U.PORTO
FLUP FACULDADE DE LETRAS
UNIVERSIDADE DO PORTO

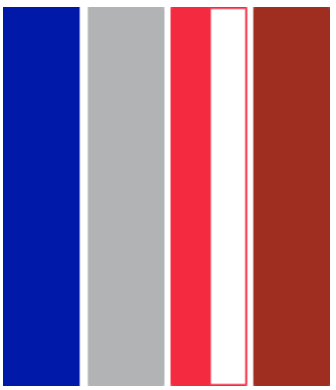
CICLO DE ESTUDOS
MESTRADO EM CIÊNCIAS DA COMUNICAÇÃO (MEDIA E JORNALISMO)

OSINT NO JORNALISMO:
Potenciais, limites e dilemas éticos das investigações jornalísticas em fontes abertas

Fernando Ameno Pinheiro Martins

M

2025



Fernando Ameno Pinheiro Martins

OSINT NO JORNALISMO:
Potenciais, limites e dilemas éticos das investigações jornalísticas em fontes abertas

Dissertação realizada no âmbito do Mestrado em Ciências da Comunicação (Media e Jornalismo), orientada pelo Professor Doutor Fernando Zamith

Faculdade de Letras da Universidade do Porto

2025

Este trabalho está licenciado ao abrigo de uma licença CC BY 4.0

Aos acasos, que me trouxe nesse lugar,

As adversidades, que nunca me impediram de sonhar,

Aos caminhos, que mesmo sinuosos, têm muito a nos ensinar

Sumário

Agradecimentos 8
Resumo 9
Abstract 10
Índice de Figuras 11
Índice de Tabelas 12
Lista de abreviaturas e siglas 13
INTRODUÇÃO 14
Contextualização da era digital e surgimento de OSINT 14
Justificativa do tema 16
Objetivos 17
Estrutura do trabalho 17
1. CONCEITUAÇÃO DE OSINT 18
1.1. Definições e fundamento teórico 18
1.2. Evolução histórica 21
1.3. Métodos, técnicas e automação 23
2. OSINT EM DIFERENTES DOMÍNIOS 27
2.1. OSINT e cibersegurança 28
2.2. OSINT em investigação criminal e segurança pública 31
2.3. OSINT em contexto de conflito e geopolítica 34
3. OSINT E JORNALISMO 35
3.1. Deontologia jornalística e jornalismo de dados 37
3.2. OSINT como fact-check 40
3.3. Comunidades colaborativas e crowdsourcing 42
3.4. Casos de utilização de OSINT no jornalismo investigativo 44
3.5. Privacidade e proteção de dados pessoais 48
4. METODOLOGIA 51
4.1. Perguntas de investigação 51
4.2. Estratégia metodológica 52
4.3. Modelo de questionário 53
5. ANÁLISE DE DADOS 55
CONCLUSÃO 68
Principais achados 68
Limitações do estudo 70
Possibilidades futuras de pesquisa 71
Referências Bibliográficas 73

Declaração de honra / *Declaration of Honour*

Declaro que a presente dissertação é de minha autoria e não foi utilizada previamente noutro curso ou unidade curricular, desta ou de outra instituição. As referências a outros autores (textos, trabalhos, ideias) respeitam escrupulosamente as regras de atribuição de autoria e encontram-se devidamente indicadas no texto e nas referências bibliográficas, de acordo com as normas de referenciação. Tenho consciência de que a prática de plágio e auto-plágio constitui um ilícito académico.

I hereby declare that this dissertation is of my authorship and has not been used previously in another course, degree, curricular unit or subject, at this or any other institution. References to other authors (statements, ideas, thoughts) scrupulously respect the rules of attribution and are duly indicated in the text and bibliographical references, in accordance with the rules of referencing. I am aware that the practice of plagiarism and self-plagiarism is an academic offence.

Declaro, ainda, que utilizei ferramentas de inteligência artificial generativa (chatbots baseados em grandes modelos de linguagem) para realização de partes da presente dissertação, encontrando-se todas as interações (prompts e respostas) transcritas em anexo ao trabalho.

I further declare that I have used generative artificial intelligence tools (chatbots based on large language models) to carry out parts of this dissertation/report, and that all interactions (prompts and responses) have been transcribed in the annex to this work.

Porto, 30 de Setembro de 2025 / *Porto, September, 30rd, 2025*

Fernando Ameno Pinheiro Martins

Agradecimentos

A vida é um processo, já dizia um advogado. Repleta de nuances e surpresas, ela nos instiga a dançar conforme o ritmo, ainda que as evidências apontem para um rumo diferente. No percurso desta investigação, aprendi não apenas sobre o potencial que o OSINT tem de transformar o jornalismo, mas também sobre a brevidade de nossa existência neste plano mundano. No fim das contas, tudo se resume às pessoas: seja para orientar os resultados que uma máquina oferece, seja para proporcionar as emoções que apenas o humano é capaz de transmitir. E, por falar em pessoas, não poderia deixar de mencionar aquelas que contribuíram de forma fundamental para mais esta conquista…

Palmério, Isabel, Laerte, Francisco e Olívia, por agregar igual feijão tropeiro à brasileira,

Thiago, pel'amar além da fronteira,

Mainha e Nhambiquara, por me ensinar o questionar e induzir o persistir,

A Raquel, pelo partilhar do mesmo sonhar!

Resumo

Esta dissertação analisa a utilização da inteligência em fontes abertas (OSINT) no jornalismo, entendendo "inteligência" no sentido de produção e tratamento de informações a partir de dados acessíveis publicamente. O estudo investiga sua aplicabilidade, limitações e dilemas éticos, a partir de revisão bibliográfica, análise de reportagens e de 25 inquéritos com profissionais de diferentes áreas. Buscou-se compreender de que forma o processo de OSINT é incorporado às práticas jornalísticas e quais potencialidades ainda permanecem pouco exploradas. Os resultados indicam que, embora o jornalismo já recorra a técnicas de OSINT, sua aplicação concentra-se sobretudo na coleta de dados, com menor domínio das etapas de análise e visualização. A pesquisa também evidenciou preocupações éticas e legais recorrentes, especialmente relacionadas ao uso de dados pessoais e à confiabilidade das ferramentas. Conclui-se que o jornalismo pode ampliar significativamente sua capacidade investigativa ao adotar abordagens interdisciplinares de OSINT, desde que alinhadas a princípios éticos, metodológicos e legais.

Palavras-chave: OSINT; Inteligência em fontes abertas; Jornalismo investigativo; Ética; Privacidade

Abstract

This dissertation examines the use of Open Source Intelligence (OSINT) in journalism, understanding “intelligence” as the production and processing of information derived from publicly accessible data. The study explores OSINT’s applicability, limitations, and ethical dilemmas, combining a literature review with surveys conducted with 25 professionals from different fields. The research aimed to understand how OSINT processes are incorporated into journalistic practice and which potentialities remain underexplored. Findings indicate that, although journalism already employs OSINT techniques, their use is mostly limited to data collection, with less mastery of analysis and visualization stages. The study also revealed recurrent ethical and legal concerns, particularly regarding the handling of personal data and the reliability of tools. It concludes that journalism can significantly enhance its investigative capacity by adopting interdisciplinary OSINT practices, provided they remain consistent with ethical, methodological, and legal principles.

Key-words: OSINT; Open-source intelligence; Investigative journalism; Ethics; Privacy.

Índice de Figuras

Figura 1- Tipos de fontes OSINT disponíveis 22
Figura 2 - Metodologia OSINT 24
Figura 3 - Princípios para profissionais OSINT 25
Figura 4 - Tipos de OSINT utilizados no Jornalismo 25
Figura 5 - Tipos de aplicação OSINT 27
Figura 6 - Fases de um ataque cibernético e aplicação OSINT 28
Figura 7 - Framework Verificação Multimídia 41
Figura 8 - Média do grau de essencialidade do uso de OSINT por etapa 61

Índice de Tabelas

Tabela 1 – Área profissional e identificação dos participantes 56

Tabela 2 – Ferramentas OSINT e suas funções 57

Tabela 3 – Utilização OSINT em diferentes áreas 62

Lista de abreviaturas e siglas

OSINT	Open source intelligence
OSINV	Open source investigation
SOCMINT	Social Media Intelligence
GEOINT	Geospatial Intelligence
SIGNINT	Signals Intelligence
CTI	Cyber Threat Intelligence
PENTEST	Penetration Test
TTP	Tactics, Techniques and Procedures
GDPR	General Data Protection Regulation
LGPD	Lei Geral de Proteção de Dados (Brasil)
CIR	Centre of Information Resilience

INTRODUÇÃO

Contextualização da era digital e surgimento de OSINT

O presente estudo busca compreender de que maneiras as técnicas, ferramentas e metodologias OSINT (*open-source intelligence*) podem ser utilizadas no jornalismo, bem como analisar as implicações decorrentes de seu uso no fazer jornalístico.

A importância da temática se evidencia no atual contexto da era digital, em que transformações tecnológicas profundas remodelaram práticas sociais, econômicas e políticas. Computadores e smartphones tornaram-se parte inseparável da vida cotidiana, mediando desde interações pessoais até atividades profissionais, educacionais e de lazer. Nesse cenário, a experiência social passa a ser também uma experiência digital.

Com a digitalização crescente, governos, empresas, organizações da sociedade civil e indivíduos passaram a gerar e disponibilizar enormes volumes de dados em redes abertas, muitas vezes de forma pública e acessível. Essa explosão informacional, marcada pela lógica do Big Data, cria tanto oportunidades quanto riscos: a transparência e a possibilidade de rastrear informações convivem com dilemas éticos, problemas de privacidade e a manipulação de dados.

É nesse ambiente que se insere o conceito de OSINT. Diferentemente de métodos tradicionais de coleta de informação, a inteligência de fontes abertas não se limita a softwares ou ferramentas isoladas. Trata-se de um conjunto de práticas que combinam técnicas de busca, cruzamento e análise de dados oriundos de fontes acessíveis ao público: redes sociais, registros oficiais, bases públicas, imagens de satélite, fóruns digitais e até informações indexadas em mecanismos de busca. O diferencial não está apenas no acesso a dados já disponíveis, mas na capacidade de tratá-los de forma sistemática, extraindo deles padrões, narrativas e evidências que vão gerar inteligência e sustentar a tomada de decisões.

Embora tenha ganhado notoriedade recentemente, o conceito de OSINT tem origem no campo militar e de inteligência governamental. Desde a Guerra Fria,

informações coletadas em fontes abertas já eram utilizadas por agências de defesa para complementar relatórios estratégicos. O que mudou com a expansão da internet e, sobretudo, com as redes sociais, foi a escala e a velocidade na circulação e processamento de dados, tornando possível que jornalistas, pesquisadores independentes e até cidadãos comuns se apropriem dessas metodologias antes restritas a ambientes estatais.

Do ponto de vista democrático, o uso de OSINT representa uma ferramenta poderosa de accountability. Ao permitir o rastreamento de informações públicas de maneira sistemática, amplia-se a capacidade de controle social sobre governos e grandes corporações. No entanto, esse mesmo recurso pode ser apropriado de forma abusiva, gerando riscos de vigilância em massa, de perseguição a opositores políticos ou até de violação de direitos fundamentais ligados à privacidade e à proteção de dados pessoais.

A relevância prática da OSINT no fazer jornalístico já pode ser observada em diversos episódios recentes. Na guerra da Ucrânia, por exemplo, jornalistas e coletivos independentes utilizaram metodologias de inteligência em fontes abertas para mapear movimentações militares, verificar a origem de armamentos e identificar áreas atingidas por bombardeios a partir de imagens de satélite e registros em redes sociais (Bellingcat, n.d.). O que antes dependia de relatórios oficiais ou acesso a documentos restritos passou a ser possível a partir da sistematização de dados publicamente disponíveis, permitindo análises detalhadas em tempo quase real.

Casos semelhantes também vêm sendo relatados em outros conflitos, em que a coleta e cruzamento de dados abertos têm fornecido informações estratégicas tanto para a imprensa quanto para organizações de direitos humanos.

No campo das investigações jornalísticas, técnicas de OSINT têm sido empregadas em variadas vertentes: a identificação de redes de corrupção até crimes cometidos em contexto de conflitos geopolíticos.

Essas práticas demonstram que o uso de fontes abertas ultrapassa o universo da verificação de informações falsas, alcançando um patamar em que a coleta,

organização e análise de dados públicos se tornam elementos centrais da apuração jornalística.

Considerando a velocidade das transformações digitais, ferramentas de OSINT se apresentam como um vetor capaz de impactar não apenas o modo como jornalistas investigam, mas também a forma como a sociedade entende a própria circulação da informação. Se por um lado representam novas possibilidades de investigação e transparência, por outro tensionam fronteiras entre privacidade, ética e o interesse público.

Justificativa do tema

O uso de metodologias de inteligência de fontes abertas (OSINT) tornou-se cada vez mais recorrente em práticas jornalísticas nos últimos anos, ainda que muitas vezes de forma não declarada. A possibilidade de acessar, cruzar e verificar informações disponíveis em ambientes digitais ampliou o alcance da investigação jornalística, permitindo revelar tramas complexas que, em outros tempos, dependiam de fontes confidenciais ou acesso privilegiado.

Apesar dessa relevância crescente, nota-se que o campo acadêmico ainda oferece poucos trabalhos sistematizados sobre a relação entre OSINT e jornalismo, o que abre espaço para contribuir com uma discussão original e necessária. Segundo Nelliyullathil (2020), a escassez de literatura nesta área não é coincidência, mas resultado de alguns fatores, apontando que “the integration of open-source intelligence (OSINT) into media activities is still in its early stages” (p. 62).

O impacto desse movimento é particularmente visível no jornalismo investigativo. Casos recentes em escala internacional e nacional demonstram que o emprego de técnicas de OSINT permite expandir hipóteses e métodos de apuração jornalística. Minha própria trajetória como jornalista investigativo mostra essa intersecção: mesmo antes de me aprofundar no conceito, percebi que já utilizava metodologias e ferramentas que hoje são reconhecidas como OSINT em investigações sobre governo, privacidade e tecnologia. Essa experiência prática oferece um pano de fundo pessoal que reforça a relevância do tema, não apenas como objeto de pesquisa acadêmica, mas como campo aplicado.

Além disso, a natureza interdisciplinar do OSINT permite “pegar emprestado” métodos desenvolvidos em áreas como cibersegurança, segurança pública e análise geopolítica, adaptando-os às necessidades e princípios jornalísticos. Tal trânsito entre domínios é uma oportunidade de inovação para a profissão, ao mesmo tempo em que exige reflexão crítica sobre seus limites, riscos e implicações éticas. É nesse espaço que se justifica a presente investigação.

Objetivos

O objetivo central desta pesquisa é compreender como OSINT pode ser utilizado no fazer jornalismo, com foco especial em sua aplicação na prática investigativa. Parte-se da hipótese de que tais métodos já estão incorporados de maneira difusa ao fazer jornalístico, mas carecem de sistematização conceitual e metodológica dentro da literatura acadêmica da área.

Como objetivos específicos, a pesquisa se propõe a:

- analisar como OSINT é utilizado atualmente no jornalismo, excetuando-se seu emprego em verificações factuais (*fact-checking*), que já constituem um campo em si;
- identificar como outras áreas — como a cibersegurança, a segurança pública e a análise de conflitos — empregam OSINT, avaliando de que modo o jornalismo pode aprender com essas experiências;
- discutir as implicações e restrições do uso de OSINT no jornalismo, incluindo aspectos de ética, privacidade e responsabilidade profissional.

Esses objetivos permitem conectar a dimensão prática da apuração jornalística às discussões mais amplas sobre inovação tecnológica, metodologias interdisciplinares e deontologia, produzindo conhecimento com relevância tanto acadêmica quanto profissional.

Estrutura do trabalho

A presente investigação está organizada em cinco capítulos, além da introdução e conclusão. Após uma breve introdução, em que também se aborda a justificativa do

tema, objetivos e estrutura do trabalho, o Capítulo 1 dedica-se à conceituação de OSINT, abordando definições, fundamentos teóricos, evolução histórica e métodos e técnicas emergentes. O Capítulo 2 explora o uso de OSINT em diferentes domínios, com três focos específicos: cibersegurança, investigação criminal/segurança pública e contextos de conflito e geopolítica.

