categorization of open sources, criteria for assessing informational reliability, and the role of technological tools in producing strategic knowledge. The study highlights the importance of critical analysis, information triangulation, and the cognitive competencies required of intelligence analysts, with special emphasis on the application of *OSINT* in combating complex crimes such as cultural heritage trafficking. It concludes that *OSINT* is essential for modernizing intelligence, improving decision-making, and strengthening public security policies.

Keywords: intelligence; *OSINT*; intelligence analysis; public security; strategic decision-making.

1. INTRODUÇÃO

A inteligência, enquanto campo de conhecimento e prática institucional, possui um desenvolvimento histórico complexo e multifacetado. Desde suas formulações iniciais, diferentes autores buscaram definir seus elementos constitutivos, muitas vezes enfatizando sua relação com a capacidade humana e organizacional de adquirir, aplicar e transformar informações em conhecimentos e ações eficazes. Nesse sentido, Legg e Hutter (2007) reúnem um conjunto de definições que convergem na compreensão da inteligência como um processo cognitivo estruturado, voltado à resolução de problemas, ao aprendizado contínuo e à adaptação a ambientes incertos. Tal perspectiva sugere que tanto indivíduos, grupos, organizações e sistemas organizacionais buscam compreender o ambiente, antecipar consequências e tomar decisões fundamentadas com base na melhor informação disponível.

No plano coletivo, instituições e Estados se deparam cotidianamente com desafios que afetam a segurança, a estabilidade e o bem-estar social. A crescente complexidade das ameaças contemporâneas, caracterizadas por velocidade, transversalidade e impacto ampliado, demanda atividades especializadas orientadas à coleta, ao tratamento, à análise e à interpretação de dados e informações. A Doutrina da Atividade de Inteligência (ABIN, 2023) define esse processo como sistemático, contínuo e tecnicamente estruturado, tendo como finalidade apoiar o processo decisório, reduzir incertezas e proteger interesses nacionais e institucionais. Dessa forma, a inteligência é compreendida como uma ação integrada de obtenção, análise e difusão de conhecimentos provenientes de múltiplas fontes, abertas ou sigilosas, com o propósito de avaliar temas sensíveis, antecipar ameaças e identificar oportunidades estratégicas.

Bimfort (1958) e Carlisle (2005) ressaltam que o produto de inteligência não consiste apenas no acúmulo de dados, mas na sua transformação em sínteses interpretativas orientadas à tomada de decisão. A relevância da interpretação analítica diferencia a informação bruta do conhecimento estratégico, sendo este último caracterizado pela capacidade de orientar ações, minimizar riscos e aperfeiçoar o planejamento institucional. Essa distinção fundamenta a importância da Inteligência de Fontes Abertas (*Open Source Intelligence – Osint*), cuja expansão nas últimas décadas decorre da crescente digitalização da vida social e da abundância de dados publicamente disponíveis.

A *Osint* compreende o uso sistemático e metodologicamente orientado de informações abertas, obtidas por meio de mídias digitais, registros oficiais, plataformas públicas, redes sociais, bancos de dados, entre outros, para a produção de conhecimento. Embora tais dados estejam acessíveis a qualquer indivíduo, seu valor analítico depende de processos rigorosos de coleta, organização, filtragem, contextualização e interpretação. Portanto, a *Osint* não se confunde com simples pesquisa na internet: trata-se de uma disciplina estruturada da atividade de inteligência que exige método, crítica e validação.

Ainda de acordo com a Doutrina da Atividade de Inteligência (ABIN, 2023), a eficácia da *Osint* deriva da aplicação de métodos especializados de análise, da triangulação de informações e do uso criterioso de processos de avaliação de credibilidade, como a Técnica de Avaliação de Dados (TAD). A crescente velocidade de circulação da informação, aliada à proliferação de conteúdos manipulados, enviesados ou fraudulentos, demanda do analista de inteligência uma postura crítica e capacidade de verificar fontes de maneira contínua e metódica. Assim, a *Osint* emergiu como uma das categorias mais relevantes da atividade de inteligência contemporânea, especialmente pela possibilidade de monitoramento em tempo real do ambiente informacional, identificação de tendências emergentes e antecipação de ameaças em diferentes escalas.

No campo da segurança pública, a *Osint* tornou-se uma ferramenta indispensável para compreender, monitorar e enfrentar redes ilícitas cada vez mais sofisticadas. O acompanhamento sistemático de mídias sociais, plataformas de comércio eletrônico, registros públicos, bases de dados, fóruns digitais e conteúdo jornalístico permite identificar padrões suspeitos, detectar discursos de incitação à violência, mapear conflitos territoriais entre facções, reconhecer movimentações atípicas associadas ao tráfico de drogas, armas e pessoas, além de subsidiar diagnósticos e prognósticos sobre áreas sensíveis, rotas ilícitas e dinâmicas criminais emergentes.

Na prática, por exemplo, a *Osint* possibilita para a segurança pública:

a) monitorar anúncios de armas, munições e explosivos em plataformas digitais;
b) acompanhar postagens de grupos criminosos que exibem arsenais, territórios dominados ou ameaças;
c) detectar mobilizações violentas a partir de *hashtags*, transmissões ao vivo e massas digitais coordenadas;
d) correlacionar perfis, contatos, geolocalizações e padrões comportamentais de suspeitos ligados ao tráfico, milícias e crimes ambientais;
e) identificar golpes financeiros, fraudes e esquemas de estelionato amplamente divulgados *on-line*;
f) rastrear movimentações e rotas de contrabando e descaminho, incluindo comércio irregular de cigarros, eletrônicos e produtos de alto valor;
g) detectar e mapear redes de tráfico ilícito de bens histórico-artístico-culturais, com base em imagens, anúncios e transações em plataformas especializadas;
h) apoiar investigações relacionadas à exploração sexual infantil, pornografia infantil e pedofilia, por meio de monitoramento de perfis, códigos, salas fechadas e *marketplaces* clandestinos;
i) identificar sinais de extremismo violento de motivação interna (EVM-I), incluindo discursos de ódio, radicalização rápida, ameaças veladas e referências simbólicas típicas de grupos extremistas;
j) monitorar potenciais autores de incidentes de violência armada em massa (*mass shootings*), com base em postagens premonitórias, ideação violenta, tentativas de

aquisição irregular de armas e padrões comportamentais consistentes com atiradores em ambientes públicos.

No setor privado, a *Osint* também assume papel significativo, permitindo que analistas e pesquisadores desenvolvam investigações complexas combinando dados *online* e *offline*. A Nato *Osint* Handbook (2002) já apontava que a aplicação sistemática de fontes abertas possibilita reconstruir eventos, identificar atores envolvidos e inferir motivações, padrões e tendências a partir de evidências acessíveis ao público. A *Osint* não apenas contribui para a compreensão de incidentes isolados, mas também auxilia na formulação de hipóteses analíticas e previsões estratégicas.

Diversas áreas se beneficiam diretamente dessa disciplina. A *Osint* é amplamente utilizada na análise de países, organizações e indivíduos, em especial para mapear redes de relacionamento (análise de redes sociais) e compreender percepções e comportamentos coletivos (Pastor-Galindo *et al.*, 2020). Ademais, mostra-se valiosa na identificação de vulnerabilidades processuais, permitindo delinear pontos de intervenção contra atividades ilícitas (Senekal; Kotzé, 2019; Chainey; Berbotto, 2022). No campo da cibersegurança, a *Osint* tornou-se um instrumento essencial para investigar cibercrimes, ataques digitais e ameaças emergentes (Tabatabaei; Wells, 2016; Sari, 2018; Hwang et al., 2022), sendo capaz de antecipar riscos e fortalecer a resiliência organizacional.

Dessa forma, a *Osint* amplia de maneira significativa a capacidade investigativa, preventiva e analítica das instituições policiais e órgãos governamentais, permitindo respostas mais integradas, precisas e tempestivas. Seu uso estruturado fortalece ações interinstitucionais, aprimora o mapeamento de ameaças e contribui para uma atuação estatal mais eficiente diante da crescente complexidade do ambiente criminal contemporâneo.

Ao contrário das atividades estritamente sigilosas, a natureza aberta da *Osint* favorece a cooperação interinstitucional e internacional, estimulando a interoperabilidade entre órgãos governamentais, setor privado, academia e sociedade civil. Essa característica amplia a eficácia na prevenção e no combate a crimes complexos, como tráfico de pessoas, crimes ambientais, terrorismo, fraudes digitais, lavagem de dinheiro e tráfico ilícito de bens culturais. Assim, a *Osint* se apresenta como uma inteligência complementar que robustece as abordagens tradicionais e fortalece a governança informacional do Estado.

A consolidação da *Osint* como disciplina estruturante das ciências policiais representa um avanço significativo para a segurança pública contemporânea. Em um ambiente marcado pela complexidade criminal e pela transnacionalidade das organizações ilícitas, torna-se indispensável desenvolver capacidades de monitoramento, correlação e análise integradas. Este artigo contribui para esse campo ao sistematizar categorias de fontes abertas, métodos de avaliação informacional e ferramentas tecnológicas adequadas ao contexto investigativo e estratégico das instituições policiais.

Na prática, a *Osint* potencializa a atuação das forças de segurança ao possibilitar análises mais precisas, contextualizadas e tempestivas, reduzindo incertezas e ampliando a capacidade de

antecipação. Sua aplicação imediata reforça investigações, otimiza recursos, favorece a cooperação interagências e fortalece o planejamento estratégico, contribuindo diretamente para a eficácia e a modernização das instituições de segurança pública.

Os tópicos subsequentes aprofundam essa análise, abordando inicialmente o conceito de inteligência, suas tipologias e o ciclo de produção do conhecimento. Em seguida, examinam-se os tipos de fontes abertas, critérios de confiabilidade e metodologias de análise. Na sequência, são exploradas ferramentas tecnológicas contemporâneas, seguidas de uma proposta metodológica integrada. Por fim, apresentam-se estudos de caso que demonstram a aplicabilidade prática da *Osint* em contextos reais.

2. O CICLO DE INTELIGÊNCIA

A análise de inteligência constitui um processo estruturado em fases interdependentes, conhecido como ciclo de inteligência, que descreve a trajetória metodológica pela qual dados brutos se transformam em conhecimento aplicável ao processo decisório. Embora diferentes modelos tenham sido propostos (Jensen *et al*., 2017; Phythian, 2013), todos compartilham a lógica de um processo contínuo, dinâmico e retroalimentado, em que cada etapa depende da anterior e contribui para a seguinte.

Na literatura internacional, um dos modelos clássicos é o proposto por Thomas Smith (2003), que organiza o ciclo em cinco fases: (1) planejamento e direção; (2) coleta; (3) processamento; (4) análise e produção; e (5) disseminação. Esse modelo, amplamente difundido em contextos acadêmicos e corporativos, enfatiza a importância da gestão das necessidades informacionais desde o início até a entrega do produto de inteligência.

Por outro lado, a Doutrina da Atividade de Inteligência (ABIN, 2023), que norteia doutrinariamente a atividade de inteligência estatal brasileira, adota uma estrutura semelhante, porém adaptada às especificidades da atividade governamental, com cinco fases principais: (1) planejamento da atividade de inteligência; (2) reunião de dados e informações; (3) processamento de dados e informações; (4) análise e produção de conhecimento; e (5) difusão do conhecimento.

Ao comparar os dois modelos, observa-se que ambos se baseiam em uma lógica cíclica e contínua, mas a doutrina da Agência Brasileira de Inteligência (ABIN) aprofunda o caráter institucional e estratégico do processo. O planejamento, em ambos os casos, representa a etapa de definição de objetivos e requisitos informacionais, porém, enquanto Smith (2003) dá ênfase à direção e coordenação das atividades, a ABIN (2023) incorpora a noção de alinhamento com os interesses e políticas de Estado, além da observância dos princípios de legalidade, legitimidade e oportunidade.

A fase de coleta no modelo de Smith corresponde à reunião de dados e informações na doutrina brasileira. Em ambos, trata-se da obtenção de insumos provenientes de diversas fontes - abertas,

restritas ou sigilosas, mas a ABIN destaca a importância do controle da credibilidade da fonte e da confiabilidade do conteúdo, por meio de métodos como a TAD.

A etapa de processamento, comum aos dois modelos, envolve a transformação dos dados brutos em informações utilizáveis, por meio de filtragem, classificação, codificação ou tradução (Gibson, 2004). A ABIN, contudo, amplia o escopo dessa fase ao incluir o tratamento de dados em ambientes digitais e o emprego de tecnologias de inteligência artificial, reforçando a necessidade de proteção informacional e de segurança cibernética.

A análise e produção de conhecimento é o núcleo de ambos os modelos. Tanto Smith quanto a ABIN concebem essa etapa como o momento em que as informações reunidas são correlacionadas, interpretadas e sintetizadas em hipóteses ou inferências úteis ao processo decisório. Entretanto, a doutrina brasileira enfatiza o caráter coletivo e interdisciplinar da análise, destacando a importância da validação e da revisão crítica do produto final antes de sua difusão.

Por fim, a etapa de disseminação, em Smith (2003), e de difusão do conhecimento, na ABIN (2023), têm o mesmo propósito: entregar ao tomador de decisão um produto de inteligência oportuno, claro e relevante. A diferença reside no enfoque: enquanto Smith trata a disseminação como um ato final, a doutrina da ABIN a entende como uma etapa que realimenta o ciclo, permitindo que o retorno do usuário gere novas demandas informacionais e retroalimente o processo.