O Capítulo 3 trata da relação entre OSINT e jornalismo. Nele são discutidos princípios deontológicos, a prática do fact-checking, o papel das comunidades colaborativas e do crowdsourcing, estudos de caso de uso de OSINT no jornalismo investigativo, bem como as implicações éticas, de privacidade e de responsabilidade. Esses capítulos (1, 2 e 3) configuram a revisão de literatura.

O Capítulo 4 apresenta a metodologia da pesquisa, incluindo as perguntas de investigação, a estratégia metodológica e o desenho dos questionários realizados. O Capítulo 5 traz a análise de dados, discutindo os resultados das respostas obtidas e estabelecendo um comparativo entre as diferentes áreas em que OSINT é aplicado. Por fim, apresenta-se a conclusão, reunindo os principais achados, as limitações do estudo e possíveis caminhos para futuras pesquisas. Essa estrutura busca equilibrar consistência teórica, análise empírica e diálogo interdisciplinar, sustentando a proposta investigativa do trabalho.

1. CONCEITUAÇÃO DE OSINT

1.1. Definições e fundamento teórico

Cibertecnologias tem se tornado uma importante dimensão da globalização, envolvendo tanto instituições governamentais quanto atores privados (Zureik, 2020). As novas ferramentas da internet e das tecnologias digitais trouxeram uma mudança cultural chave: o que a ativista Vandana Shiva chama de “insurreição do conhecimento subjugado contra o conhecimento dominante do poder” (Pilger, 2011, XVI). As investigações feitas por meio de fontes abertas são um advento desta mudança cultural.

Como qualquer ramo do conhecimento que surge com os adventos tecnológicos, a própria investigação em fontes abertas também foi se conceituando com a medida de sua implementação e aprofundamento no âmbito profissional e também acadêmico. *Open-source intelligence*, que normalmente é referenciada como OSINT, pode significar coisas variadas para pessoas diferentes (Bazzell, 2022, p. 7).

O termo "open-source intelligence" tem origem no campo da inteligência estatal, onde o termo "open" se refere a todos os tipos de fontes que estão disponíveis publicamente e podem ser acessadas, de maneira ética e legal, de fontes públicas, diferentemente da coleta de informação clandestina ou secreta, que normalmente são obtidas de maneira ilegal (Ganguly, 2022, p. 23).

O Departamento de Defesa dos Estados Unidos (2011) define OSINT como inteligência produzida de fontes públicas e disponíveis, em que a coleta, análise e disseminação ocorre para se alcançar um objetivo específico de inteligência.

Esta origem do ramo da inteligência gerou uma diferenciação de conceitos para alguns autores entre *open-source intelligence* e *open-source investigation*, ambos comumente abreviados de OSINT, relacionadas aos objetivos e abordagem metodológica. Para Banks (2008), *open source intelligence* tem o foco mais amplo, voltado à análise estratégica, com coleta de dados para decisões de longo prazo, enquanto *open-source investigations* tem foco mais prático voltado para resolução de casos específicos.

Baack (2015) observa que o jornalismo investigativo, ao adotar práticas de OSINT, passou a falar mais em *investigations* do que em *intelligence*, sublinhando o compromisso com transparência e interesse público, bem como as aplicações metodológicas sobre validação e propósito inerentes ao jornalismo.

O próprio conceito de OSINT foi se moldando com o decorrer do tempo e suas inovações tecnológicas. Quando foi concebido, OSINT era considerado somente inteligências em fontes abertas, que poderiam ser acessadas por qualquer um (Pournis, 2022). Atualmente, há o entendimento de que nem toda investigação que utiliza informações publicamente disponíveis podem ser consideradas open-source intelligence. Sobre o tema, pondera o autor:

> "OSINT is a specific methodology and process that involves gathering, analyzing, and disseminating information from open sources in order to produce intelligence that can be used for decision-making. It is often carried out by specialized organizations and professionals who have the necessary skills and tools to collect, process, and interpret the information they gather. While open-source investigations may involve the use of publicly available information, they may not necessarily follow the same methodology and process as OSINT and may not produce intelligence that can be used for decision-making. Therefore, it is important to distinguish between open-source investigations and OSINT, as they are not synonymous." (p. 22).

Cumpre ressaltar ainda que fontes abertas não são necessariamente sinônimo de "fontes gratuitas": bancos de dados comercialmente disponíveis e legal e eticamente obtidos também se englobam no conceito de OSINT (Jota, 2022). Gibson (2004) aponta que OSINT é a exploração analítica de informações que estão legalmente disponíveis e no domínio público. Ou seja, não são adquiridas clandestinamente por meio de espionagem ou meios ilegais, nem "restritas" ao público por sensibilidade governamental ou comercial (p.19).

Ainda há possibilidade de integrar nas ferramentas de OSINT outros tipos de informação que não são exatamente acessíveis a todo público, mas sim obtidas com emprego de alguma técnica que permite acessar determinado conteúdo, e que não é utilizado por qualquer pessoa (Ganguly, 2022, p. 35). Em alguns casos, há até mesmo aquisição de bancos de dados, bem como outras informações privadas, que são integradas ao instrumento de investigação aberta, para enriquecer os dados trabalhados pela ferramenta.

A literatura também aponta para uma tipologia conceitual que ajuda a organizar esse campo. Van Puyvelde e Rienzi (2025) propõem distinguir OSINF (open-source information — as fontes abertas em si), OSINV (open-source investigation — o processo de investigação que mobiliza essas fontes) e OSINT (open-source intelligence — o produto analítico final).

Há diferenciação entre OSINF e OSINT na discussão acadêmica e prática. Eijkman e Weggemans (2023) afirmam que "OSINF forma a base do Open Source Intelligence (OSINT)" já que passa por todo o processo de análise, edição, filtro e validação.

"OSINF is the raw data, and OSINT is the actionable intelligence derived from that raw data through careful analysis and processing" (OSINT Industries, 2025). Dessa forma, a diferença entre OSINF e OSINT está justamente na passagem do dado bruto ao conhecimento aplicável: enquanto *OSINF* constitui o substrato de informação, *OSINT* implica combinação de método, julgamento crítico e estrutura analítica para gerar *insights* acionáveis.

O próprio Steele, sendo entrevistado por Berghel (2014), pondera que "OSINT is the art and science of creating ethical, evidence-based decision support using only open sources and methods — legal and ethical in every respect.". Para o autor, que é referência na área, OSINT consiste em dois tipos de processamento: no universo do Big Data para encontrar os dados de interesse nos kits de análise de dados, que vão permitir encontrar padrões e anomalias em *datasets* menores. "Beyond that, OSINT is all about humans—analysts who can think, and deciders who can listen" (p. 76).

Ainda que o debate conceitual seja amplo, a convergência está na ideia de que OSINT só pode ser entendido plenamente quando contextualizado em relação a outras disciplinas de inteligência/investigação e sua aplicação metodológica. Assim, defini-lo exige não apenas estabelecer fronteiras, mas reconhecer sua natureza interdisciplinar.

1.2. Evolução histórica

O uso de fontes abertas na produção de inteligência já é observado desde a Segunda Guerra Mundial, quando serviços de inteligência aliados analisavam jornais estrangeiros, transmissões de rádio e panfletos como forma de antecipar movimentos militares e medir o moral de populações inimigas (Steele, 2007). Essa prática continuou ao longo da Guerra Fria, quando o monitoramento de notícias, literatura científica e publicações técnicas era empregado como complemento a métodos mais sigilosos (Lowenthal, 2017).

Na Guerra Fria, OSINT tinha um papel auxiliar, era visto como secundário frente a informações obtidas por espionagem direta. Entretanto, mesmo nesse contexto, mostrou-se fundamental. Lowenthal (2017) observa que "uma parcela significativa da inteligência relevante para os Estados Unidos poderia ser encontrada em fontes

abertas" (p. 92), ainda que a cultura da época favorecesse o segredo em detrimento da abertura.

Enquanto o conceito era utilizado restritamente no âmbito das agências de inteligências, a classificação das fontes de dados era dividida em seis categorias: medias; internet; dados públicos e governamentais; publicações acadêmicas; dados comerciais e literaturas alternativas (Steele, 1995, p. 457). Estas categorias são utilizadas até hoje, apesar da maior parte dos investigadores *open-source* conduzirem suas investigações de maneira exclusivamente online.

Figura 1- Tipos de fontes de OSINT disponíveis

SOURCE	INCLUDES
Media	All forms of content, such as newspapers, radio, TV, digital.
Internet	Online publications like blogs, discussion forums like Reddit, social media websites.
Public government data	Budgets, hearings, press conferences, public government reports, speeches.
Academic publications	Journals, dissertations, academic papers, theses, symposia.
Commercial data	Databases, financial and industrial information, commercial imagery.
Grey literature	Working papers, patents, preprints, business documents, newsletters.

Fonte: (Ganguly, 2022, p.26)

A virada ocorreu nos anos 1990, com a massificação da internet, que permitiu o acesso instantâneo às informações num contexto globalizado e a emergência dos primeiros bancos de dados digitais. De acordo com Steele (2014), 80% das informações que as agências de inteligência precisam já estão publicamente disponíveis (p. 77).

A partir dos 2000, as redes sociais consolidaram um cenário em que OSINT passou a lidar com volumes gigantescos de informação, onde a questão deixou de ser acesso e passou a ser filtragem e validação (Van Puyvelde & Rienzi, 2025). Como ressaltam os autores, a verdadeira inteligência não consiste em acumular dados, mas em transformá-los em conhecimento útil, distinguindo informação relevante de ruído (p. 13).

A massificação das várias comunidades digitais que surgiram nesse contexto criaram condições para que agentes das mais variadas áreas — não apenas estatais, mas também jornalistas e ONGs — trabalhassem com fontes abertas praticamente em tempo real (Schauner & Störger, 2010).

Entretanto, os autores ponderam que essa democratização da coleta de informação exigiu a criação de métodos mais robustos de triagem e análise crítica na investigação, sendo o balizar humano indispensável nesse processo: “Ultimately, it will always be human expertise that really makes the difference in the intelligence tradecraft” (p. 9).

O volume de dados criados e disponibilizados na internet explodiu nos últimos anos: estima-se que 200 mil milhões de gigabytes em dados online serão produzidos em 2025, enquanto este número era em torno de 70 mil milhões em 2020 (Rees, 2023). O papel do jornalismo investigativo dependerá do domínio de extrair conhecimento dessa fonte: “não estamos descobrindo verdades escondidas, mas montando novas verdades a partir dos recursos disponíveis” (p. 8).

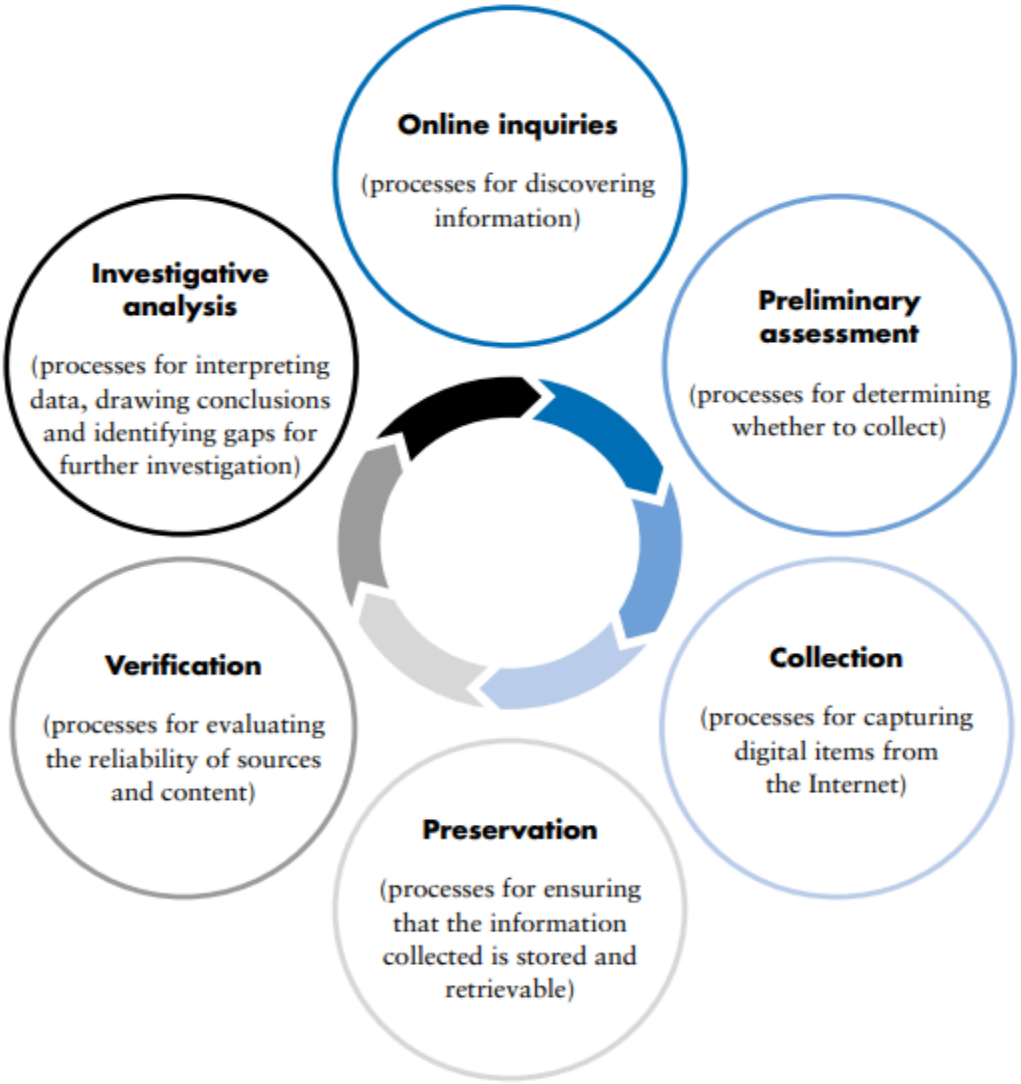
> “It means that investigative journalists no longer need to only learn how to write and turn on a tape recorder or camera. They will need to learn the tools of the internet. While computer scientists will write the programmes, journalists will need to understand the science of OSINT.” (Rees, 2023, p. 8).

Esse percurso histórico demonstra a transformação que a inteligência de fontes abertas passou: de insumo complementar na Guerra Fria, tornou-se disciplina em tempos de hiperconectividade, com usos que atravessam da geopolítica ao jornalismo.

1.3. Métodos, técnicas e automação

Um componente fundamental na coleta de informação em fontes abertas é a necessidade de se estabelecer um *workflow* eficiente que é possível se repetir (Bazzel, 2021). Antes de sair pesquisando nas fontes abertas de qualquer maneira, é necessário pensar e definir como se procederá a investigação (p. 461). A metodologia de investigação por OSINT determina também que é fundamental documentar todo o seu processo, principalmente a coleta e análise de dados, até por variáveis futuras que podem comprometer a integridade ou disponibilidade dos dados tratados.

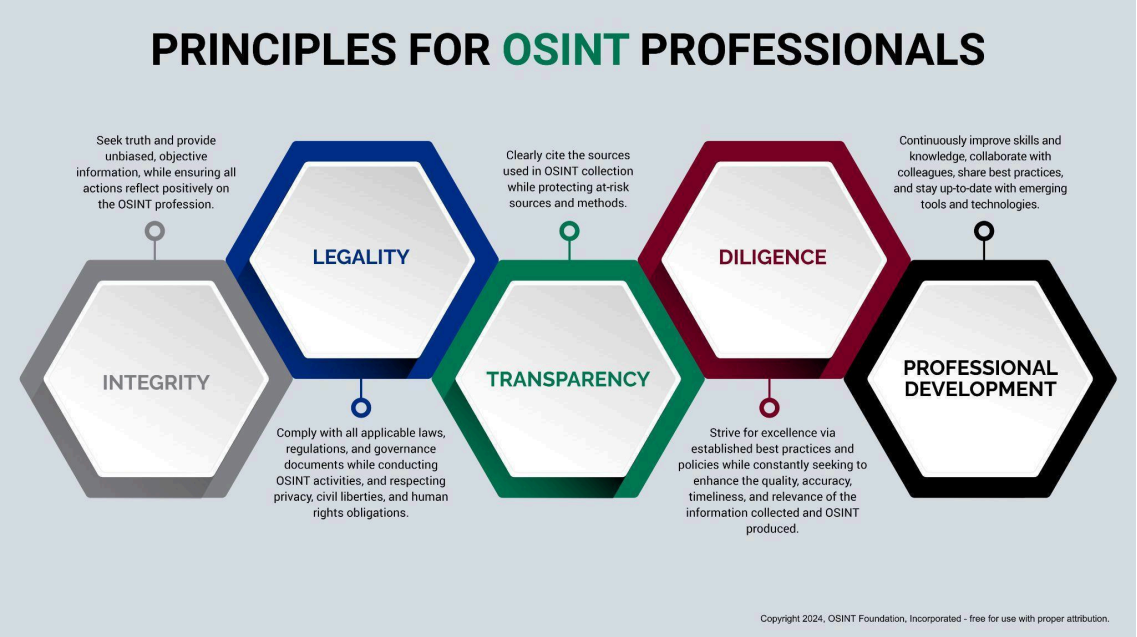
Figura 2- Metodologia OSINT



Fonte: (OHCHR, 2022, p. 68)

Todo método se guia por princípios estruturantes. Mesmo que tecnologias, ferramentas e técnicas utilizadas em investigações em fontes abertas mudem com o tempo, alguns métodos e princípios éticos devem durar (OHCHR, 2022). A identificação destes princípios, além de ser um importante passo para a profissionalização do campo OSINT, serão fundamentais para garantir a qualidade destas investigações, além de "bolster their credibility, reliability and potential usefulness for the purpose of ensuring accountability and minimize potential harm to diverse stakeholders" (p. 11).