Em síntese, a principal distinção entre o modelo clássico de Thomas Smith e o modelo da ABIN reside no enfoque institucional e sistêmico da doutrina brasileira. Enquanto o primeiro privilegia uma visão operacional e analítica da produção de inteligência, o segundo integra dimensões éticas, legais e estratégicas, reforçando o papel da inteligência como instrumento permanente de assessoramento ao Estado e à segurança nacional. Ambos, entretanto, convergem na ideia de que o ciclo de inteligência deve ser contínuo, iterativo e adaptável, garantindo a transformação eficiente de dados em conhecimento confiável e relevante para a decisão.

2.1 Tipos de inteligência moderna

A partir do século XX, o avanço tecnológico e a crescente complexidade dos cenários políticos e militares promoveram uma ampla diversificação das disciplinas de inteligência, cada uma voltada a formas específicas de obtenção, tratamento e análise de informações. O Departamento de Defesa dos Estados Unidos (DoD) consolidou uma classificação amplamente aceita, composta por cinco principais tipos de inteligência, definidas segundo as suas fontes de informação (Thomas Smith, 2003). Essas disciplinas são essenciais para a segurança nacional e a defesa, pois oferecem subsídios estratégicos sobre ameaças potenciais, vulnerabilidades institucionais e oportunidades de ação. Compreender a natureza e as limitações de cada uma permite que gestores públicos, formuladores de políticas e autoridades militares tomem decisões mais precisas e baseadas em evidências.

No contexto brasileiro, a Doutrina da Atividade de Inteligência (ABIN, 2023) também reconhece a existência de múltiplas fontes e disciplinas de coleta, enfatizando que a pluralidade de origens informacionais é indispensável para garantir a abrangência, confiabilidade e tempestividade do conhecimento produzido. Cada modalidade de inteligência é entendida como parte integrante de um sistema unificado, que visa reduzir incertezas e apoiar o processo decisório no âmbito do Estado e da segurança pública.

As principais disciplinas da inteligência moderna incluem:

a) Inteligência de Fontes Humanas (*Human Intelligence – Humint*): coleta de informações obtidas diretamente de pessoas, por meio de entrevistas, observação, agentes, informantes ou fontes confidenciais. No campo da segurança pública, a *Humint* é crucial para acessar dados inacessíveis por meios técnicos, permitindo compreender motivações, intenções e comportamentos (Trisolini, 2020). A Doutrina da Atividade de Inteligência (ABIN, 2023) ressalta que a *Humint* deve ser conduzida de forma ética, legal e orientada pelo princípio da necessidade de conhecer.
b) Inteligência de Imagens (*Imagery Intelligence – Imint*): baseia-se na coleta e interpretação de imagens obtidas por sensores aéreos, satélites ou outros meios ópticos e geoespaciais. Essa disciplina possibilita a análise de terrenos, infraestrutura e movimentação de alvos, sendo amplamente utilizada tanto em contextos militares quanto em operações de segurança e defesa civil.
c) Inteligência de Sinais (*Signals Intelligence – Sigint*): refere-se à interceptação e análise de sinais eletromagnéticos, incluindo comunicações, radares e transmissões eletrônicas. Essa modalidade se subdivide em *Comint* (*Communications Intelligence)* e *Elint* (*Electronic Intelligence*), permitindo identificar comunicações estratégicas e padrões de emissão eletrônica de potenciais adversários.
d) Inteligência de Medição e Assinatura (*Measurement and Signature Intelligence – Masint*): trata-se da coleta e análise de características físicas e técnicas específicas de objetos, fenômenos ou emissões, como assinaturas acústicas, térmicas, nucleares e eletromagnéticas. A *Masint* é utilizada para identificar padrões únicos que diferenciam um alvo de outros, sendo um componente importante em operações de contramedidas e monitoramento tecnológico.
e) Inteligência de Fontes Abertas (*Open Source Intelligence – Osint*): Compreende o uso sistemático de informações disponíveis ao público, como mídias de massa, bases de dados abertas, publicações acadêmicas, relatórios oficiais, registros comerciais e redes sociais. Segundo a ABIN (2023), a *Osint* representa uma das fontes mais acessíveis e de rápido emprego na atividade de inteligência moderna, especialmente em um ambiente informacional caracterizado pela sobrecarga de dados e pela ubiquidade das mídias digitais.

As disciplinas de inteligência diferem quanto aos métodos de coleta e às fontes empregadas, mas convergem em um objetivo comum: transformar dados dispersos em conhecimento estratégico. Assim, tanto no modelo conceitual de Thomas Smith (2003) quanto na abordagem sistêmica da ABIN

(2023), a integração entre as diversas modalidades, humanas, técnicas e abertas, constitui a base de uma inteligência moderna, capaz de responder aos desafios complexos e multifatoriais da segurança e da defesa no século XXI.

2.2 Foco na Inteligência de Fontes Abertas

A coleta de informações para fins de segurança nacional possui uma longa trajetória histórica, sendo uma prática consolidada e constantemente aperfeiçoada (Lowenthal; Clark, 2015; Böhm; Lolagar, 2021). Contudo, a partir da expansão exponencial da internet e da transformação digital das sociedades contemporâneas, a quantidade de dados publicamente disponíveis atingiu proporções inéditas. Estima-se que, no futuro próximo, o volume global de conhecimento poderá duplicar a cada 12 horas (Pllana, 2019). Esse cenário de sobrecarga informacional reposicionou a Inteligência de Fontes Abertas como uma das disciplinas mais relevantes dentro da atividade de inteligência moderna.

De acordo com Ghioni *et al.* (2023), entre 70% e 90% das necessidades informacionais das agências de inteligência e das forças de segurança podem ser supridas por dados provenientes de fontes abertas. Essa estimativa demonstra que a *Osint* não é apenas uma modalidade complementar, mas um eixo estruturante da produção de conhecimento de inteligência na era digital. A Doutrina da Atividade de Inteligência (ABIN, 2023) corrobora essa perspectiva ao reconhecer que as fontes abertas constituem insumos estratégicos essenciais para a produção de conhecimento tempestivo, especialmente em contextos que demandam agilidade e custo reduzido, desde que se preserve a análise crítica e a verificação da credibilidade da informação.

A análise de inteligência não depende apenas de ferramentas ou de volume de dados, mas da capacidade cognitiva e epistemológica do analista. Conforme destaca Clark (2024), a atividade analítica exige pensamento crítico e lógico, habilidade para identificar vieses, formular e testar hipóteses concorrentes e avaliar a consistência interna das informações. Além disso, demanda perspectiva ampla, compreensão histórica e instintos analíticos formados pela experiência e pela exposição a padrões complexos. Dessa forma, a qualidade do produto de inteligência depende tanto da robustez metodológica quanto da maturidade analítica do profissional envolvido.

Em síntese, a ascensão da *Osint* representa uma reconfiguração paradigmática da atividade de inteligência, que passa a operar em um ambiente informacional caracterizado pela abundância de dados, pela velocidade de circulação da informação e pela necessidade crescente de análise crítica e validação de fontes. Tanto a doutrina nacional (ABIN, 2023) quanto a literatura internacional convergem em um ponto essencial: a inteligência contemporânea é, em grande parte, uma inteligência de fontes abertas, cuja eficácia depende menos da exclusividade das informações e mais da capacidade analítica de transformá-las em conhecimento confiável e estratégico.

2.3 Categorizando recursos de inteligência de fontes abertas

Um dos maiores desafios enfrentados na pesquisa em *Osint* consiste na identificação, acesso e validação dos dados disponíveis. O analista que busca construir um panorama completo sobre determinado evento, país, empresa ou indivíduo precisa compreender a ampla variedade de fontes acessíveis e, sobretudo, aplicar o princípio da triangulação informacional, isto é, confirmar informações provenientes de uma fonte a partir de outras fontes independentes, reduzindo riscos de viés, erro ou desinformação (Dorton *et al.*, 2019). A Doutrina da Atividade de Inteligência (ABIN, 2023) também enfatiza a importância da corroboração cruzada de dados como requisito metodológico essencial para a credibilidade do conhecimento produzido, especialmente em um contexto marcado pela proliferação de informações falsas ou manipuladas.

A seguir, são apresentadas as principais categorias de fontes utilizadas na pesquisa *Osint*, bem como suas potencialidades e limitações.

a) Registros Oficiais: os registros oficiais, mantidos por órgãos públicos, constituem uma das fontes mais seguras e detalhadas de informações. Esses bancos de dados oferecem documentos produzidos por instituições governamentais, frequentemente atualizados e juridicamente reconhecidos. No entanto, as diferenças nos sistemas de registro, nos padrões de coleta e nas ferramentas empregadas podem introduzir vieses cognitivos e técnicos (Mariuta, 2014; McDermott et al., 2021). Apesar dessas limitações, continuam sendo o ponto de partida preferencial para análises envolvendo indivíduos, empresas ou propriedades, fornecendo lastro documental e confiabilidade à coleta de dados.

b) Registros Públicos de Empresas: essas bases de dados permitem identificar estruturas de propriedade, afiliações e vínculos corporativos. A análise dessas informações pode revelar relações ocultas, conflitos de interesse, redes ilícitas e práticas de dissimulação. No mercado de arte, por exemplo, traficantes de bens culturais criam empresas de fachada para mascarar atividades ilegais (FATF, 2023). A Doutrina da ABIN (2023) recomenda que o analista utilize técnicas de análise relacional para identificar vínculos entre pessoas jurídicas e físicas, explorando padrões de co-localização, sociedades cruzadas e conexões financeiras. Contudo, o acesso a tais registros varia conforme a legislação de cada país, algumas jurisdições exigem transparência total, enquanto outras permitem constituição de empresas anônimas, o que dificulta a rastreabilidade (Pacini; Stowell, 2020; Montenarh; Marsden, 2024).

c) Registro de Imóveis: os registros de propriedade constituem uma fonte de informações sobre posses, copropriedades e transações imobiliárias, possibilitando a identificação de relações econômicas ou familiares não evidentes. Contratos de compra e herança podem revelar vínculos ocultos ou negócios antigos, servindo como indícios de ligações estratégicas ou ilícitas. Essa abordagem é amplamente utilizada em investigações financeiras e patrimoniais, incluindo casos de corrupção, lavagem de dinheiro e financiamento de atividades criminosas.

d) Listas de Sanções Internacionais: compiladas por governos e organismos multilaterais, como a União Europeia e o Office of Foreign Assets Control (OFAC) dos Estados Unidos, as listas de

sanções reúnem pessoas, empresas e países envolvidos em atividades consideradas ameaçadoras à paz e à segurança internacional. Elas impõem restrições financeiras, comerciais e de deslocamento, configurando ferramentas de pressão política e econômica. Para o analista *OSINT*, essas listas são fundamentais para verificação de conformidade (compliance) e análise de risco reputacional, sendo amplamente empregadas em investigações de due diligence e controle de exportações.

e) Arquivos de Julgamentos Judiciais: os registros judiciais oferecem informações sobre litígios, sentenças, associações criminais e condutas ilícitas de indivíduos e empresas. São fontes decisivas para compreender o histórico legal e reputacional de um alvo investigado, além de permitir a identificação de coautores ou cúmplices. O cruzamento de nomes mencionados nesses processos com outros bancos de dados amplia a capacidade de reconstrução de redes de relacionamento e de análise comportamental.

f) Relatórios Oficiais de Autoridades Públicas: publicações e relatórios técnicos de órgãos governamentais, agências de segurança e instituições de pesquisa contêm dados estatísticos, análises e avaliações setoriais. Embora sejam fontes valiosas, a Doutrina da ABIN (2023) alerta para a necessidade de considerar o contexto institucional e político da produção desses documentos, já que prioridades governamentais ou restrições orçamentárias podem introduzir viés institucional. Ainda assim, são insumos relevantes para a validação de tendências e hipóteses.

g) Imagens Visuais: as imagens comerciais, aéreas, orbitais e de rua representam uma dimensão visual complementar à análise textual. Elas permitem a verificação empírica de informações, como localização, infraestrutura e movimentação de pessoas ou bens (Kovarik, 2011). Plataformas gratuitas, como Google Earth e Street View, e bancos de dados pagos de alta resolução podem ser combinados para compor uma visão mais precisa da área de interesse. Essa técnica é amplamente empregada em due diligence, mapeamento de rotas logísticas, análise de instalações industriais e verificação de incidentes.

h) Mídias de Notícias: os meios de comunicação desempenham papel essencial na obtenção de informações atualizadas e na revelação de fatos ausentes dos registros oficiais. Jornalistas investigativos muitas vezes trazem à luz dados inéditos e contextos políticos, econômicos ou criminais (Hunter, 2011). Ferramentas como Factiva e Nexis Diligence+ oferecem acesso a acervos extensos de notícias e transcrições históricas. Entretanto, é indispensável que o analista *OSINT* aplique critérios de verificação e evite a propagação de desinformação, considerando o impacto das fake news sobre a credibilidade do produto final (Mpala, 2023; Oakley; Rogg, 2024).

i) Literatura Acadêmica: a produção científica (artigos, dissertações e periódicos especializados) constitui fonte de conhecimento técnico e analítico de alta confiabilidade. A revisão por pares e o rigor metodológico garantem qualidade, embora a linguagem especializada possa exigir interpretação crítica. Tais fontes são fundamentais para a contextualização teórica de fenômenos investigados e para a elaboração de hipóteses de pesquisa em inteligência estratégica e de segurança.

j) Blogs e Mídias Sociais: com a explosão das plataformas digitais, conteúdos gerados por usuários se tornaram fontes ricas e dinâmicas de informação (Golbeck, 2015). Fóruns, blogs, redes sociais e plataformas de compartilhamento de vídeos oferecem dados espontâneos, não estruturados e contextuais. No entanto, exigem habilidade analítica, ética e técnica para interpretar o conteúdo de forma confiável (Rønn; Søe, 2019). O uso de mídias sociais na *OSINT* requer cautela quanto à autenticidade, intenção e contexto das postagens, evitando interpretações distorcidas (Trottier, 2015).