Figura 3- Princípios para profissionais OSINT



Fonte: (Osint foundation, n.d.)

Com a consolidação do OSINT, emergiram subcategorias que refletem diferentes modalidades de coleta e análise.

Figura 4 - Tipos de OSINT utilizadas no jornalismo

TYPE OF OSINT	SHORT FOR	INCLUDES
SOCMINT	Social media intelligence	Information mined from social media profiles on Facebook, Instagram, Tumblr, Twitter, LinkedIn, SoundCloud etc. such as personal information, activity data, social network mapping of bots and such, location information, personal connections, and more.
GEOINT	Geospatial intelligence	The rise of commercial satellites and the availability of satellite data from companies like Maxar and Planet Labs has made this easily accessible to journalists and the civil community. This provides unimaginable scope for visual investigations, from location tracking and geolocation, to remote surveillance of conflict zones.
SIGINT	Signals intelligence	This exists primarily within the domain of state security as it refers to what is commonly known as 'wire-tapping' or the interception of signals, mostly illegally. The state agencies commonly associated with this activity are the NSA in the US and GCHQ in the UK-- both of whom were exposed for mass surveillance by Snowden. However, there is a secondary type of signals interception that journalists and civil society can/do engage in-- the monitoring of signals off transportation networks. This information exists within the public domain, and includes flight data, data of tankers and marine vessels, as well as network traffic data which can be manually found by forensically analysing a particular website.

Fonte: (Ganguly, 2022, p. 25)

Omand, Bartlett e Miller (2012) cunharam o termo SOCMINT (Social Media Intelligence) para definir a sistematização da análise de dados oriundos de redes sociais. Para Zubiaga (2019), com o aumento de sua popularidade, as redes sociais se tornaram uma ferramenta poderosa para o jornalismo. Entretanto, o autor pondera que "When social media is used for newsgathering, however, it presents the challenge that the stream of updates flows much faster than a human can follow", ressaltando para a necessidade "to curate all these contents in such a way that the end user can follow" (p. 2).

A técnica de coletar dados em redes sociais de forma automatizada é conhecida por mineração de dados, que permite acessos aos dados quase que instantâneo e "viabiliza a criação de inteligência de negócios utilizando os dados obtidos para auxiliar nas tomadas de decisões" (Perondi et. al, 2022). Algumas redes sociais disponibilizam APIs que facilitam a extração de dados nas mesmas (p. 2). Entretanto, APIs podem ser pagas ou limitadas em seus termos de uso.

Já a técnica de *web scraping* "allows the extraction of huge amount of data that is constantly generated online with a relatively low cost" diretamente das redes sociais, por meio de algoritmos de coleta de dados (Khder, 2021, p. 147). Nestes casos, os dados coletados por essa técnica precisam ser pré-processados e limpos para que possam ser utilizados e agreguem valor ao objetivo que se busca.

Por fim, cumpre ressaltar que a automação e o uso de inteligência artificial ampliaram as possibilidades de todas essas modalidades de uso de OSINT.

A busca automatizada envolve o uso de ferramentas de software e algoritmos para extrair grandes quantidades de dados de fontes disponíveis publicamente. Embora mais eficiente do que a busca manual, esse método exige filtragem e análise meticulosas para garantir a precisão das informações (Stalder & Hirsh, 2002).

No jornalismo, a automação seguiu as lógicas de produção, sendo implementada na produção de notícias, na distribuição de notícias e no consumo de notícias. Na produção de notícias, ferramentas automatizadas foram desenvolvidas para simular julgamento, criar conteúdo e detectar histórias – mas o julgamento

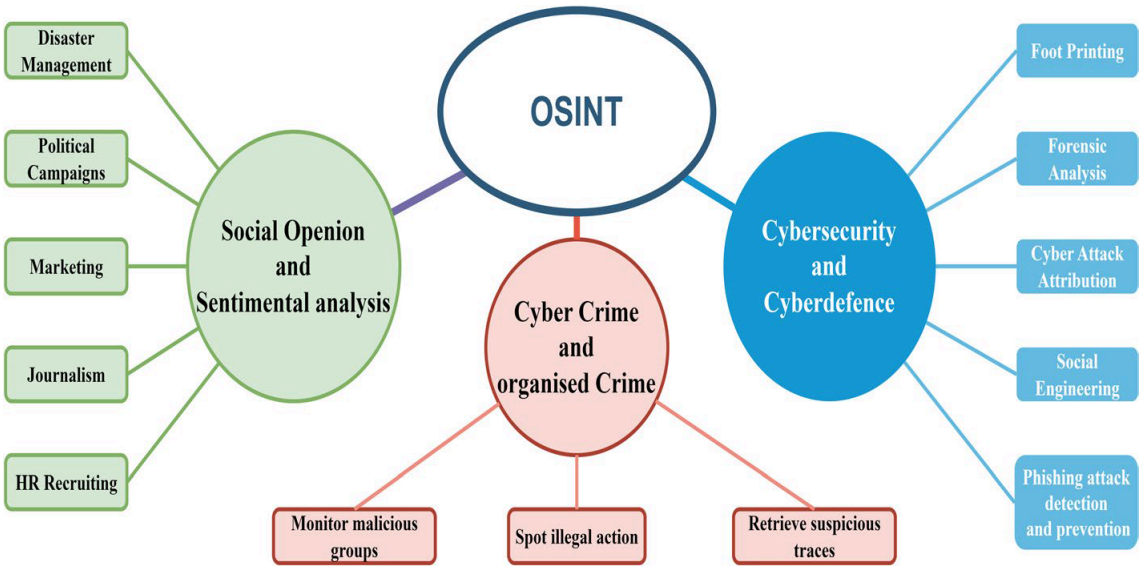
editorial dos jornalistas tem sido difícil, senão impossível, de simular (Ganguly, 2022, p. 59).

2. OSINT EM DIFERENTES DOMÍNIOS

Adoção de OSINT tem crescido em várias áreas de atuação, inclusive no jornalismo. Entretanto, tem escopo de maior utilização e relevância na área da cibersegurança e de investigação criminal, em que atua num papel crucial de determinadas atividades, principalmente para gerar inteligência sobre potenciais ameaças que podem atingir o ambiente cibernético da organização (Yadav, Kumar & Singh, 2023, p. 12400).

Em cada um desses ambientes, o que muda não é apenas a tecnologia disponível, mas a finalidade: um repórter busca narrativa verificável; um analista de segurança da informação busca indicadores e padrões que permitam antecipar incidentes; um investigador público busca evidência passível de sustentação jurídica.

Figura 5 - Tipos de aplicação OSINT



Fonte: (Yadav, Kumar, & Singh, 2023, p. 12411)

Esta secção descreve como OSINT é aplicado em três domínios centrais: cibersegurança, investigação criminal/segurança pública e contextos de conflito e geopolítica.

2.1. OSINT e cibersegurança

Conforme apontam Yadav, Kumar & Singh (2023), mesmo que a estratégia de OSINT para cibersegurança varia de caso a caso, existem métodos que produzem inteligência a partir da coleta e análise de dados em fontes abertas (p. 12411).

Neste meio, um dos usos centrais de OSINT é a produção de inteligência de ameaças (*Cyber Threat Intelligence* – CTI). Segundo Tounsi e Rais (2018, p. 213), trata-se de "informação contextualizada, priorizada e acionável sobre potenciais ou atuais ataques". Esse caráter acionável distingue a simples coleta de dados do processo de inteligência, pois envolve interpretação e priorização para que decisões operacionais possam ser tomadas no contexto de eventual ataque cibernético.

Em termos práticos, CTI analisa dados abertos para produzir inteligência sobre atores, campanhas maliciosas e TTPs (*Tactics, Techniques and Procedures*). TTP é a abordagem que ajuda a identificar estratégias e métodos utilizados por atores maliciosos para explorar sistemas alvos, sendo que a tática reflete sobre o objetivo que o invasor quer alcançar, técnica explica como essa tática é implementada e o procedimento refere-se ao passo-a-passo para executar um ataque (Faidin, Rimbawa & Saputro, 2025, p. 1).

O modelo *Cyber Kill Chain* define fases sequenciais em uma campanha de ataque (Yadav & Rao, 2015). De acordo com os autores, *cyber kill chain* serve para modelar e analisar ações ofensivas de um hacker, para que o analista de segurança possa desenvolver técnicas defensivas a estes ataques. "This knowledge can help one think on the same lines of that of an attacker" (p. 439).

Esse enquadramento metodológico é útil para mapear onde OSINT pode proporcionar alertas antecipados, permitindo que defensores interceptem (´kill') atividades de um ataque cibernético em diferentes fases, como de reconhecimento, comando e controle e outras (Gioti, 2024).

Figura 6 - Fases de um ataque cibernético e aplicação OSINT

Fase do ataque	Descrição	Utilização de OSINT nesta fase	Fontes

Reconhecimento	Início da cadeia, coleta de informações sobre o alvo (nível da empresa, pessoal, infra)	OSINT é fundamental: WHOIS, subdomínios, redes sociais, paste sites, metadados, perfis de funcionários	(Hutchins, Cloppert & Amin, 2011; Yadav, Kumar, & Singh, 2023; Gioti, 2024)
Preparação	Criação e preparação do vetor de ataque (malware, phishing, payloads)	Identificação de vulnerabilidades públicas, software exposto, engenharia social via LinkedIn etc.	(Hutchins, Cloppert & Amin, 2011; Yadav, Kumar, & Singh, 2023; Gioti, 2024)
Entrega	Envio do vetor (e-mail, link, site)	Análise de DNS, domínios falsos, reputação de URLs — OSINT ajuda a identificar sinalizadores de entrega maliciosa	(Hutchins, Cloppert & Amin, 2011; Yadav, Kumar, & Singh, 2023; Gioti, 2024)
Exploração	Execução do vetor; comprometimento inicial do sistema	Menos foco direto de OSINT, mas análise de exploits conhecidos, kits de exploração públicos	(Hutchins, Cloppert & Amin, 2011; Yadav, Kumar, & Singh, 2023; Gioti, 2024)
Instalação	Instalação de malware ou backdoor no sistema alvo	Uso de certificados, buscas abertas para URLs, pegadas de instalação (*footprints*)	(Hutchins, Cloppert & Amin, 2011; Yadav, Kumar, & Singh, 2023; Gioti, 2024)
Comando e Controle (C2)	Estabelecimento de comunicação com servidor de controle	OSINT útil para identificar domínio C2, tráfego suspeito, certificados TLS, infraestrutura externa	(Hutchins, Cloppert & Amin, 2011; Yadav, Kumar, & Singh, 2023; Gioti, 2024)
Ação nos Objetivos (AOO)	Execução de objetivos maliciosos (roubo de dados, ransomware, espionagem)	Monitoração em redes sociais, paste sites, dark web, metadados de documentos vazados	(Hutchins, Cloppert & Amin, 2011; Yadav, Kumar, & Singh, 2023; Gioti, 2024)

Outra atividade no âmbito da cibersegurança em que OSINT exerce um papel fundamental é no teste de penetração (*pentest*). *Pentest* consiste na simulação de um ataque para verificar a segurança de determinado sistema ou ambiente digital a ser analisado (Denis, Zena, & Hayajneh, 2016). Tem por objetivo testar ou examinar, mesmo sob condições extremas ou adversas, o comportamento de redes, sistemas e dispositivos pessoais, “in order to identify their weaknesses and vulnerabilities”,

podendo somente fazer essa análise prévia, ou até mesmo consumar o ciberataque para encontrar vulnerabilidades (p. 1).

Ainda na fase de reconhecimento, *pentesters* realizam uma etapa inicial de verificação de vários tipos de dados antes de iniciar qualquer exploração ativa, o que possibilita uma significativa redução de custos, além de aumentar a precisão dos testes (Yadav & Rao, 2015).

Entre os dados mais valiosos para CTI e *pentest* estão os metadados, inclusive informações em EXIF de imagens, *timestamps* de vídeos e cabeçalhos HTTP, que podem revelar localizações, sequências temporais e autoria de certos conteúdos (NIST, 2008). WHOIS, enumeração de subdomínios, repositórios públicos e credenciais vazadas são alguns exemplos de outras informações que *pentesters* buscam em fontes abertas ao conduzir os testes de penetração.

A dark web, por ser uma "key enabler for cybercrime", oferece uma gama de sinais adicionais e capacidades de um potencial *cyberattack* (IOCTA 2024, p. 10). Neste ambiente da dark web também operam mercados anônimos e clandestinos que contrabandeiam uma gama de produtos de origens ilícitas, inclusive senhas e dados vazados (Soska & Christin, 2015).

A engenharia social é outro campo no qual OSINT tem papel destacado. Mouton, Leenen e Venter (2014, p. 186) definem engenharia social como a exploração deliberada de interações sociais para manipular o comportamento humano. O uso de informações abertas (como cargos, agendas públicas e fotografias) aumenta a credibilidade de potenciais ataques em e-mails ou contatos diretos. Estudos experimentais mostram que campanhas baseadas em dados públicos têm maior eficácia que ataques genéricos (p. 198). "Publicly available information provides the backbone of many social engineering pretexts" (p. 201).

O crescimento e popularidade de modelos de inteligência artificial generativa tem expandido as possibilidades de fraudadores e criminosos alcançarem mais vítimas, além de melhorarem as suas técnicas de engenharia social, conforme aponta o relatório da Europol sobre crime organizado na internet (IOCTA 2024, p. 31).

De igual modo, automação e inteligência artificial são cada vez mais utilizadas para triagem de indicadores no contexto de CTI. Além da automação na coleta de dados em fontes abertas, *frameworks* de IA automatizam as etapas de análise e enriquecimento de dados, bem como de compartilhamento de CTI para respostas mais ágeis (Spyros et. al, 2025).

Conclui-se que OSINT é um componente crucial no âmbito da cibersegurança, até pela rápida evolução que perpassa o ambiente digital.

> "The confluence of OSINT and CTI is where the true potential of both fields is realized. OSINT serves as an invaluable source of information that can provide early warnings of cyber threats. It supplements other intelligence sources by offering a vast repository of publicly accessible data. When integrated into CTI operations, OSINT enriches the intelligence landscape, enabling more informed decision-making and proactive threat mitigation" (Gioti, 2024, p. 27).

2.2. OSINT em investigação criminal e segurança pública

Outro campo em que OSINT tem exercido um papel fundamental e se disseminando rapidamente é no contexto de investigações criminais.

A era moderna atual guiada pelas inovações digitais transformou as atividades criminosas, trazendo desafios significativos para as agências de segurança pública (Vaughan, 2024). Neste contexto, OSINT tem se tornado crucial para as investigações criminais, particularmente pela quantidade de dados disponíveis online e sua capacidade de acessar à essas informações (p. 2).

De acordo com o autor, "Open-Source Intelligence (OSINT) plays a vital role in law enforcement activities by gathering and analyzing publicly available information from diverse sources to create actionable intelligence" (p. 4). Nesse sentido, OSINT auxilia os investigadores em descobrir pistas, identificar suspeitos e compreender padrões comportamentais de criminosos (Vaughan, 2024).