k) Portais de Dados Abertos Governamentais: os portais de dados abertos governamentais – como dados.gov.br, IBGE, Eurostat, DataGov (EUA) e plataformas temáticas da ONU – representam um ecossistema estruturado de informações oficiais disponibilizadas de forma transparente pelo Estado. Essas bases, compostas por séries estatísticas, indicadores socioeconômicos, ambientais, territoriais e administrativos, permitem análises macroestratégicas e diagnósticos aprofundados sobre dinâmicas populacionais, infraestruturais e setoriais. Para a ABIN (2023), tais dados constituem insumos essenciais para análises prospectivas, modelagem de cenários e identificação de tendências estruturais. Contudo, sua utilização exige rigor metodológico, dado que a periodicidade de atualização, a granularidade das variáveis e as assimetrias regionais podem introduzir lacunas analíticas, demandando complementação com outras fontes independentes.

l) Bases de dados de bens histórico-artístico-culturais subtraídos e alertas patrimoniais: constituem instrumentos estratégicos na proteção do patrimônio e no enfrentamento ao tráfico ilícito. Plataformas especializadas, como INTERPOL Works of Art, ICOM Red Lists, Carabinieri TPC e registros de museus internacionais, possibilitam a verificação de proveniência, a identificação de objetos subtraídos e o rastreamento de redes envolvidas em crimes contra o patrimônio cultural. Esses sistemas estruturam informações sobre peças desaparecidas, rotas de tráfico, modus operandi de grupos criminosos e classificações iconográficas sensíveis, permitindo análises de correlação e atribuição. A integração dessas bases a metodologias *OSINT* amplia significativamente a capacidade de validação e *cross-matching*, ao possibilitar o confronto entre imagens, descrições, medidas, marcas distintivas, histórico de circulação e proveniências declaradas. Ainda assim, a eficácia desse processo depende da notificação prévia de roubos e da cooperação interinstitucional, uma vez que grande parte dos artefatos subtraídos nunca chega a ser formalmente registrada. Nessas situações, torna-se indispensável a triangulação com fontes visuais, registros de mercado, *marketplaces* on-line, leiloeiras, mídias abertas e, quando aplicável, varreduras em ambientes *deep web* e *dark web,* a fim de identificar padrões, ofertas suspeitas e conexões com redes internacionais.

m) Registros de Propriedade Intelectual e Patentes: Sistemas internacionais de propriedade intelectual, como WIPO, EPO, USPTO e INPI – constituem um núcleo de dados estratégicos sobre inovação tecnológica, titularidade de patentes, padrões de desenvolvimento industrial e redes tecnológicas emergentes. No campo da análise de inteligência, esses registros permitem mapear capacidades produtivas, identificar empresas-laranja atuando como fachada tecnológica, caracterizar cadeias de inovação e antecipar disputas geoeconômicas. Patentes também revelam padrões de investimento e prioridades de Pesquisa & Desenvolvimento (P&D) de Estados e corporações. Todavia, sua interpretação exige

competências técnicas especializadas, uma vez que a linguagem científica e jurídica pode ocultar relações indiretas ou operações de dissimulação estruturadas para evitar rastreamento.

n) Portais de Licitações, Contratos e Compras Públicas: Plataformas como PNCP, ComprasGov, e sistemas estaduais e municipais de licitação permitem o escrutínio de fluxos financeiros públicos, padrões de contratação, vínculos entre empresas concorrentes e histórico de fornecimento ao Estado. No campo da inteligência, são ferramentas indispensáveis para análises de integridade, identificação de cartéis, rastreamento de corrupção, mapeamento de favorecimentos ilícitos e detecção de empresas de fachada. A ABIN (2023) recomenda que os analistas correlacionem esses registros com bases societárias, dados financeiros e relatórios públicos, permitindo identificar anomalias estatísticas, concentrações artificiais e redes econômico-administrativas. Contudo, contratos fragmentados, editais pouco transparentes e consórcios empresariais opacos podem dificultar a rastreabilidade, exigindo maior triangulação.

o) Bases de Tráfego Marítimo (AIS): Sistemas de Identificação Automática (AIS), como MarineTraffic e VesselFinder, fornecem dados em tempo real sobre posição, rotas, bandeiras, proprietários e características técnicas de embarcações. Esses sistemas são fundamentais para rastrear fluxos logísticos internacionais, identificar rotas suspeitas, detectar transponders desligados (*dark vessels*) e mapear redes marítimas associadas ao tráfico ilícito, contrabando ou escoamento de bens culturais. A análise *OSINT* dessa categoria integra dados geoespaciais, indicadores portuários e registros alfandegários, permitindo compreender padrões operacionais e comportamentos anômalos. Contudo, o uso de embarcações sem identificação, bandeiras de conveniência e triangulações logísticas reduz a completude dos registros, demandando validação cruzada com imagens de satélite e dados aduaneiros.

p) Dados de Aviação (ADS-B e Registros Aeronáuticos): Dados provenientes de ADS-B Exchange, FlightRadar24, ICAO e ANAC possibilitam monitorar trajetórias, proprietários, matrículas e padrões de voo de aeronaves. Na perspectiva da inteligência, essas fontes permitem rastrear deslocamentos estratégicos, identificar aeronaves de fachada, correlacionar movimentações aéreas com eventos investigados e monitorar rotas potencialmente usadas para transporte ilícito de bens culturais ou atividades clandestinas. A análise integrada desses registros permite detectar padrões de voo incompatíveis, trajetórias ocultadas por bloqueio de transponders e vínculos com empresas situadas em paraísos fiscais. No entanto, trusts aeronáuticos e registros parcialmente públicos impõem limitações que exigem complementaridade com dados corporativos e aduaneiros.

q) Infraestrutura Digital (Whois, DNS, SSL e Certificados Digitais): Investigação de ativos digitais por meio de consultas de Whois, DNS inverso, servidores, certificados SSL e logs de transparência (CT Logs) constitui um componente crucial para a atribuição cibernética e o rastreamento de atores digitais. Esses dados revelam proprietários de domínios, hospedagem, padrões de anonimização, data de criação, estrutura de rede e vínculos tecnológicos associados a operações ilícitas, campanhas de desinformação ou comércio clandestino. O cruzamento dessas informações com bases de reputação digital permite caracterizar ecossistemas de risco. Contudo, o uso de proxies, registradores internacionais

permissivos e redes de anonimização limita a capacidade de atribuição direta, impondo a integração com técnicas avançadas de correlação *OSINT*.

r) Repositórios de Código, Pastes e Vazamentos Digitais: Plataformas como GitHub, GitLab, Bitbucket, Pastebin e fóruns de vazamentos são fontes de alto valor para identificar credenciais expostas, configurações internas, códigos de sistemas, APIs sensíveis e indícios de compromissos cibernéticos. Esses ambientes frequentemente revelam falhas operacionais, erros de configuração, práticas inseguras e informações inadvertidamente divulgadas por desenvolvedores. Na análise de inteligência, esse recurso permite mapear capacidades digitais, identificar vulnerabilidades e antecipar explorações maliciosas. No entanto, o analista deve atuar em estrita conformidade com normativos legais e éticos, uma vez que o manuseio de dados sensíveis exige salvaguardas e conformidade com a proteção de dados e privacidade.