O "Berkeley Protocol on digital open source investigations" é uma diretriz internacional, elaborada pela ONU em conjunto com a Berkeley School of Law da Universidade da Califórnia, para definir padrões profissionais do uso de OSINT nos casos de crimes internacionais e violações de direitos humanos (OHCHR, 2022). O

relatório sistematiza princípios de coleta, preservação e verificação de conteúdo digital aberto, destacando a importância de registrar contexto, metadados e garantir a cadeia de custódia para "maximizar a utilidade probatória" do material.

No contexto de investigação criminal, o investigador *open-source* deve assegurar que a informação coletada seja relevante, confiável, probatória e admissível no tribunal (OHCHR, 2022, p. 25). O relatório recomenda preservar originais, registrar URLs, *timestamps* e ambientes de coleta e gerar hashes verificáveis, sobretudo quando imagens e vídeos podem vir a embasar acusações ou pedidos de cooperação internacional. Deve-se ainda garantir a cadeia de custódia da evidência coletada, que consiste na documentação cronológica desta prova, inclusive com data e hora, transferência e disposição da mesma, garantindo sua autenticidade e integridade (p. 61).

O Protocolo aponta ainda para a preocupação com a proteção de dados pessoais e privacidade no curso de investigações com OSINT: "Open source investigators must respect human rights and should be particularly sensitive to the right to privacy, which is frequently raised in the context of digital information" (p. 27).

Há uma série de ferramentas OSINT que são utilizadas por *law enforcement agencies* em todo o mundo. Uma das mais disseminadas é a Maltego, que apresenta uma interface *friendly-user* com capacidade de transformar consultas em gráficos que revelam correlação e coocorrências entre uma série de informações disponíveis (pessoas, domínios, veículos, empresas, endereços, organizações, etc.) o que facilita hipóteses e triagens iniciais quando o universo informacional é amplo. O próprio fabricante descreve casos de uso em que a correlação de fontes abertas antecipa diligências e evita "pistas mortas" (Maltego, 2023).

Uma ferramenta OSINT chamada Snap Sinapses Desktop tem se difundido rapidamente aos órgãos de investigação do Brasil (Ameno, 2024). O produto integra os softwares da Maltego e consegue cruzar informações até mesmo de contas fechadas das redes sociais do Grupo Meta, além de conseguir acessar vários outros tipos de dados de fontes abertas. A ferramenta ainda tem sido integrada aos bancos de dados sigilosos de uso exclusivo dos órgãos de investigação criminal.

O estudo “As práticas de Inteligência de Fontes Abertas (OSINT) são amigas ou inimigas dos direitos humanos?” da ONG Artigo 19 (2023) aponta ainda que “Um grande número das iniciativas de OSINT são projetadas para fins de segurança e podem implicar excesso de vigilância e monitoramento por parte de agentes públicos e privados, com risco de violação de direitos humanos” (p. 12).

Além do Maltego, ecossistemas como Paliscope e Vortimo têm se difundido em forças de segurança. A Paliscope combina coleta, organização e exibição de cadeia de custódia para relatórios que podem ser submetidos à supervisão judicial; casos de uso reportados incluem investigações de exploração infantil e *money laundering* com trilhas abertas e fechadas reunidas em dossiês de provas (Paliscope, 2024). O Vortimo, por sua vez, oferece um navegador investigativo com anotação, *tagging* e *timelines*, útil para reconstruir jornadas online e reduzir a perda de contexto em coletas longas (Vortimo, 2023).

Num workshop realizado no Brasil, os participantes usaram o ESPY OSINT Profiler para mapear a rede de um policial suspeito de envolvimento com tráfico. A metodologia foi, a partir de um dado pessoal básico — nome, foto, identidade — vasculhar redes sociais, sites institucionais, perfis deletados, marketplaces, e com o auxílio de inteligência artificial, conseguiram revelar vínculos não óbvios (EspySys, s.d.).

Há muitas ferramentas OSINT que também conseguem fazer a identificação de uma pessoa através de técnicas de reconhecimento facial. A EagleEye é uma OSINT em código *Python* que precisa somente de uma imagem de uma pessoa e seu nome ou apelido, para encontrar potenciais redes sociais do alvo (Alqudah et al, 2023). PimEyes é outra aplicação que consegue identificar uma pessoa e utiliza uma fotografia como *input* e aplica técnicas de *reverse image search*[1] e *web scraping* para encontrar uma potencial correspondência (p. 2).

Ressalta-se que esse e outros tipos de utilização de OSINT podem esbarrar em limites éticos e legais aplicáveis. O direito à privacidade é um direito fundamental e muitas legislações impõem uma série de regras e restrições ao uso de dados pessoais

[1]RIS (Reverse Image Search – Busca Reversa de Imagens) é uma técnica que permite identificar e correlacionar imagens com base em suas características visuais, agilizando processos como verificação de originalidade, rastreamento de uso indevido e análise de conteúdo visual em massa (Hoffmann & de la Rocha Ladeira, 2024).

(OHCHR, 2022). Além disso, a coleta massiva e a exposição pública de dados sensíveis podem ferir direitos se não houver necessidade e proporcionalidade (p. 13-14).

2.3. OSINT em contexto de conflito e geopolítica

A Organização das Nações Unidas, em parceria com o Human Rights Center da Universidade da Califórnia, elaborou o "Berkeley Protocol on Digital Open Source Investigations", que é o protocolo internacional descrevendo os padrões profissionais e diretrizes para informações de fonte aberta em investigações criminais internacionais e de direitos humanos. Entretanto, deve-se notar que o processo de produção de mídia para informações de fonte aberta em investigações naturalmente será diferente, devido a considerações de narrativa, apelo ao público, contextualização e outros fatores, como meio de publicação, formato e recursos disponíveis (p. 146).

O Berkeley Protocol consolidou padrões mínimos para identificação, preservação e verificação de conteúdo digital aberto, com o objetivo explícito de aumentar a utilidade probatória em investigações de violações graves de direitos humanos (OHCHR, 2022).

O uso de OSINT em contextos de conflito tem sido amplamente documentado por iniciativas como o Bellingcat, que demonstram como informações abertas podem ser empregadas para reconstruir narrativas em zonas de guerra e violações de direitos humanos. A capacidade de cruzar dados de redes sociais, imagens de satélite e registros públicos transformou a investigação jornalística em algo muito mais transparente e colaborativo (Ganguly, 2022).

Segundo a própria organização, eles utilizaram dados publicamente disponíveis para "desdobrar narrativas sobre conflitos, crimes e abusos de direitos humanos", e com base nestes dados provaram relevantes acontecimentos – "desde chefes do narcotráfico mexicano e crimes contra a humanidade, até o rastreamento do uso de armas químicas e conflitos em todo o mundo" (Bellingcat, n.d.). Este know-how iniciado pela Bellingcat, e também por outros atores, demonstrou o potencial em que as investigações em fontes abertas têm para se proceder à coleta e análise de informações de interesse público por meio de fontes abertas.

A investigação *open-source* realizado pela Bellingcat em conjunto com a equipe de investigações da BBC árabe para documentar crimes de guerra na Síria recebeu a atenção do International, Independent and Impartial Mechanism (IIIM) sobre a Síria, criado pela Assembleia Geral da ONU para reunir evidências de potenciais crimes de guerra e outras violações (International, Independent and Impartial Mechanism, s.d.). Em ambos os casos, da Síria e do voo MH17, os trabalhos investigativos foram usados como prova nas investigações criminais em curso nas Cortes Internacionais de Justiça (Ganguly, 2022).

Uma iniciativa do *Centre of Information Resilience* - CIR é o projeto "Eyes on Russia", que documenta incidentes do conflito utilizando fontes abertas. O projeto publica relatórios semanais, além de colaborar com outras organizações e indivíduos da comunidade OSINT na alimentação do Russia-Ukraine Monitor Map, um mapa colaborativo de incidentes verificados (CIR, 2022). Segundo o próprio CIR, o banco de dados construído pela organização é utilizado pela mídia na cobertura dos acontecimentos na Ucrânia, por grupos que atuam na proteção de refugiados ucranianos, e por organizações focadas na responsabilização de violações de Direitos Humanos.

Casos recentes ocorridos no conflito em Gaza ilustram a maturidade das investigações *open-source* atualmente. Em outubro de 2023, análises independentes geolocalizaram e avaliaram o impacto da explosão no Hospital Al-Ahli, a partir de imagens de satélite, vídeos, áudios e criação de mapas colaborativos (Bellingcat, 2023). Em 2024 e 2025, novas análises documentaram padrões de destruição em Rafah e no norte de Gaza, com estimativas de danos a partir de imagens antes e depois, além de mapeamentos de ataques específicos, como o ocorrido contra a equipe da World Central Kitchen, para os quais foi possível constatar características de munições e assinaturas de impacto por meio de técnicas OSINT (Bellingcat, 2024; 2025).

3. OSINT E JORNALISMO

Apesar do conceito de OSINT já existir há tempos, a evolução das comunicações digitais propiciou a coleta de informações de um determinado público de maneira

muito mais fácil. Neste sentido, Nelliyullathil (2020) pondera que, “open-source intelligence (OSINT), encompasses the retrieval, analysis, and verification of information from publicly accessible sources, including social media platforms, online databases, and other digital reservoirs” (p. 62). Para o autor, o advento deste tipo de investigação digital transformou o cenário do jornalismo, expandindo as possibilidades de investigação e remodelando a natureza da prática jornalística.

A integração da inteligência de fontes abertas (OSINT) nas atividades midiáticas ainda está em estágios iniciais, apesar dos avanços de empresas pioneiras como a Bellingcat (Nelliyullathil, 2020). Os principais veículos de mídia ainda não adotaram plenamente essa metodologia, embora alguns incorporem fontes abertas na produção de notícias, focando principalmente em dados disponíveis publicamente. Além disso, a prática predominante de identificar tendências em dados numéricos contrasta com a adoção de metodologias contemporâneas de OSINT, como análise de imagem, vídeo, áudio, geolocalização e cronolocalização, na preparação de conteúdo jornalístico (p. 62-63).

Os jornalistas têm várias metodologias à sua disposição para conduzir investigação OSINT, incluindo pesquisas manuais, análise de redes sociais e pesquisas automatizadas. A pesquisa manual envolve a realização de buscas por palavras-chave em motores de busca e plataformas de mídia social para encontrar informações pertinentes (Nelliyullathil, 2020). A análise de redes sociais envolve a análise dos padrões de comunicação e dos relacionamentos entre indivíduos e organizações em plataformas de mídia social para identificar figuras influentes e fontes de informação. Essa abordagem pode ajudar no desenvolvimento de pistas e na identificação de possíveis fontes para reportagens (p. 63).

De acordo com Nelliyullathil, independentemente da metodologia escolhida, a verificação é um componente essencial do OSINT no jornalismo (2020). Os jornalistas devem avaliar e corroborar cuidadosamente as informações de múltiplas fontes para assegurar sua precisão e confiabilidade (p. 63). O OSINT deve complementar os métodos tradicionais de reportagem, em vez de substituir os processos rigorosos de verificação e checagem de fatos.

3.1. Deontologia jornalística e jornalismo de dados

Um dos grandes desafios da utilização de OSINT como fonte jornalística perpassa a própria deontologia que permeia esta atividade profissional. Por mais que cada país construa o seu código de ética profissional para atuação do jornalista naquele território, o jornalista deve atuar com um "raciocínio moral", de forma a desenvolver neles uma ética da convicção e da responsabilidade social que advém da profissão (Cavaco, 2019). "A credibilidade e a fiabilidade são essenciais ao valor de uso do jornalismo" (p. 59).

Pegando o Código Deontológico dos jornalistas portugueses como base, há previsão expressa de que o "jornalista deve usar de meios leais para obter informações", além do dever de "assumir a responsabilidade por todos os seus trabalhos e atos profissionais" (Sindicato dos Jornalistas, 2017). O código dispõe ainda que o "jornalista deve usar como critério fundamental a identificação das fontes", além da previsão expressa quanto ao respeito à privacidade dos cidadãos, obrigando o jornalista a "atender às condições de serenidade, liberdade, dignidade e responsabilidade das pessoas envolvidas" antes da recolha de declarações e imagens.

Um princípio elementar do jornalismo que se extrai de uma interpretação sistemática da sua deontologia é o de *accountability*. Nesse sentido, Sawant (2019) pondera que "Accountable communication exists where authors (originators, sources, or gatekeepers) take responsibility for the quality and consequences of their publication, orient themselves to audiences and others affected, and respond to their expectations and those of the wider society" (p. 2).

Outro pilar do jornalismo é a verificação: "The essence of journalism is a discipline of verification" (Kovach e Rosenstiel, 2007, p. 79). Segundo os autores, o processo de verificação diferencia o jornalismo de propaganda, entretenimento, ficção ou arte, sendo dever do jornalista trazer aquilo que aconteceu com precisão.

Não há como falar de OSINT no jornalismo sem falar sobre jornalismo de dados — em analogia com taxonomia, OSINT é espécie dentro do gênero *data journalism*.

Muito além da literal interpretação desse termo — jornalismo de dados = jornalismo + dados — esse ramo do jornalismo amplia possibilidades ao combinar o "afã pelas notícias" inerente à investigação jornalística com a capacidade de se contar histórias com a vasta gama de informações disponíveis no ambiente digital (Gray, Bounegru & Chambersp, 2012, p. 2).

A análise de dados tem potencial de revelar a "forma da história", ou até mesmo nos disponibilizar "uma nova câmera" (Gray, Bounegru & Chambersp, 2012). "By using data, the job of journalists shifts its main focus from being the first ones to report to being the ones telling us what a certain development might actually mean" (p. 4).

A prática responsável de jornalismo de dados exige disponibilizar, sempre que a segurança de terceiros permitir, os conjuntos de dados, capturas e procedimentos que deram origem à apuração (Gray, Bounegru & Chambersp, 2012). Os autores ressaltam a importância de publicar dados e *pipelines* analíticos como forma de aumentar a verificabilidade externa.

Nesta mesma linha, jornalista Rui Barros, em entrevista exploratória com este discente, pondera que "o jornalista deve ser transparente também com sua audiência" quando trabalha com jornalismo de dados, destacando a necessidade de explicar as técnicas de recolha e análise de dados aplicadas na apuração jornalística, para que "o leitor leigo consiga no mínimo entender o que foi feito, até também para desconfiar do jornalista" (Anexo 1).

Barros afirma ainda que tanto o jornalismo de dados quanto a investigação por OSINT apresentam abordagens e valores semelhantes: ambos irão beber do conceito de "Precise journalism" insculpido por Philip Meyer, do jornalismo voltado para ciência. Ou seja, levanta a suspeita, formula hipótese, procede a coleta e análise de dados, para então confirmar ou refutar a hipótese formulada.

O próprio Meyer pondera: "Today's generation of journalists, even more than mine, needs to understand and appreciate the importance of hands-on computer experience. We are locked in a battle with less reputable suppliers of information, and truth made visible is our weapon" (Gehrke & Mielniczuk, 2017, p. 2).

Quando investigações utilizam fontes de grande volume de dados e procedência incerta, o media precisa ter um fluxo interno de responsabilidades, para fazer checagem, revisão e eventuais correções (Gray, Bounegru & Chambersp, 2012). Além disso, todo o veículo de comunicação social, da redação ao conselho de administração, precisa ter um senso ético de responsabilidade (Kovach e Rosenstiel, 2007, p. 231).

O professor Helder Bastos, em entrevista exploratória realizada com esse discente (Anexo 1), afirma que, do ponto de vista deontológico, é correto e legítimo o jornalista utilizar em tudo que esteja disponível publicamente, seja recolher, tratar, analisar dados, mas sempre verificando a autenticidade do que é recolhido e analisado, já que é possível falsificações neste contexto, fora os casos em que não seja possível sequer identificar as fontes daquela informação recolhida.

Para Bastos, as novas ferramentas como OSINT apresentam grandes oportunidades, mas também perigos que o jornalista nunca enfrentou desde a concepção deste campo do conhecimento, já que a escala de volume de informações não têm quaisquer precedentes. E este "ambiente supersaturado e datificado é muito propício para bloquear o trabalho jornalístico" (Anexo 1).

Em conversa com este discente, o professor António Granado, citando Bill Kovack e Tom Rosenstiel, argumenta que o primeiro compromisso do jornalismo é com a verdade. Neste sentido, as ferramentas e inovações tecnológicas como OSINT são fundamentais no exercício das atividades jornalísticas, mas devem sempre ser utilizadas com a supervisão humana.

Granado, ao comentar sobre OSINT no jornalismo, afirma que "o jornalismo não deixa de ser, apenas tem uma ferramenta mais potente" (Anexo 1), reiterando sobre a imprescindibilidade da verificação das informações também neste contexto, já que a verificação é requisito elementar da atividade jornalística.

OSINT encontra-se na interseção entre tecnologia, direitos humanos, jornalismo, pesquisa forense e *accountability* (Ganguly, 2022). Um dos principais indicadores de uma investigação em fontes abertas é a transparência: uma investigação OSINT mostra o seu funcionamento, tornando mais fácil a verificação dos fatos e mais

difícil a refutação (p. 29). Entretanto, falta transparência quando se analisa como os fabricantes das principais ferramentas de OSINT coletam os dados que a alimenta, bem como estes softwares processam estes dados para chegar ao resultado, sendo esta uma dimensão ética importante a ser verificada (Ganguly, 2022).

Ganguly pontua ainda que "“It is critical to not treat OSINT tools as a silver bullet, because they aren't, and to invest instead in OSINT journalism talent which bring human judgment and OSINT experience to investigations to be able to spot errors in results and tools" (p. 342).

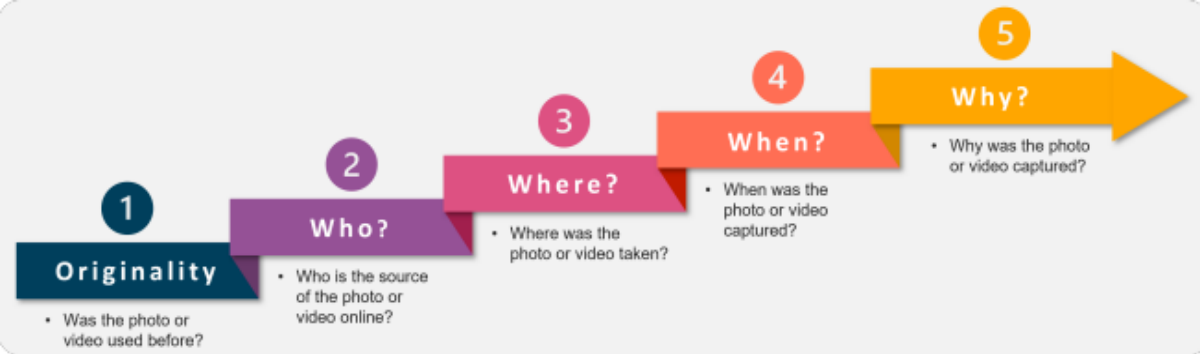
3.2. OSINT como fact-check

Apesar de não ser o objeto dessa investigação, já que uso de OSINT como *fact-check* (verificação de fatos) constitui um campo por si, é importante tecer breves considerações a respeito da temática, que se encontra amplamente difundida nos dias atuais.

"In today's digital era, social media platforms play a crucial role in news consumption and dissemination. They provide instant access to global news stories and a vast amount of real-time multimedia content" (Khan et al., 2023). Entretanto, para os autores, o uso de redes sociais no jornalismo atua como uma faca de dois gumes: aumenta a audiência e se conecta com eventos globais, mas também são terrenos férteis para disseminação de desinformação. "Consequently, it is crucial to responsibly utilise multimedia content from these platforms, particularly during breaking news events, by effectively fact-checking and verifying the information" (p. 1).

Como consequência, vários medias, tais como Associated Press e BBC, estabeleceram times dedicados exclusivamente a verificação de conteúdo multimídia online, com intuito de garantir a autenticidade e confiabilidade das informações que eles disseminam (Khan et al., 2023). A maior parte desses veículos de comunicação utilizam um *framework* que consiste na análise de 5 elementos centrais: originalidade; quem; onde; quando e porquê.

Figura 7 - Framework com 5 passos de verificação multimídia



Fonte: (Khan et al., 2023, p. 3)

Independente do *framework* utilizado, ferramentas OSINT são fundamentais para certificar a propriedade de uma imagem ou identificar a geolocalização desta imagem (Fenza et al., 2023). “The process mainly consists of verifying a piece of content’s provenance, source, date, location, and motivation” (p. 5).

Os autores argumentam que é possível obter o conteúdo original (*provenance*) de determinado arquivo multimídia para melhor compreender as outras etapas do *workflow* e entender o quem, onde, quando e porquê daquele arquivo ter sido disseminado. Ponderam ainda que técnicas de “Reverse Image Search, consisting of searching for the content in large databases (e.g., Google Images), can be a solution for images. In the case of videos, a frame from a video can be subjected to a reverse image search through the Reverse Video Search” (p. 5).

Outro método de verificação de autenticidade de conteúdo visual é a partir da análise dos metadados associados a uma imagem ou vídeo (Khan et al., 2023). “Metadata contains valuable information about the creation time and location of the content, which can aid in assessing its authenticity.” (p. 5). Entretanto, os autores alertam que em muitos casos esses metadados são retirados quando postados em redes sociais, ou podem até mesmo serem manipulados ou modificados. Nesses casos, o jornalista busca pela pessoa que postou o conteúdo e pede o arquivo original, ou evidências suplementares que comprovem a presença do indivíduo naquele local (p. 7).

A guerra entre Rússia e Ucrânia alçou a outro patamar a utilização de OSINT como *fact-check* (Niu et al., 2025). De acordo com os autores, o conflito “has amplified the role of social media in modern warfare", destacando que “Open Source Intelligence

(OSINT) communities have emerged as pivotal players in this digital arena, utilizing publicly available data to analyze, fact-check, and counter misinformation" (p. 1).

Muitos dos vídeos e fotos postadas sobre o conflito são de testemunhas oculares ou de *citizen journalist* (Hamouda, 2023). Segundo o autor, o termo *citizen journalist* "refers to a person who is not professionally trained in journalism and who happens to document an event of sociopolitical significance", ressaltando ainda a importância que este tipo de registros tem no contexto de combate à desinformação (p. 2036).

Apesar do crescente número de organizações que atuam como *fact-checkers*, a UNESCO, em seu manual sobre desinformação, aponta que os jornalistas não podem relegar o seu trabalho de verificação a essas organizações (2019). "O jornalismo também precisa ser proativo para detectar e revelar novos casos e tipos de desinformação" (p. 11).

Ganguly aponta ainda sobre as similaridades do papel do jornalista que usa OSINT no combate à desinformação com o repórter que quer trazer o furo jornalístico.

> "OSINT investigators working on the verification beat have a reactionary job similar to breaking news reporters – their task is to battle disinformation and misinformation before it clouds the truth and do it as swiftly as possible and as many times as needed. The process is three-step: to find dis or misinformation, verify it, and declare it true or false" (Ganguly, 2022, p. 164).

3.3. Comunidades colaborativas e crowdsourcing

Crowdsourcing consiste na utilização de conhecimento coletivo de um vasto grupo de pessoas para resolução de algum problema que esse grupo tem em comum (Antonopoulos et. al., 2020). Contudo, avanços recentes nas tecnologias de comunicação permitiram que esse grupos buscassem atenção de uma audiência mais acessível e interessada naquele tema. Com efeito, surgiram algumas mídias interessadas em "access collective intelligence and creativities from the virtual crowd, and to reduce costs" (p. 28).

Nesse contexto, surgiu a Bellingcat, media pioneira na utilização de OSINT no jornalismo, tendo desenvolvido várias investigações com ferramentas que extraíram

informações através de fontes abertas. Inclusive, umas das descrições mais acuradas do que a prática de investigação de fonte aberta seja hoje em dia é feita pelo media investigativo Bellingcat: “a unique field where advanced technology, forensic research, journalism, investigations, transparency and accountability come together”.

Na introdução do livro que conta sobre o Bellingcat, o seu fundador Eliot Higgins escreve: “Nós provamos que o ditador sírio Bashar al-Assad jogou armas químicas no seu próprio povo. Mostramos quem estava por trás do abatimento do voo MH17. Localizamos apoiadores do Estado Islâmico na Europa. Identificamos os neo-Nazis que aterrorizaram Charlottesville, Virginia. Ajudamos a conter a inundação de desinformações espalhadas junto com o Covid-19. E expusemos o ‘kill team’ do Kremlin” (Higgins, 2021, p. 6-7).

A importância dessas investigações pode ser entendida pelo impacto que elas tiveram (Ganguly, 2022). Pegue o exemplo do Voo 17 da Malaysian Airlines, ou MH17, que caiu em julho de 2014 no leste da Ucrânia. Inicialmente, foi relatado como um acidente. Mas, usando vídeos publicamente disponíveis nas redes sociais, dados de satélite e arquivos feitos por *citizen journalists*, a Bellingcat conseguiu descobrir que o MH17 foi derrubado por um míssil BUK lançado de uma base russa na Ucrânia. Na verdade, eles conseguiram localizar o campo exato de onde o míssil foi lançado, provando o envolvimento do exército russo (p. 27).

A investigação open-source realizada pela Bellingcat em conjunto com a equipe de investigações da BBC árabe para documentar crimes de guerra na Síria recebeu a atenção do International, Independent and Impartial Mechanism (IIIM) sobre a Síria, criado pela Assembleia Geral da ONU para reunir evidências de potenciais crimes de guerra e outras violações (International, Independent and Impartial Mechanism, s.d.). Em ambos os casos, da Síria e do voo MH17, os trabalhos investigativos foram usados como prova nas investigações criminais em curso nas Cortes Internacionais de Justiça (Ganguly, 2022).

No campo da utilização da OSINT para fins jornalísticos, a mídia Bellingcat foi pioneira. Segundo a própria organização, eles utilizaram dados publicamente disponíveis para “desdobrar narrativas sobre conflitos, crimes e abusos de direitos

humanos", e com base nestes dados provaram relevantes acontecimentos – "desde chefes do narcotráfico mexicano e crimes contra a humanidade, até o rastreamento do uso de armas químicas e conflitos em todo o mundo" (Bellingcat, n.d.). Este *know-how* iniciado pela Bellingcat, e também por outros atores, demonstrou o potencial que as investigações open-source têm para se proceder à coleta e análise de informações de interesse público por meio de fontes abertas.

Outro media que surge nesse contexto e também pode ser classificado como crowdsourcing é o Centre of Information Resilience - CIR.

Uma iniciativa do CIR é o projeto "Eyes on Russia", que documenta incidentes do conflito Rússia-Ucrânia utilizando fontes abertas. O projeto publica relatórios semanais, além de colaborar com outras organizações e indivíduos da comunidade OSINT na alimentação do Russia-Ukraine Monitor Map, um mapa colaborativo de incidentes verificados (CIR, 2022). Segundo o próprio CIR, o banco de dados construído pela organização é utilizado pela mídia na cobertura dos acontecimentos na Ucrânia, por grupos que atuam na proteção de refugiados ucranianos, e por organizações focadas na responsabilização de violações de Direitos Humanos.

3.4. Casos de utilização de OSINT no jornalismo investigativo

Mesmo que seja algo relativamente novo, a utilização de ferramentas OSINT para fins jornalísticos tem crescido em ritmo acelerado nos últimos anos.

O Instituto de Mídia da Al Jazeera elaborou um material denominado Open Source Investigations Handbook, em que prescreve questões relevantes sobre a metodologia de investigação de fontes abertas voltadas para o jornalismo. O manual aborda temas gerais de OSINT, como conceito e implicações éticas e legais, mas também apresenta como conduzir investigações do ponto de vista prática, como, por exemplo: rastrear embarcações e aviões; identificação de armas; encontrar sócios de empresas e proceder à análise de imagens de satélites (Creta & Rees, 2023). O livro ainda lista algumas das ferramentas e redes que podem ser utilizadas nas investigações open-source, além de apresentar alguns estudos de casos em que ferramentas de OSINT foram utilizadas com finalidade jornalística, trazendo à tona condutas criminosas perpetradas por governos (p. 45-48).

Müller e Wiik (2021) sugerem que as guerras de hoje são documentadas de forma mais detalhada do que em qualquer outro momento da história. As redes sociais têm contribuído enormemente para a disseminação de conteúdo relacionado à guerra e propaganda, ao dar a indivíduos, grupos e governos um meio de compartilhar informações, imagens e vídeos com um público amplo de forma rápida e fácil. Além disso, as plataformas de redes sociais facilitam a criação e distribuição de notícias falsas e desinformação, que podem ser usadas para influenciar a opinião pública e o resultado dos conflitos. Como resultado, o OSINT é utilizado, por voluntários e por profissionais na área, não só na coleta e análise de dados para investigação, mas também na verificação de notícias e informações falsas (Müller & Wiik, 2021).

Neste sentido, várias organizações da comunidade *open-source*, dentre elas, a própria Bellingcat, o Centre for Information Resilience (Reino Unido), e o site Knack (Bélgica), têm coberto o conflito Rússia-Ucrânia como *fact-checkers*, tendo em vista o incrível aumento de desinformação e fake news relacionadas com esta disputa geopolítica.

Alguns dos principais veículos de comunicação, tais como CNN, The New York Times e The Guardian, já utilizam investigações open-source na cobertura de guerra, principalmente no conflito Rússia x Ucrânia.

Um dos exemplos é a reportagem especial da CNN intitulada “Anatomy of the Mariupol hospital attack" (Polglase, et al, 2022). A matéria se distingue pelo formato distinto das notícias tradicionais, já que é apresentada em formato de vídeos e infográficos, com pouco texto corrido, e conta sobre um ataque russo a um hospital em Mariupol em 09 de março de 2022. Para ilustrar a matéria e demonstrar que a maternidade ainda era utilizada por civis, criou-se um modelo 3D do edifício bombardeado, com base em imagens de satélites e fotos postadas em redes sociais.

Vários tipos de informações foram obtidas a partir de OSINT. Utilizou-se imagens de satélites de poucas horas antes do ataque, que mostram veículos civis estacionados no parque do hospital, para apontar que havia civis no local na hora do ataque. Imagens de satélite posteriores ao ataque mostram a dimensão dos estragos. Imagens coletadas em redes sociais, principalmente Facebook, Twitter e Telegram,

mostram pessoas feridas momentos após o ataque. Postagens de redes sociais foram utilizadas para apontar que o hospital permanecia ativo poucos dias antes do ataque, apesar das afirmações do lado russo de que o local era utilizado por militares ucranianos. A partir de imagens da cratera e consulta de especialistas militares, foi possível estimar a quantidade de explosivos de uma bomba lançada no local por uma aeronave.

A matéria “Satellite images show bodies lay in Bucha for weeks, despite Russian claims.”, do The New York Times, utilizou imagens de satélites de um período de tempo enquanto forças russas ocuparam a cidade de Bucha no subúrbio de Kiev (Willis, 2022). Vários corpos foram encontrados na região após os militares russos deixarem o local. Apesar do governo russo se posicionar afirmando que estas mortes ocorreram após seus militares saírem do local, o media estadunidense conseguiu provar, a partir de imagens de satélite do período em que a cidade estava ocupada, que a morte de civis ocorreu ainda enquanto o local estava sitiado. Em alguns casos, demonstrou-se que os corpos ficaram no mesmo local por um período de 3 semanas. Imagens obtidas por redes sociais (Instagram) e drone complementam a reportagem.

Em outra investigação conduzida pelo The New York Times (“Evidence Suggests Ukrainian Missile Caused Market Tragedy”) também utilizou-se informações de fontes abertas (Cardia, 2023). Em 06 de setembro de 2023, um míssil atingiu um mercado na cidade ucraniana de Kostiantynivka, matando 15 pessoas e ferindo outras 30. De imediato, o presidente Volodymyr Zelensky acusou a Rússia de ser responsável pelo ataque, acusação que foi replicada por vários veículos de comunicação. Entretanto, a investigação do media americano aponta, com robustas evidências, que o ataque foi, na verdade, um acidente ocasionado por um míssil ucraniano errante.

A reportagem apresenta uma série de elementos para chegar a esta conclusão. Dentre as informações que foram obtidas via *open-source*, utilizaram postagens em canal de Telegram local, além de “*before-and-after satellite imagery*”, que demonstram que houve militares ucranianos que dispararam mísseis perto do local do mercado, no momento em que houve a explosão reportada. A investigação é complementada ainda com testemunhas, vídeos de câmera de segurança que mostram o explosivo vindo da

direção da posição ucraniana e não das posições russas, além de especialistas em armas que apontaram que os fragmentos do míssil são distintos do artefato que a Ucrânia acusou a Rússia de ter disparado.

O cenário da guerra entre Rússia e Ucrânia representa um marco na consolidação e assimilação das investigações em fontes abertas. Mas é possível perceber uma assimilação das práticas de investigação jornalística open-source a nível global.