s) Perfis Profissionais, Currículos e Anúncios de Emprego: Perfis profissionais em LinkedIn, plataformas corporativas, repositórios de currículos e anúncios de emprego constituem fontes essenciais para mapear competências individuais, reestruturações organizacionais, necessidades de recrutamento e adoção de tecnologias sensíveis. Esses dados permitem inferir capacidades operacionais, identificar mudanças estratégicas em instituições e detectar padrões de mobilidade profissional. No campo da inteligência estratégica, auxiliam na compreensão de ecossistemas profissionais, formações de equipes e expansão de empresas. Entretanto, informações exageradas, contas falsas e construções de marketing pessoal impõem cautela, exigindo verificação cruzada com outras fontes.

t) Plataformas de Comércio Eletrônico e Marketplaces Digitais: Marketplaces como eBay, Mercado Livre, Etsy, leilões digitais e plataformas baseadas em criptomoedas compõem um ambiente dinâmico para a detecção de objetos culturais suspeitos, artefatos de procedência duvidosa e padrões de comercialização ilícita. Esses espaços permitem monitorar volumes de oferta, preços anômalos, recorrência de vendedores, uso de métodos de pagamento criptografados e estratégias de ocultação. A análise *OSINT* desse recurso integra técnicas visuais, histórico de anúncios, correlação com bases de arte roubada e identificação de perfis vendedores. Contudo, contas efêmeras, uso de VPNs e mercados emergentes do dark web dificultam a rastreabilidade, exigindo

O quadro sinóptico a seguir sintetiza, de maneira estruturada e funcional, as vinte categorias de recursos de Inteligência de Fontes Abertas (*OSINT*) apresentadas na seção anterior, relacionando cada tipo de fonte às suas utilidades analíticas e aos produtos típicos gerados no âmbito da atividade de inteligência. Essa sistematização permite visualizar, de forma integrada, como diferentes modalidades de dados (documentais, digitais, visuais, estatísticas, normativas e relacionais) alimentam distintas fases do ciclo de inteligência, apoiando análises táticas, operacionais e estratégicas. Ao organizar os recursos segundo sua natureza e aplicabilidade, o quadro auxilia o analista na seleção metodológica mais apropriada para cada problema de inteligência, em consonância com a abordagem de triangulação e validação preconizada pela Doutrina da Atividade de Inteligência (ABIN, 2023).

Quadro 1 – Utilização Analítica dos Recursos *Osint*

Categoria *OSINT*	Tipo de Dado	Uso Analítico na Inteligência	Produto Gerado
Registros oficiais	Documental	Verificação jurídica e contextual	Dossiê básico
Registros de empresas	Societário	Análise de vínculos e ocultação	Mapa relacional
Registro de imóveis	Patrimonial	Identificação de laços econômicos	Perfil patrimonial
Sanções internacionais	Normativo	Avaliação de risco e compliance	Quadro de restrições
Arquivos judiciais	Legal	Reconstrução de histórico e redes	Linha do tempo jurídica
Relatórios governamentais	Técnico-institucional	Identificação de tendências	Análise setorial
Imagens visuais	Geoespacial	Verificação de locais e rotas	Mapa analítico
Notícias	Midiático	Atualização e contextualização	Síntese factual
Literatura científica	Teórico-analítica	Formulação de hipóteses	Fundamentação
Mídias sociais	Comportamental	Monitoramento de atores e discursos	Análise sociotécnica
Dados governamentais abertos	Estatístico	Análise macroestrutural	Cenários e tendências
Bens histórico-artístico-culturais subtraídos	histórico-artístico-cultural	Verificação de proveniência	Atribuição de objeto
Patentes	Tecnológico	Mapeamento de capacidades	Estudo geoeconômico
Licitações	Financeiro-administrativo	Detecção de irregularidades	Due diligence
AIS marítimo	Logístico	Rastreio de rotas e navios	Análise portuária
ADS-B aeronáutico	Mobilidade	Monitoramento de trajetórias	Relatório de movimentação
Whois/DNS/SSL	Digital	Atribuição técnica	Mapa cibernético
Repositórios de código	Técnico-operacional	Detecção de vulnerabilidades	Alerta de risco
Perfis profissionais	Recursos humanos	Análise de competências e estruturas	Organograma inferido
Marketplaces	Comercial	Identificação de objetos ilícitos	Relatório de mercado

Fonte: Elaborado pelos autores.

A inclusão desse quadro sinóptico no artigo tem relevância metodológica e científica significativa, pois consolida de forma clara e objetiva o conjunto de recursos *OSINT* que fundamentam a atividade analítica contemporânea. Ao oferecer uma visão panorâmica e comparativa das fontes, o quadro orienta o leitor, especialmente profissionais de segurança pública, analistas de inteligência e pesquisadores, quanto às possibilidades, limites e aplicações práticas de cada tipo de dado. Além disso, favorece o alinhamento do processo investigativo às boas práticas descritas na Doutrina da Atividade de Inteligência (ABIN, 2023), reforçando a necessidade de escolhas criteriosas de fontes, validação cruzada e rigor técnico. Em síntese, o quadro contribui para a padronização conceitual, fortalece a compreensão da arquitetura operacional da *OSINT* e amplia a robustez analítica do artigo.

Em síntese, a efetividade da *OSINT* depende da integração de múltiplas fontes e da triangulação sistemática das informações. Conforme orienta a Doutrina da Atividade de Inteligência (ABIN, 2023), o analista deve combinar a amplitude das fontes abertas com o rigor metodológico da análise crítica, garantindo que os produtos de inteligência derivados dessas informações mantenham credibilidade, precisão e valor estratégico

2.4 Avaliando Fontes Disponíveis

A credibilidade de qualquer produto de inteligência depende diretamente da qualidade das fontes utilizadas. Conforme apontam autores clássicos da área, os três pilares fundamentais de um processo de inteligência são fontes, software e análise, elementos que se integram para transformar dados dispersos em conhecimento estratégico validado. Entretanto, como enfatiza a Doutrina da Atividade de Inteligência (ABIN, 2023), a abundância informacional traz consigo o desafio da avaliação crítica das fontes, uma vez que nem todas apresentam o mesmo grau de confiabilidade, atualidade ou precisão.

Para mitigar esses riscos, as agências de inteligência (civis, militares e de aplicação da lei) empregam sistemas padronizados de avaliação de fontes e informações, que auxiliam o analista a mensurar tanto a confiabilidade da origem quanto a veracidade ou plausibilidade do conteúdo. Entre esses modelos, destaca-se o sistema 6×6, amplamente consagrado e utilizado no Brasil, cuja influência matricial é norte-americana. Ele foi desenvolvido a partir da obra seminal de Washington Platt, *A Produção de Informações Estratégicas* (Platt, 1974, p. 240), e permanece adotado pelo Exército dos Estados Unidos, conforme previsto no *Field Manual* de Operações de Coleta de Inteligência Humana (FM 2-22.3).

Esse método atribui classificações independentes à fonte e à informação, gerando uma matriz combinada que orienta o analista quanto ao grau de confiabilidade e à consistência do dado. Assim, o sistema 6×6 se torna um instrumento fundamental para reduzir incertezas, padronizar julgamentos analíticos e aprimorar a qualidade das estimativas produzidas no ciclo de inteligência.

Quadro 2 – Sistema 6 × 6

Avaliação da fonte	Descrição	Avaliação da informação	Descrição
A	Fonte absolutamente idônea	1	Confirmado por outras fontes
B	Fonte usualmente idônea	2	Provavelmente verdadeiro
C	Fonte razoavelmente idônea	3	Possivelmente verdadeiro
D	Fonte nem sempre idônea	4	Duvidoso
E	Fonte inidônea	5	Improvável
F	Não pode ser julgada a idoneidade da fonte	6	Difícil de determinar

Fonte: Adaptado de Platt (1974, p. 240).

No modelo, a avaliação da fonte diz respeito à análise da sua credibilidade e histórico de acerto, levando em consideração fatores como:

a) a competência técnica ou experiência no tema tratado;

b) o acesso direto ou indireto à informação;

c) o registro de confiabilidade anterior (veracidade das informações previamente fornecidas);

d) o grau de independência da fonte (possíveis interesses, alinhamentos ou motivações pessoais).

Já a avaliação da informação se refere à consistência e plausibilidade dos dados apresentados, considerando aspectos como:

a) a coerência interna do conteúdo;

b) o nível de detalhe e precisão factual;

c) a corroboração com outras fontes independentes;

d) a verificação empírica (por meio de evidências, documentos ou observações diretas).

Dessa forma, uma informação classificada como A1 - fonte confiável e informação confirmada independentemente - representa alto grau de confiança, enquanto uma informação C3 ou E5 indica incerteza significativa, exigindo verificação complementar antes de ser incorporada ao produto de inteligência.

A Doutrina da Atividade de Inteligência (ABIN, 2023) reforça a importância dessa sistematização, especialmente na Técnica de Avaliação de Dados (TAD), que constitui um procedimento oficial brasileiro para mensurar a credibilidade da fonte e a veracidade do conteúdo. Tal metodologia é aplicada rotineiramente em operações de obtenção e análise, garantindo que o produto final seja construído sobre fundamentos verificáveis e metodologicamente sólidos.

Em síntese, a avaliação das fontes disponíveis deve combinar rigor técnico, discernimento analítico e registro sistemático, permitindo que o analista atribua pesos diferenciados às informações e evite conclusões precipitadas. Assim, tanto o modelo 6 × 6 quanto a TAD representam ferramentas essenciais para o controle de qualidade da inteligência, assegurando que o conhecimento produzido mantenha alta confiabilidade, rastreabilidade e valor estratégico para os tomadores de decisão.

3. CONSIDERAÇÕES FINAIS

A Inteligência de Fontes Abertas consolidou-se como um dos pilares fundamentais da atividade de inteligência contemporânea, especialmente em um cenário marcado pela hiperconectividade, pela velocidade da informação e pela crescente sofisticação das ameaças à segurança pública e institucional. A análise desenvolvida ao longo deste artigo demonstra que a *OSINT* não é apenas uma modalidade técnica de coleta de dados, mas um verdadeiro sistema de produção de conhecimento, que articula tecnologia, metodologia e capacidade crítica do analista para transformar informações dispersas em insumos estratégicos de alto valor.

A eficácia da *OSINT* está diretamente relacionada à habilidade humana de interpretar contextos, identificar padrões, questionar evidências e validar hipóteses, competências que exigem pensamento crítico, lógica apurada, objetividade e uma compreensão histórica dos fenômenos investigados. Assim, embora os instrumentos tecnológicos ampliem significativamente o alcance e a velocidade da análise, é o analista, com seus juízos, sua experiência e sua capacidade de síntese, o elemento central para garantir clareza, precisão e utilidade ao produto final.

O estudo realizado também evidencia que, no campo das ciências policiais e da segurança pública, a *OSINT* constitui uma ferramenta estratégica para antecipar ameaças, identificar redes criminosas, detectar fluxos ilícitos, compreender dinâmicas territoriais e apoiar decisões em níveis tático, operacional e estratégico. A sistematização apresentada sobre categorias de fontes abertas, métodos de avaliação informacional e ferramentas tecnológicas oferece aos profissionais uma base metodológica sólida para aprimorar processos investigativos, fortalecer o planejamento institucional e promover uma cultura de inteligência orientada pela evidência.

No entanto, a complexidade crescente do ambiente informacional indica que este é apenas o início de uma trajetória mais ampla de desenvolvimento da disciplina. Os desafios relacionados à desinformação, aos vieses algorítmicos, à manipulação de conteúdos e à necessidade de proteção da privacidade e da segurança operacional demandam abordagens cada vez mais sofisticadas, integradas e tecnicamente fundamentadas.

Diante disso, abrem-se diversos caminhos promissores para trabalhos futuros:

a) Desenvolvimento de metodologias padronizadas de *OSINT* adaptadas às necessidades específicas das polícias e agências de segurança pública, visando padronizar processos e elevar o nível de interoperabilidade entre instituições.

b) Estudos sobre a integração entre *OSINT*, análise preditiva e técnicas de prospecção de cenários, com foco em fortalecer a atuação estratégica em contextos de elevada volatilidade e incerteza.

c) Pesquisa aplicada sobre o uso de inteligência artificial e mineração de dados em *OSINT*, examinando limites éticos, mecanismos de responsabilização e formas de mitigação de vieses algorítmicos.

d) Modelagem de redes criminosas utilizando dados exclusivamente de fontes abertas, de modo a avaliar até que ponto a análise relacional pode revelar estruturas encobertas sem recorrer a fontes sigilosas.

e) Criação de indicadores de desempenho da atividade *OSINT*, permitindo mensurar sua efetividade, pertinência e impacto real no processo decisório policial e governamental.

f) Estudos específicos sobre o emprego de *OSINT* no enfrentamento do tráfico de bens culturais, temática ainda pouco explorada, mas que apresenta amplo potencial para cooperação internacional e inovação metodológica.

g) Investigações sobre a formação, capacitação e perfil cognitivo esperado de analistas *OSINT*, considerando que habilidades como pensamento crítico, visão global, criatividade, objetividade e sensibilidade ética são determinantes para a qualidade da inteligência produzida.