Uma investigação feita também pelo The New York Times, ganhadora do *Human Rights Press Award 202*4, utilizou várias informações obtidas por processos OSINT. A reportagem "The Country That Bombs Its Own People" conta um pouco sobre a situação de Myanmar, um país que teve um golpe de estado recente, e atualmente é governado por uma força militar (Cai, 2023). Para tentar conter uma oposição crescente que também pegou em armas e hoje controla metade do país, o governo tem procedido a bombardeios e demais formas de violência contra os seus próprios cidadãos. O media procedeu à análise de imagens de satélites (antes e depois), fotografias e vídeos postados em redes sociais, somando a apuração com relatos de testemunhas e câmeras de drones das forças oposicionistas, para demonstrar e contabilizar vários tipos de ataques, aéreos e terrestres, feitos pelas forças militares contra vilas e população civil em variadas localidades.

Uma notória investigação jornalística que o uso de OSINT foi fundamental para a apuração foi o caso dos Panamá Papers, que consistiu no vazamento massivo de milhões de documentos internos do escritório de advocacia Mossack Fonseca que expuseram empresas de offshore usadas por políticos, empresários e celebridades (ICIJ, 2016). A investigação foi coordenada pelo Consórcio Internacional de Jornalistas Investigativos em parceria com várias redações ao redor do mundo. Apesar dos documentos serem frutos de um vazamento, ou seja, fonte privada, OSINT exerceu papel fundamental nos processos de verificação e checagem. Procedeu-se ao cruzamento dos documentos vazados com os registros públicos, como registros corporativos, bases de propriedade, websites, redes sociais, índice de embarcações e bases cadastrais públicas, bem como utilizaram ferramentas de análise e visualização

de dados para compreender redes e conectar beneficiários com as empresas offshore. A publicação surtiu impacto no mundo todo, com renúncias de políticos envolvidos e abertura de inquéritos em múltiplos países.

Uma recente investigação do CIR, através do seu projeto Sudan Witness, utilizou metodologia OSINT de variadas fontes para descobrir o local do acampamento militar do grupo rebelde RSF, responsável por ataques a campos de refugiados no país (CIR, 2025). A partir de vídeos postados nas redes sociais, o media procedeu a análise e identificação de veículos, equipamentos, pessoas e até mesmo símbolos para vincular os acontecimentos que ocorreram. Constatou-se que veículos e pessoas que estavam nos acampamentos militares participaram dos ataques ao campo de refugiados. Além disso, foi possível identificar o local exato do acampamento militar, que se localizava no deserto do país vizinho Líbia. Formulou-se a hipótese de que um comboio de veículos daquele porte precisava ter uma estrada por perto. A partir daí, analisou-se imagens de satélites em uma vasta área com estradas, e conseguiu localizar um pequeno ponto luminoso no deserto a partir de imagens noturnas. Para verificar e confirmar o local, elaborou-se um modelo digital com as características físicas e geológicas obtidas a partir dos vídeos, como montanhas, pedras e dunas, e foi possível confirmar a localização, já que os padrões encontrados nos vídeos correspondiam ao local encontrado pelas imagens de satélite.

3.5. Privacidade e proteção de dados pessoais

Não há como dissociar o uso de OSINT da questão da privacidade e proteção de dados pessoais. Invariavelmente muitos dos dados que são coletados e analisados por meio de ferramentas open-source, são também dados pessoais. Nesse sentido, a GDPR define dado pessoal como “informação relativa a uma pessoa singular identificada ou identificável” (GDPR, 2016). Isto significa que a noção de “dado pessoal” é ampliada, e uma série de informações podem ser consideradas dados pessoais quando razoavelmente vinculáveis a uma pessoa.

A maioria das legislações de proteção de dados pessoais prevê ainda uma série de princípios que norteiam o tratamento desses tipos de dados. Dentre os princípios previstos pela GDPR, estão (GDPR, 2016, art. 5º):

- Licitude, lealdade e transparência;
- Finalidade determinada, explícita e legítima;
- Minimização dos dados;
- Exatidão;
- Limitação da conservação;
- Integridade e confidencialidade;
- *Accountability*:

O artigo 6 define as hipóteses legais de tratamento de dados pessoais, definindo seis tipos de bases legais que autorizam a utilização de dados pessoais por pessoas físicas e jurídicas: consentimento; execução de contrato; obrigação legal; defesa de interesses vitais; autoridade pública e legítimo interesse (GDPR, 2016). Ou seja, tratamento de dados pessoais devem estar amparados em pelo menos uma dessas bases legais.

De acordo com Shere (2020), o Capítulo 2 (arts. 5–11) da GDPR possui relevância direta para os investigadores open source e "may have the longer-term effect of curtailing their ability to operate as normal" (p. 6). O autor destaca ainda que investigadores OSINT devem observar os princípios da finalidade determinada e da minimização, restringindo-se ao propósito pelo qual o dado foi coletado e mantendo o armazenamento de dados pessoais apenas pelo período necessário.

O uso indiscriminado de dados comercial e publicamente disponíveis têm efeitos diretos nos direitos à proteção de dados e à expectativa de privacidade da coletividade. Wetzling e Dietrich (2022) defendem que opções claras do titular de dados pessoais se opor ao tratamento de seus dados, além de uma abordagem baseada no potencial risco, elevam os índices de compliance e prestação de contas dos controladores de dados e fortalecem os direitos dos titulares dos dados.

Em continuidade a esse raciocínio, os autores ponderam:

> "The higher the risk for negative impacts on the data subject's rights, freedoms, and interests, the stricter the compliance mechanisms applying to data processing will be. The level of risk depends on which data are collected, how and by whom they are processed, and the severity and likelihood of negative impacts. The level of compliance mechanisms is determined by the accountability obligations which

> apply to the controller. In addition, the GDPR adds purpose limitation as a significant safeguard, which forbids data from being collected and sold for a purpose not defined at the moment of collection" (p. 20).

Os riscos relativos à privacidade ganham especial contorno quanto ao uso de OSINT por agências de inteligência e *law enforcement*. Neste contexto, frequentemente se usa termos como "open source" e "informação publicamente disponível" para coleta de informações com pouco ou nenhum requisito (Oerlemans & Langenhuijzen, 2025). Entretanto, é fundamental considerar que essa informação rotulada como "open source", na verdade, pode não ser de fato acessível para o público. "The use of modern OSINT techniques raises concerns regarding privacy, civil liberties, and the potential for abuse" (p. 585).

Os autores apontam que, "From a European legal point of view, it is clear that collecting and processing data with OSINT tools interfere with the right to privacy as protected in Article 8 of the European Court of Human Rights (ECtHR)" (p. 585). Essa interferência na privacidade é significativa e pode requerer regulação e adoção de salvaguardas adicionais. Além disso, os tipos de dados coletados, a escala da recolha de dados e o tipo de análise que o investigador OSINT realiza pode ajudar a determinar a extensão da violação à privacidade no caso concreto (Oerlemans & Langenhuijzen, 2025).

> "For example, the interference with the right to privacy is minimal when data is copied from news articles and the publicly accessible parts of social media services. The interference with the right to privacy can be significant when location data and leaked data sets are processed. It is clear, including from European case law on the processing of location data by the intelligence and security services, that the processing of location data seriously interferes with the right to protection of personal data and privacy. Location data allow determination of the profile and routine of life, the place where one stays and for how long one stays in a given place. Location data can also be sensitive when combined with other data, such as the type of app from which they are collected" (Oerlemans & Langenhuijzen, 2025, p. 587).

O Art. 85 do GDPR estabelece que, embora atividades jornalísticas possam ser uma exceção da legislação e demandar tratamento de dados pessoais em nome do interesse público, a proporcionalidade e a finalidade devem guiar toda decisão (GDPR,

2016). Em termos práticos, isso significa que deve se observar os princípios legais em relação às informações pessoais coletadas por OSINT para fins jornalísticos.

Enquanto existe uma tendência cada vez maior da publicização de dados, OSINT *skills* são úteis para transformar esses dados em inteligência acionável (Shere, 2020). “However, the danger of doing so is a loss of privacy that may not be reversible. The evolution of regulations such as the GDPR signifies the widespread prioritisation of privacy, rather than facilitation of civilian investigative capabilities” (p. 8).

4. METODOLOGIA

4.1. Perguntas de investigação

No presente estudo, foram formuladas 3 perguntas de investigação e 3 hipóteses associadas às questões, todas embasadas na literatura revista nos capítulos anteriores.

QI01: Em que medida OSINT (open-source intelligence) pode ser utilizado no jornalismo?	Hipótese 1: OSINT pode oferecer ótimos substratos jornalísticos, mas deve ser utilizado em conformidade com os princípios jornalísticos e diretrizes definidas.
QI02: Atualmente, em que medida OSINT é utilizado no meio jornalístico (excetuando *fact-check*)?	Hipótese 2: OSINT é utilizado essencialmente para coleta de dados, em especial dados públicos/governamentais, imagens de satélite e fotos/vídeos e postagens em redes sociais
QI03: Quais são as principais potencialidades e funcionalidades OSINT que ainda são poucas utilizadas no meio jornalístico?	Hipótese 3: Coleta de dados em meios menos convencionais, como dark web; análise de dados com utilização de inferências estatísticas para extração de inteligência, além da própria metodologia de investigação OSINT são funcionalidades e potencialidades ainda pouco exploradas no uso de OSINT no jornalismo.

4.2. Estratégia metodológica

O presente estudo adotou uma metodologia qualitativa, estruturada segundo as etapas propostas por Quivy e Campenhoudt (1992). Partindo de uma fase exploratória, procedeu-se a uma revisão bibliográfica aprofundada, que permitiu mapear o estado da arte sobre a utilização de OSINT em diferentes domínios e orientar a formulação da problemática.

As perguntas foram embasadas a partir de uma extensa revisão de literatura sobre a utilização de OSINT em diferentes domínios. Complementou-se a investigação com a análise de matérias jornalísticas que notoriamente utilizaram informações apuradas por ferramentas e metodologias em fontes abertas. Essa etapa de análise das reportagens complementa a pesquisa bibliográfica, mas, conforme os fundamentos de Quivy e Campenhoudt, também já introduz a fase da problemática, na medida em que permite relacionar o referencial teórico com casos concretos e formular questões de investigação mais precisas.

Foi elaborado um conjunto de questionamentos que têm relação direta com as perguntas de investigação desta dissertação. O estudo adotou modelo de questionário semi-estruturado, com objetivo de obter um ponto de vista fidedigno dos participantes e com riquezas de detalhes sobre o objeto da investigação (Bryman, 2012).

Buscou-se por jornalistas, mas também por profissionais de diferentes áreas para obter uma visão interdisciplinar da temática, bem como obter *insights* de outras áreas que já tem mais consolidada o uso de OSINT em sua prática profissional.

Foram conduzidos um total de 25 questionários com utilizadores de OSINT em variadas áreas, incluindo jornalismo, cibersegurança, investigação criminal e geopolítica.

Elaborou-se um questionário via formulário Google e procedeu-se à recolha de dados no período de Março à Setembro de 2025. Foram feitas duas versões, em português e inglês, contendo as mesmas perguntas, tendo em vista que grande parte dos utilizadores de OSINT são de outras nacionalidades.

O questionário é composto por 19 perguntas, dividido em 3 secções. Na primeira secção, (perguntas 1 a 5) pediu-se algumas informações pessoais do

respondente, para que pudesse fazer a conferência e verificação das pessoas, já que a seleção de participação é feita de maneira direcionada (utilizadores de OSINT no exercício profissional).

Os participantes foram informados sobre a confidencialidade de suas respostas, e ainda facultou-se aos respondentes a possibilidade de não se identificarem, considerando a sensibilidade da temática. Das 25 respostas, duas pessoas optaram por permanecer no anonimato. Analisou-se as respostas dessas duas pessoas, e em seu conteúdo, apresentaram considerações pertinentes, indicando serem utilizadores profissionais de OSINT, então optou-se por manter suas contribuições no conjunto de dados recolhidos e analisados.

A segunda secção aborda especificamente como as ferramentas OSINT são utilizadas no trabalho investigativo do participante, contemplando as perguntas 6 a 16. A maior parte das perguntas são com opções de respostas abertas, mas as perguntas 13, 14 e 15, contém opções de respostas em escala de Likert, em que o participante responde se é “dispensável” ou “indispensável” em uma escala de 0 a 5, o uso de OSINT nos processos de coleta, análise e visualização de dados. Optou-se por utilizar número “par” ao definir este tipo de escala, para evitar uma tendência natural do ser humano em escolher a opção do meio.

A terceira secção busca avaliar as percepções críticas sobre o uso de OSINT, bem como limites éticos, legais e técnicos, contemplando 3 perguntas diretas e uma opção para comentários livres dos participantes sobre a temática.

Por fim, cumpre mencionar ainda que, na elaboração desta dissertação, houve utilização de ferramentas de inteligência artificial generativa nos processos de pesquisa bibliográfica, elaboração e edição de texto e análise de dados para reconhecimento de padrões das respostas recolhidas. Assim como na metodologia OSINT e no jornalismo, houve verificação e validação dos *outputs* que foram utilizados com o uso desse tipo de tecnologia.

4.3. Modelo de questionário

SECÇÃO 1 - Detalhes pessoais

Este formulário faz parte de uma pesquisa de dissertação de mestrado em Ciências da Comunicação (Jornalismo) na Universidade do Porto. O estudo investiga como ferramentas OSINT (*Open Source Intelligence*) podem ser utilizadas como fontes jornalísticas, analisando a sua utilização por profissionais em diferentes áreas investigativas.

Para saber mais sobre minha vinculação institucional e o projeto de dissertação aprovado, acesse:

As respostas são **estritamente confidenciais** e utilizadas apenas para fins acadêmicos. Nenhuma informação identificável será divulgada ou associada às respostas. Caso prefira não informar algum dado pessoal solicitado, escreva "PDI" (Prefiro Não Informar).

Por favor, **não compartilhe este formulário com terceiros**, pois a seleção de participantes é feita de forma direcionada.

Muito obrigado pela sua colaboração!

1. Nome
2. Idade
3. Gênero
4. Cargo e organização
5. Há quanto tempo trabalha nessa função?

SECÇÃO 2 - Uso de ferramentas OSINT em investigações

Esta secção busca entender como ferramentas digitais automatizadas — em especial aquelas classificadas como OSINT — são utilizadas em seu trabalho investigativo. Considere como OSINT qualquer ferramenta que ajude a automatizar uma tarefa que, de outra forma, seria manual (ex: busca reversa de imagem, geolocalização com base em fotos, scraping de dados públicos etc.).

1. Qual área de atuação melhor descreve seu campo de investigação com uso de OSINT?

☐ Jornalismo
☐ Cibersegurança
☐ Investigação criminal
☐ Outra: _____

2. Quais ferramentas OSINT você mais utiliza em suas investigações?

3. Quantas investigações você já conduziu nas quais OSINT foi central?

4. Quais são as cinco ferramentas digitais indispensáveis para você?

5. Quais são, na sua opinião, as principais vantagens dessas ferramentas?

6. E quais são as principais desvantagens ou limitações que percebe?

7. Você utiliza ferramentas que acessam informações não públicas? Como essas informações são integradas às investigações?

8. Indique o grau de importância das ferramentas OSINT em cada etapa:

- Coleta de dados
- Análise de dados
- Visualização de dados

Resposta em Escala Likert (0 a 5) - 0 = Dispensável / 5 = Essencial

9. Qual é seu nível de autonomia no uso técnico das ferramentas OSINT?
☐ Alto – eu mesmo(a) configuro e opero as ferramentas
☐ Médio – opero algumas, mas dependo de suporte técnico para outras
☐ Baixo – dependo de terceiros ou de soluções prontas

SECÇÃO 3 - Avaliação crítica e desafios

Nesta última parte, buscamos compreender melhor suas percepções críticas sobre o uso de ferramentas OSINT, incluindo limites éticos, legais e técnicos.

10. Quais são os principais usos das ferramentas OSINT na sua área de atuação? E quais os objetivos dessas investigações?

11. Que aplicações de OSINT você acredita estarem subexploradas em sua área?

12. Que implicações éticas, legais ou morais surgem em sua prática com OSINT? Como você lida com esses dilemas?

13. Em sua visão, o uso crescente de ferramentas automatizadas melhora ou prejudica a qualidade das investigações? Por quê?