Em síntese, a *OSINT* representa uma disciplina viva, em evolução contínua, cuja relevância tende a crescer na mesma proporção em que aumenta a complexidade informacional das sociedades contemporâneas. Seu futuro será moldado pela capacidade das instituições de combinar tecnologia avançada, rigor metodológico e excelência humana, elementos indispensáveis para que o conhecimento produzido seja confiável, tempestivo e acionável. Ao investir no aperfeiçoamento da *OSINT*, avançam-se não apenas as capacidades de inteligência, mas a própria governança da segurança pública, fortalecendo a prevenção, a antecipação e a tomada de decisão baseada em evidências.

REFERÊNCIAS

BIMFORT, M. T. A definition of intelligence. **Studies in Intelligence**, v. 2, p. 75–78, 1958.

BÖHM, I.; LOLAGAR, S. Open source intelligence: introduction, legal, and ethical considerations. **International Cybersecurity Law Review**, v. 2, p. 317–337, 2021.

CARLISLE, R. **Encyclopedia of intelligence and counterintelligence**. Routledge, 2005.

CENTRAL INTELLIGENCE AGENCY (CIA). **The IC OSINT Strategy** 2024-2026. 2024. Disponível em: https://www.cia.gov/static/9d89dd9a4fe41b63cfab00c5191a8803/IC-OSINT-Strategy.pdf

CHAINEY, S.; RATCLIFFE, J. **GIS and crime mapping**. John Wiley & Sons, 2005.

DORTON, S. L.; FROMMER, I. D.; GARRISON, T. M. A theoretical model for assessing information validity from multiple observers. In: **2019 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)**. IEEE, 2019. p. 52-58.

EUROPEAN UNION. **What is OSINT:** Open-source intelligence? European Data, 2022. Disponível em: https://data.europa.eu/en/publications/datastories/what-osint-open-source-intelligence

FINANCIAL ACTION TASK FORCE (FATF). **Annual Report 2022-2023**. 2023. Disponível em: https://www.fatf-gafi.org/en/publications/Fatfgeneral/FATF-Annual-report-2022-2023.html

GHIONI, R.; TADDEO, M.; FLORIDI, L. Open source intelligence and AI: a systematic review of the GELSI literature. **AI & Society**, v. 39, p. 1827–1842, 2023.

GIBSON, S. Open source intelligence. **RUSI Journal**, v. 149, p. 16-22, 2004.

GOLBECK, J. **Introduction to social media investigation**: a hands-on approach. Syngress Publishing, 2015.

HENRICO, S.; PUTTER, D. Intelligence collection disciplines – a systematic review. **Journal of Applied Security Research**, v. 19, p. 1–25, 2024.

HWANG, Y. et al. Current status and security trend of OSINT. **Wireless Communications and Mobile Computing**, v. 2022, p. 1–14, 2022.

JENSEN, C. J.; McELREATH, D. H.; GRAVES, M. **Introduction to intelligence studies**. London: Routledge, 2017.

KOVARIK, V. **Imagery intelligence (IMINT)**. Brno: University of Defence, 2011.

LAVIGNE, V.; GOUIN, D. Visual analytics for cyber security and intelligence. **Journal of Defense Modeling and Simulation**, v. 11, p. 175–199, 2014.

LEGG, S.; HUTTER, M. A collection of definitions of intelligence. **Frontiers in Artificial Intelligence and Applications**, v. 157, p. 17–24, 2007.

LOWENTHAL, M. M.; CLARK, R. M. **The five disciplines of intelligence collection**. Sage, 2015.

MARIUTA, S. Principles of security and integrity of databases. **Procedia Economics and Finance**, v. 15, p. 401–405, 2014.

McDERMOTT, Y.; KOENIG, A.; MURRAY, D. Open source information's blind spot: human and machine bias in international criminal investigations. **Journal of International Criminal Justice**, v. 19, p. 85–105, 2021.

MONTENARH, J.; MARSDEN, S. Unmasking the oligarchs – using open source data to detect sanctions violations. **Journal of Economic Criminology**, v. 3, p. 100055, 2024.

MPALA, D. K. **Combating disinformation in modern conflict reporting**. 2023. Disponível em: https://nla.brage.unit.no/nla-xmlui/handle/11250/3119493

NORTH ATLANTIC TREATY ORGANIZATION (NATO). **NOSINT Handbook**. 2002. Disponível em: https://archive.org/details/NATOOSINTHandbookV1.2/mode/2up

OAKLEY, D. P.; ROGG, J. Spreading the "smog of war": the impact of propaganda, social media, and OSINT on U.S. civil-intelligence relations. **Intelligence and National Security**, v. 39, n. 3, p. 539–553, 2024.

PACINI, C.; STOWELL, N. F. Panama Papers and the abuse of Shell entities. In: PURDA-HEELER, L.; SAADI, S. (eds.). Corporate fraud exposed. **Emerald Publishing Limited**, 2020. p. 361-382.

PASTOR-GALINDO, J. et al. The not yet exploited goldmine of OSINT. **IEEE Access**, v. 8, p. 10282–10304, 2020.

PHYTHIAN, M. **Understanding the intelligence cycle**. Routledge, 2013.

PLATT, W. **A produção de informações estratégicas**. Tradução de Álvaro Galvão Pereira e Heitor Aquino Ferreira. Rio de Janeiro: Biblioteca do Exército; Livraria Agir Editora, 1974.

PLLANA, D. Expanding entire volume of knowledge. **Global Journal of Human-Social Science**, v. 19, n. 8, p. 32–42, 2019.

RØNN, K.; SØE, S. Is social media intelligence private? **Intelligence and National Security**, v. 34, p. 362–378, 2019.

SABRY, F. **Gestione del ciclo dell'intelligence**. Un Miliardo Di Ben Informato, 2024.

SARI, A. Context-aware intelligent systems for fog computing environments. In: MAHMOOD, Z. (ed.). **Fog computing**. Springer, 2018. p. 205–255.

SENEKAL, B.; KOTZÉ, E. Open source intelligence for conflict monitoring. **African Security Review**, v. 28, p. 1–19, 2019.

SMITH, C. L.; BROOKS, D. J. **Security science**: the theory and practice of security. Butterworth-Heinemann, 2013.

TABATABAEI, F.; WELLS, D. OSINT in the context of cyber-security. In: **Open Source Intelligence Investigation**. Springer, 2016. p. 213–231.

THOMAS SMITH, W. **Encyclopedia of the Central Intelligence Agency**. Infobase Publishing, 2003.

TOMINSKI, C.; SCHUMANN, H. **Interactive visual data analysis**. A K Peters/CRC Press, 2020.

TRISOLINI, M. **Intelligence di polizia**: Le forze dell'ordine come human sensors. Società Italiana di Intelligence, 2020. Disponível em: https://press.socint.org/index.php/home/catalog/book/2020_12_trisolini

TROTTIER, D. Open source intelligence, social media and law enforcement. European **Journal of Cultural Studies**, v. 18, p. 530–547, 2015.

VAN PUYVELDE, D.; TABÁREZ, R. F. The rise of open-source intelligence. **European Journal of International Security**, p. 1-15, 2025. Disponível em: https://doi.org/10.1017/eis.2024.61.