14. Deseja acrescentar alguma consideração, experiência ou comentário livre sobre o uso de OSINT em sua área de atuação?

5. ANÁLISE DE DADOS

Este capítulo apresenta e discute os resultados obtidos a partir do questionário aplicado a profissionais que utilizam OSINT em suas investigações. O objetivo central é compreender como esses atores incorporam tais ferramentas em seu cotidiano, quais são os benefícios percebidos, as limitações encontradas e os dilemas éticos

enfrentados. Além disso, busca-se avaliar a importância atribuída às OSINT nas diferentes etapas do processo investigativo.

O levantamento contou com 25 respondentes de diferentes áreas de atuação. A amostra revelou diversidade em termos de idade e tempo de experiência, com alguns profissionais em fase inicial de carreira e outros com décadas de prática consolidada. Parte significativa dos participantes declarou ter conduzido múltiplas investigações nas quais o OSINT foi elemento central. Um respondente apontou que “Every investigation I have done was centered on OSINT” (Participante W).

Houve diversidade também quanto a área de atuação. Ao elaborar a pergunta, deixei como opção 3 áreas (jornalismo, cibersegurança e investigação criminal), mas também deixei a cargo do respondente a opção de informar “outro” campo de atuação. Desse modo, assim se identificaram os respondentes:

Tabela 1 - Área profissional e identificação dos participantes

ÁREA PROFISSIONAL	IDENTIFICAÇÃO (Participante)
Jornalistas	A, B, C, D, E, F, G, H
Cibersegurança	I, J, K, L, M, N, O, P
Investigação criminal	Q, R, S, T, U, V
Direitos humanos e investigação criminal internacional	W
Consultor e treinamento	X
Investigação e segurança corporativa	Y

As respostas indicam que o uso de OSINT está fortemente associado a ferramentas digitais específicas, tanto gratuitas quanto pagas. Entre as mais citadas estão buscadores avançados, bancos de dados de registros públicos e serviços de monitoramento de redes sociais.

Todas as ferramentas citadas foram listadas na tabela abaixo. Complementou-se a tabela com a função de cada ferramenta, de acordo com informações do próprio fabricante.

Tabela 2 - Ferramentas OSINT e suas funções

FERRAMENTA	O QUE FAZ	FONTE
Sherlock	Pesquisa de usernames em mais de 300 sites para verificar perfis associados	Sherlock Project. (n.d.)
Maltego	Ferramenta de análise e visualização de redes e relacionamentos (pessoas, domínios, IPs).	Maltego Technologies. (n.d.)
Google Dorking	Uso de operadores avançados de busca para encontrar dados expostos.	Imperva (n.d.)
Reverse Image Search (Google, Yandex, TinEye)	Busca por imagens semelhantes para verificar autenticidade, origem e manipulação	Tineye; Yandex (n.d.)
PimEyes	Reconhecimento facial a partir de técnicas de reverse image search	Pimeyes (n.d.)
IntelTechniques Tools	Conjunto de ferramentas de Michael Bazzell para buscas OSINT (emails, usernames, domínios).	Bazzell (n.d)
Google Earth / Maps	Análise geoespacial para verificação de locais e imagens	Google (n.d.)
Copernicus	Imagens de satélite e dados de observação da Terra.	Copernicus. (n.d.)
Telegago	Busca e monitoramento de grupos públicos no Telegram.	Telegago (n.d)
Who Posted What	Busca de posts antigos no Facebook por data e palavra-chave	Whopostedwhat (n.d.)
Osint.rocks	Ferramenta para busca de números de telefone e emails	Osint.rocks. (n.d.)
WhatsMyName	Verificação de usernames em diversos sites.	WhatsMyName. (n.d.).
OCCRP Aleph	Base de dados aberta para investigações financeiras e corporativas.	OCCRP. (n.d.)
OpenSanctions	Repositório global de sanções, pessoas de interesse público e listas restritivas.	OpenSanctions. (n.d.)
OpenCorporates	Banco de dados aberto de registros corporativos	OpenCorporates. (n.d.)
Draw.io	Criação de diagramas e mapas de investigação	Draw.io. (n.d.)
Wayback Machine	Arquivamento histórico de páginas da web	Internet Archive. (n.d.).
Darkside by District 4	Ferramenta comercial para investigação OSINT avançada	District 4. (n.d.)
ForensicOSINT	Plataforma para análise forense de informações abertas	Forensic OSINT. (n.d.)
OSINT Industries	Soluções comerciais para coleta de OSINT em escala.	OSINT Industries. (n.d.)
Alias by SockPuppet	Criação e gerenciamento de perfis falsos controlados (sockpuppets) para investigação	SockPuppet. (n.d.)
Hypestat	Análise de tráfego e dados de websites	Hypestat. (n.d.)

Whois	Identificação de informações de registro de domínios	ICANN. (n.d.)
Social Links	Integração de fontes OSINT ao Maltego para investigações	Social Links. (n.d.)
Pipl	Busca de pessoas baseada em emails, usernames e telefones	Pipl. (n.d.).
AvatarAPI	Identificação de perfis de usuários a partir de imagens	AvatarAPI. (n.d.)
StealthMole	Plataforma comercial para dark web e cyber threat intelligence	StealthMole. (n.d.)
DomainTools	Inteligência de domínios, DNS e infraestrutura	DomainTools. (n.d.)
Atlos	Plataforma colaborativa para investigação baseada em OSINT.	Atlos.io (n.d.)
WeVerify	Ferramenta da UE para verificação de imagens e manipulações.	WeVerify. (n.d.)
Blackbird	Busca de perfis e usernames em redes sociais	GitHub. (2019)
FaceCheck.ID	Busca de reconhecimento facial em imagens públicas.	FaceCheck.ID. (n.d.)
Maigret	OSINT para usernames (similar ao Sherlock, com mais fontes).	GitHub. (2021)
Osint-Brazuca	Conjunto de ferramentas brasileiras para OSINT (usuários, domínios, redes sociais).	Osint-Brazuca. (n.d.)
Shodan	Motor de busca para dispositivos conectados à internet.	Shodan. (n.d.)
Hunter.io	Descoberta de emails corporativos.	Hunter.io (n.d.)
Feedly	Plataforma de agregação de notícias que permite aos usuários coletar, analisar e compartilhar informações de fontes abertas	Feedly (n.d.)
Jusbrasil	Plataforma brasileira que reúne documentos jurídicos públicos, como processos, jurisprudência, leis e artigos	Jusbrasil (n.d.)
Osint Framework	Organiza recursos gratuitos para coleta de OSINT	Osint Framework (n.d.)
Flipboard	Plataforma de agregação de notícias e redes sociais	Flipboard (n.d.)

Dentre as vantagens citadas, muitos participantes apontaram para a grande quantidade de informações que é possível acessar com o emprego de ferramentas OSINT. “They help expand the footprint of a username, email, IP address, phone number, profile picture or any other PII related selector”, apontou o Respondente T.

Automação e agilidade também foram vantagens citadas. “Increased quality of reports, volume management, precision, automation”, destacou o Participante Y, que trabalha com investigações corporativas. Em alguns casos, os respondentes apontaram que utilizam cada vez mais inteligência artificial para automatizar processos, e criam

seus próprios *scripts* de programação para testar as hipóteses que têm sobre determinado tema (Participante X).

Entretanto, há quem não utiliza nenhuma ferramenta específica de OSINT, somente os mecanismos de busca avançados da internet e redes sociais. “Tools are overrated. More important are mindset, skillset & communication ability (in regards to reporting)” apontou Respondente X que é referência internacional em investigações OSINT.

Este mesmo participante ressalta uma limitação importante do uso dessas ferramentas: “Often tools lack attribution (how was the information found)”. Essa mesma limitação foi apontada por outros participantes. “Falta de validação inicial das fontes, isso fica a cargo do profissional”, afirmou o Participante K. “How do tool providers process customer data? Do tool providers save data?” aponta a Participante O demonstrando preocupação não só com a forma que ferramentas OSINT obtém os dados, mas também como aqueles fornecedores de soluções OSINT processam os dados que o utilizador fornece.

Outra problemática lembrada por alguns participantes é o preço de algumas ferramentas OSINT. “I am a freelance journalist, so cost is a problem for me”, aponta o Participante E. “These tools can be quite pricey, so for teams with smaller budgets they can be tough to acquire. I have found this to be especially true for journalism”, destaca o Participante T, que utiliza várias ferramentas pagas em suas investigações *open-source*.

Respondente W ressaltou que há casos que não só a ferramenta é paga, mas também o sítio em que ela extrai determinada informação: “The internet changes so things come and go, so sources are paywalled, some tools that were once free become paywalled”.

Quanto à integração de OSINT com dados de fontes não públicas, observou-se um padrão: todos os jornalistas que participaram afirmaram que utilizam somente informações publicamente disponíveis. Os demais participantes, a maior parte afirmou que integra informações que não são públicas a suas investigações *open-source*.

“I have not used non-public information. The methodology of the platform I work with rejects that. Everything I rely on must be accessible to the public to ensure transparency and verifiability”, destaca um jornalista (Participante D) sobre e necessidade de verificação de transparência da sua fonte.

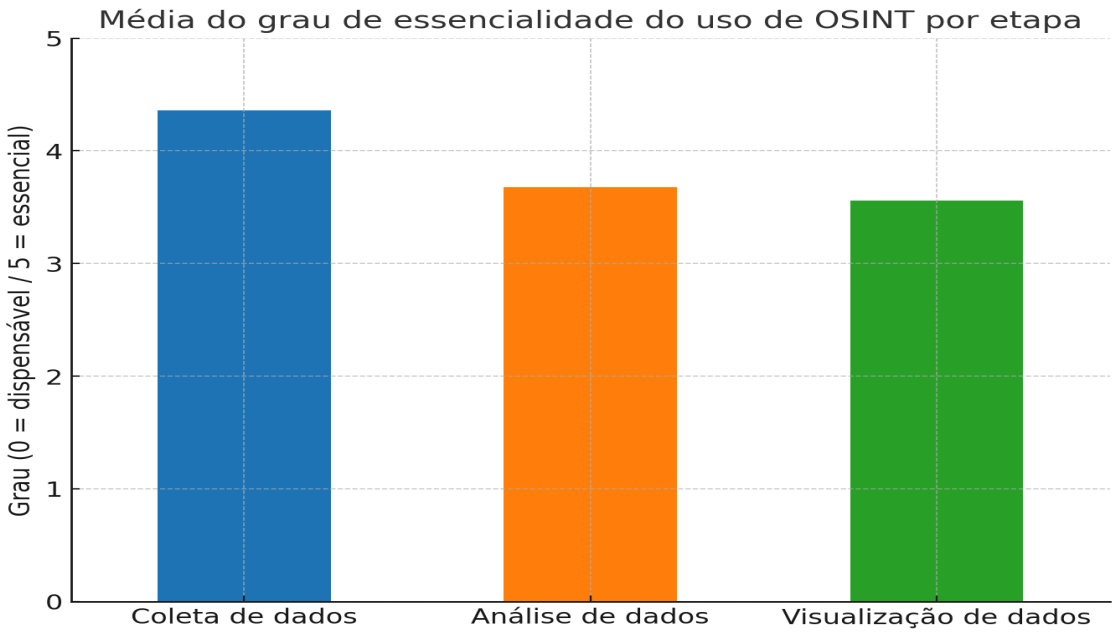
“Yes, sometimes we are either given or we acquire data that is non-public. These data sources are used to compliment, enrich or used as an additional pivot point in investigations and intelligence work.”, explica o Participante T, que é CEO de uma empresa de investigação digital, ponderando que eles consideram “públicos” bancos de dados privados que podem ser adquiridos, desde que não haja pré-requisitos para aquisição desse tipo de informação (como por exemplo, ser uma entidade governamental). “We are willing and able to pay for datasets and ultimately we are paying for the convenience rather than the data itself (breach data is a good example).”, exemplifica este participante.

Um delegado de polícia (Participante R) pondera que é necessário a integração dos dados obtidos por OSINT com bandos de dados restritos, afirmando que o faz, mas tão somente com os bancos de dados oficiais, que são de uso restrito dos órgãos de investigação pública do país.

O Respondente J pondera que “Sim, muitas vezes, é preciso integrar informações públicas com não públicas, e eventualmente preciso consultar um bureau específico”, o que demonstra que essa integração com bancos de dados privados é bastante disseminada no âmbito da segurança da informação.

Quanto às fases de utilização de OSINT, a maior parte dos participantes atribuiu um grau de importância maior na etapa de coleta de dados. Nesse sentido, a maioria apontou o grau de essencialidade como 5 ou 4 no processo de coleta de dados. 5 dos 7 jornalistas participantes atribuíram maior importância na fase de coleta de dados, e 2 jornalistas informaram que OSINT é igualmente importante na fase de coleta, análise e visualização de dados. Nas outras áreas, houve casos de participantes que selecionaram maior grau de essencialidade nas etapas de análise ou visualização de dados, fator que demonstra uma diversidade de uso.

Figura 8 - Média do grau de essencialidade do uso de OSINT por etapa



Outro padrão foi observado em relação ao nível de autonomia técnica para utilização de OSINT. Quase todos os participantes da área da cibersegurança e investigação criminal afirmaram que têm um alto nível de autonomia de uso de OSINT, fazendo eles mesmo a configuração e operacionalização dessas ferramentas.

Já dentre os jornalistas, 5 apontam para um nível médio de competências técnicas (configuram algumas ferramentas mas contam com auxílio técnico para utilizar outras funcionalidades). Um participante reconheceu o seu baixo nível técnico com OSINT e 2 afirmaram ter alto grau de autonomia e competências técnicas para configurar as ferramentas em suas investigações de fontes abertas.

Dentro dessa temática, de limitações técnicas de jornalistas para operacionalizar OSINT, o Participante T trouxe um *insight* relevante:

> "For journalism specifically I find it interesting that there's a push to teach journalists OSINT, when really they should be hiring OSINT professionals. While a journalist should definitely be familiar with the concepts of publicly available information, I think there's a limit to how much one should expect a journalist to know and do. Investigative journalism would be way more effective and impactful if journalists and OSINT professionals came together, as one, to tell stories and break news".

Foi questionado aos participantes sobre os principais usos de OSINT em sua área de atuação e com quais objetivos. Este questionamento guarda relação direta com uma pergunta de investigação dessa pesquisa, para buscar entender as potencialidades e funcionalidades do uso de OSINT em outras áreas e verificar se elas são aplicáveis também ao jornalismo.

Nesse sentido, o Participante J apontou que OSINT serve para "ajudar nos pentests e engenharias sociais, onde, usando informações públicas, posso conseguir informações sensíveis/confidenciais". Outro analista de cibersegurança cita também o monitoramento da dark web e vazamento de credenciais no contexto de *threat intelligence* (Participante M). Já um delegado de polícia afirmou que a utilização de OSINT "na investigação criminal, para formação de provas em processos formais" (Participante R).

Outros participantes apresentaram respostas mais completas que dão pistas sobre as diferentes formas de utilização de OSINT nas mais diversas áreas:

Tabela 3 - Utilização OSINT em diferentes áreas

INTERNATIONAL CRIMINAL INVESTIGATION (Participante W)	**FACT-CHECKER JOURNALISM (Participante D)**
"When it comes to international criminal investigations, we're typically looking for evidence. Evidence can show someone is guilty/responsible, is not guilty/responsible, shows a crime being committed, or other factors that can add context. Some tools are for gathering evidence, some tools are for verifying and authenticating evidence, some are for organizing evidence, and some are for further analyzing evidence."	"I use OSINT tools mainly to uncover and verify facts that are hidden, denied, or deliberately obscured, especially in conflict zones like the Middle East, where disinformation, mutual accusations, and efforts to erase evidence are widespread"
DIGITAL INVESTIGATION (Participante T)	**CIBERSEGURANÇA (Participante I)**
"Open-Source Intelligence (OSINT) tools in my field are primarily used to identify, monitor, and assess threat actors, their networks, and their digital footprints. We operate at the intersection of	"O uso de OSINT nesse contexto vai muito além de simples coleta de informações públicas; trata-se de transformar dados dispersos e muitas vezes subestimados em inteligência acionável capaz de

security, intelligence, and digital investigation — working with both public and private sector clients who rely on timely, accurate insights into online threats.”	antecipar movimentos de mercado, mapear riscos ocultos e identificar oportunidades antes da concorrência. Quando aplicado de forma estratégica, o OSINT permite integrar fontes aparentemente desconexas desde registros judiciais e indicadores econômicos discretos até sinais sutis de atividade em redes sociais, movimentos de capital on-chain e dados alternativos como transporte marítimo, consumo energético ou mudanças em APIs públicas.”
JOURNALIST (Participante H)	**CORPORATE INVESTIGATIONS (Participante Y)**
“The main use of OSINT in my field is to collect data that can be used in journalistic investigation. Normally, the typical information is public records, geoanalysis data and social network interactions.”	“Fraud investigations and corporate security. Digital risk assessments, digital footprints, online monitoring, credential verification.”

Alguns respondentes apontaram como pontos subexplorados do uso de OSINT em sua área a integração com inteligência artificial. O Participante L explica que a análise de dados ainda é uma lacuna em ferramentas de OSINT, e que ‘a IA vem pra acelerar esse processo, te dar riqueza, lapidar e dar um valor agregado à informação, porque muita OSINT vai só coletar o dado, e dado muitas vezes não é interpretável, tem que ter alguém para processar alguma coisa desse dado”.

Para alguns jornalistas, o uso de IA também pode ser implementado para “instant debunking disinformation” (Participante B e F). O Respondente B cita ainda “análises estatísticas mais avançadas” como algo sub-explorado no jornalismo. Um outro jornalista citou a utilização de dados da dark web como uma potencialidade pouco explorada em seu ramo (Participante E). “Digital forensic investigations and mapping coordinated networks on social media” também foi apontado pelo Participante D como um fator subexplorado no jornalismo.

O levantamento revelou que, embora os participantes reconheçam o valor do OSINT, há forte preocupação com implicações éticas, legais e morais. Do “uso de data brokers” (Participante K) ao “ethical hacking para benefício próprio ou de maneira

subversiva" (Participante J), foram várias as ponderações apontadas pelos participantes a respeito das implicações éticas e legais do uso de OSINT em seu ramo.

De maneira geral, o dilema ético aparece em duas dimensões, que são bem ilustradas de acordo com um investigador digital: "When conducting OSINT investigations, the primary ethical and legal concerns revolve around privacy, proportionality, and the responsible use of data". Este participante ressalta que "even though the data we collect is technically 'open source', the context in which it's gathered, analyzed, and applied matters deeply" (Participante T).

Ou seja, a primeira preocupação que foi expressada por muitos participantes está relacionada com os dados pessoais e a expectativa de privacidade. Uma jornalista sintetizou que descobre muita informação pessoal enquanto conduz investigações por OSINT, e que "a large amount of it was of regular citizens" (Participante F). Um analista em cibersegurança que atua na identificação de crimes financeiros reconhece que um limite ético em sua profissão é a "Fronteira entre dados sensíveis e dados públicos", ponderando ainda que "Tento não exceder os limites da privacidade." (Participante I).

Outra implicação lembrada por alguns respondentes diz respeito ao uso de " OSINT for Vigilantism or Revenge purposes" (Respondente N). "One key concern is ensuring investigations don't overstep into surveillance of innocent individuals or violate expectations of privacy, especially in semi-private forums or when using digital personas" (Participante T).

Do ponto de vista legal, uma investigadora criminal externou sua preocupação com a possibilidade de obtenção ilegal de informações por meio de técnicas de intrusão digital, ressaltando que "illegally obtained information is inadmissible in court" (Participante W). O Respondente R apontou as "Implicações legais de origem da fonte, por isso, há necessidade de avaliar a fonte da fonte" quando conduz investigações criminais com OSINT.

Um investigador policial explica com detalhes as implicações legais em sua área:

> "O trabalho policial precisa ser pautado por princípios e regras, e para produção de provas só são válidos os meios legítimos admitidos pelo Direito, logo, a principal dificuldade é a cadeia de custódia das informações para que estas sejam consideradas meios válidos e legítimos no ordenamento jurídico.

> Então o uso adequado e legal das informações disponíveis em fontes abertas, requer também o conhecimento jurídico, conhecimento técnico para solicitar dados oficialmente se for preciso, assim como pedidos de preservação de dados.
>
> Além do fato da cautela desde a coleta a análise e o uso dos dados de fontes não fidedignas que podem comprometer todo o trabalho policial." (Participante S).

O Participante A, que atua como *fact-checker*, aponta a "confiabilidade das fontes e manipulação da informação" como uma dimensão ética importante de sua atuação. Outro jornalista descreve que "a major concern is the manipulation of publicly available digital evidence, especially when investigations target entities with advanced technological capabilities that can control or distort what is published online" (Participante D), trazendo uma preocupação legítima que é da manipulação da informação que pode ser obtida em fontes abertas.

Esta preocupação já tinha sido externada pelo professor Helder Bastos em entrevista exploratória com este discente. Bastos alertou sobre a dificuldade de perceber a "intenção da fonte" no caso de ferramentas *open-source*, alertando ainda sobre as narrativas premeditadas montadas por agências de poder que podem ser escaladas com OSINT, já que o volume e complexidade de dados dificulta a verificação e cruzamento de informações e fontes (Anexo 1).

"O jornalismo enfrenta vários dilemas éticos no uso de OSINT, mas talvez o principal esteja no processo de verificação da informação" pondera o Participante B, ressaltando que sempre tenta checar a informação obtida em fontes abertas por outros meios para corroborar aquele achado. "Verification is crucial, since OSINT can present incomplete or misleading material" alerta o Respondente H, ressaltando ainda para o uso responsável da informação imposto pelo código de ética jornalístico o qual ele adere.

Para enfrentar todos esses dilemas éticos e legais, é fundamental que o investigador *open-source* tenha definido um regramento de conduta bem estruturado, que engloba questões éticas e legais aplicáveis, para conduzir suas investigações com OSINT. "Know the legal framework, have ethical guidelines in place before you start researching. Anything else will inevitably lead to problems", aponta o Participante X.

Um participante descreve com mais detalhes como sua atuação profissional lida com esse tipo de dilema:

> "We also maintain clear internal guidelines aligned with legal frameworks such as GDPR, CCPA, and local laws depending on jurisdiction. These cover everything from consent boundaries and data minimization to the ethical use of personas and infrastructure.
>
> On the moral side, the guiding principle is harm reduction. The intelligence we collect is used to protect people and institutions from violence, harassment, or targeted abuse. Every investigation is weighed against that mission, and we are on the side of caution when there's ambiguity.
>
> Ultimately, we treat OSINT not just as a technical capability, but as a responsibility. The work must be accountable, defensible, and aligned with both legal standards and the public interest" (Participante T).

Por fim, vale destacar que houve uma diversidade de respostas em relação ao questionamento sobre se a crescente utilização de ferramentas automatizadas melhora ou prejudica a qualidade das investigações.

Alguns participantes apontaram que o uso de ferramentas OSINT automatizadas melhora as investigações. "It improves the quality if you have experience and know how to use them properly", ponderou o Participante Y. "OSINT has significantly enhanced the way I work. With the right tools, I can easily track and expose the actions of bad actors online", refletiu o Respondente E. Um jornalista afirmou que OSINT melhora as investigações "mainly because of their capacity and scalability" de se processar uma vasta quantidade de dados e descobrir padrões que permaneceriam escondidos sem essas ferramentas, mas ressalta que "they must be used responsibly, with awareness of their limitations and potential biases. Human judgment remains essential to interpret findings accurately" (Participante H).

Para muitos participantes, essa automatização faz os dois: melhora e prejudica a qualidade das investigações. O Respondente J afirma que "toda saída de dados depende da interpretação de quem busca a informação", ressaltando que toda informação que vem de processos automatizados deve ser checada e fazer sentido. Para o Participante T, "as automated tools become the primary workflow for investigations and intelligence work, the people who are conducting that work will

become less and less technical", ponderando que, como consequência, "this will also limit their investigative capability to the tools that they are using".

Uma jornalista afirmou que "Em geral melhora, já que aumenta consideravelmente o universo informacional à disposição do jornalista. Mas o jornalista deve ter consciência de cada informação obtida de forma automatizada e quais podem estar contaminadas algoritmicamente" (Participante C).

Há quem acredite que o efeito prejudicial da automação é maior do que os efeitos positivos. Para o Respondente X, a automação "it'll make analysts dumber rather than bolster their skills".

Para uma investigadora criminal, a automação das investigações OSINT "prejudica em geral. Pode até ajudar a encontrar informação mas a análise deve ser feita pelo investigador, não pelas ferramentas", ressaltando que há uma série de variáveis que devem ser levadas em consideração: "É preciso ver, analisar, e interpretar tudo tendo em conta nuances linguísticas, um contexto socioeconômico e político da região, a vivência da população, etc. Ferramentas não são capazes de fazer isso" (Participante Q).

Jornalistas demonstraram preocupação quanto às interpretações equivocadas que esses processos automatizados podem gerar, ou mesmo desconfiança quanto a procedência da fonte em que essas ferramentas buscaram a informação. "I prefer manual verification over relying on automated tools, especially in cases involving opinions, emotions, or context-sensitive content, which such tools often fail to interpret accurately", apontou o Participante D. Os Respondentes B e I acreditam que a automação prejudica as investigações, já que é essencial o julgamento humano quando estão lidando com fontes de informação. "Automated tools often have out-of-date information and don't ensure reliablity of information and reliability source of information, because they are further away from the original source", refletiu a Respondente G.

Uma jornalista ainda se mostrou incomodada com a forma que as empresas fabricantes dessas soluções OSINT tratam os dados coletados, considerando ainda casos sensíveis em que é necessário garantir a proteção e anonimato da fonte

jornalística. “It certainly increases efficiency, but investigators have less control over where the data is recorded and stored (even claimed to be erased)” (Participante F).

Uma jornalista conclui suas contribuições com a seguinte reflexão:

> “Osint tem potencial de transformar o jornalismo, e já está fazendo. Entretanto, os princípios elementares que guiam as atividades jornalísticas continuam os mesmos, de forma que Osint só amplia o horizonte informacional ao alcance do jornalista. Todas as etapas de curadoria, validação e confiabilidade da fonte continuam sendo fundamentais na apuração jornalística, com uso de Osint ou não.” (Participante C)

CONCLUSÃO

O presente estudo buscou compreender de que forma *open-source intelligence* (OSINT) podem ser utilizadas nas investigações jornalísticas, explorando não apenas a sua adoção prática em diferentes áreas investigativas, mas também os dilemas éticos, técnicos e legais que permeiam esse uso. A partir da revisão teórica e da análise dos questionários realizados, foi possível perceber que o OSINT já ocupa um lugar consolidado em diversas áreas profissionais, mas ainda carece de amadurecimento metodológico e institucional no jornalismo. Esta dissertação contribui, assim, para ampliar o debate sobre os potenciais e limites do uso de OSINT no campo jornalístico, destacando pontos de convergência entre teoria e prática, mas também revelando lacunas importantes a serem exploradas.

Principais achados

A primeira questão de investigação (QI01) indagou em que medida OSINT pode ser utilizada como meio jornalístico. Os dados confirmam a hipótese inicial: OSINT pode oferecer ótimos substratos jornalísticos, mas a sua utilização requer alinhamento com princípios éticos, normativos e legais próprios do jornalismo. Os questionários evidenciaram que, mesmo sendo obtidos de forma aberta, os dados precisam ser contextualizados, validados e interpretados de acordo com os critérios de rigor jornalístico.

Na segunda questão (QI02), buscou-se compreender em que medida OSINT é atualmente utilizado no meio jornalístico, excetuando a prática de *fact-checking*. Os

resultados indicam que, de fato, o uso predominante ainda se concentra na coleta de dados — especialmente dados públicos, imagens de satélite, redes sociais e arquivos digitais como a *Wayback Machine*. Entretanto, observa-se que jornalistas, em geral, utilizam essas ferramentas com menor autonomia técnica do que outros profissionais, como investigadores criminais ou analistas de cibersegurança.

Já a terceira questão (QI03) investigou quais potencialidades das ferramentas OSINT ainda são pouco exploradas no jornalismo. Os achados confirmaram a hipótese de que áreas como exploração de dados da dark web, inferências estatísticas e metodologias avançadas de análise seguem subaproveitadas. Alguns respondentes mencionaram ainda a integração com inteligência artificial, tanto para acelerar processos de análise quanto para identificar padrões ocultos, como uma fronteira pouco explorada.

O estudo evidenciou que a adoção de OSINT no jornalismo ainda se encontra em estágio incipiente quando comparada a áreas como a cibersegurança e a investigação criminal. Enquanto nestes campos a utilização de bases abertas está integrada a protocolos consolidados, no jornalismo a apropriação ocorre de forma mais dispersa, dependente da iniciativa individual de repórteres e não como uma prática institucionalizada em muitos casos.

Outro achado importante foi a constatação de que muitos jornalistas ainda enfrentam barreiras técnicas significativas para operar ferramentas e processos OSINT mais avançados. A análise das respostas indicou que parte dos profissionais utiliza tais recursos apenas em sua superfície, limitando-se a buscas em redes sociais, buscadores avançados e dados governamentais, sem explorar metodologias de análise de redes, correlação de dados ou exploração da dark web.

Além disso, o levantamento revelou uma percepção ambivalente entre os participantes: de um lado, o reconhecimento de que OSINT amplia enormemente a capacidade de acesso à informação e a eficiência das investigações; de outro, a consciência de que tais práticas podem gerar riscos éticos e legais, especialmente questões relacionadas à privacidade. O dilema entre eficácia investigativa e responsabilidade ética foi recorrente nos depoimentos, mostrando que não basta

dominar tecnicamente as ferramentas — é essencial integrá-las a um marco normativo que preserve valores fundamentais do jornalismo.

O estudo também confirmou a centralidade da coleta de dados como principal etapa beneficiada pelo uso de OSINT, mas trouxe nuances relevantes sobre a análise e a visualização da informação. Profissionais de cibersegurança e investigação criminal relataram que a inteligência gerada a partir da análise de padrões, conexões e inferências é muitas vezes mais valiosa do que o simples acesso a dados brutos.

Por fim, destaca-se que a pluralidade de áreas em que OSINT é utilizado oferece ao jornalismo uma oportunidade de aprendizado interdisciplinar. Experiências de investigadores corporativos, policiais e especialistas em segurança digital mostraram que as fontes abertas podem ser aplicadas de forma estratégica em contextos profissionais distintos. Ao incorporar essas metodologias, o jornalismo pode expandir seu repertório investigativo, fortalecendo sua função democrática de fiscalização do poder e de promoção da transparência.

Limitações do estudo

Uma limitação desta pesquisa decorre do método de amostragem. Ainda que a estratégia tenha possibilitado reunir 25 respondentes com experiência direta no uso de OSINT, o tamanho e a composição da amostra não permitem generalizações amplas. Houve predominância de participantes provenientes das áreas de cibersegurança e investigação criminal, o que, por um lado, enriqueceu a visão interdisciplinar, mas, por outro, pode ter limitado a identificação de práticas mais específicas do jornalismo.

Houve também uma certa desconfiança por parte dos investigadores *open-source* em relação às perguntas, sendo que muitos optaram por não responder o questionário. Provavelmente, isto se deve ao fato da própria natureza da investigação OSINT, que é sigilosa por concepção e prevê uma série de condutas visando a salvaguarda da identidade do investigador, garantindo a segurança das operações.

Outra limitação refere-se ao caráter auto explicativo das respostas, uma vez que se tratou de questionário autoaplicado. Isso pode gerar vieses, tanto por excesso de confiança dos participantes quanto por interpretações subjetivas do conceito de OSINT.

Constatou-se também uma limitação na formulação de uma das perguntas do questionário. Na secção 2, foi feito o seguinte questionamento:

"Você utiliza ferramentas que acessam informações não públicas? Como essas informações são integradas às investigações?"

Neste quesito, um dos participantes respondeu: "I don't completely agree with the way the question is phrased. If a private person or company can buy it, it is publicly available - in contrast to information that can only be sourced by government entities".

De fato, ele tem razão. Para contemplar todas as informações que queria obter, o ideal seria destrinchar este quesito em duas perguntas: uma sobre ferramentas que acessam informações comerciais que foram adquiridas, e outra sobre acesso a bancos de dados restritos que não são considerados públicos, de acordo com entendimento consolidado do meio OSINT.

Não houve outras respostas que divergiram da pergunta feita, mas pode ter havido participantes que interpretaram a pergunta de forma restritiva e pode ter dado uma resposta menos pertinente para o objeto desta investigação.

Possibilidades futuras de pesquisa

Dada a crescente relevância do tema, há múltiplas possibilidades para aprofundar esta linha de investigação. Uma primeira direção consiste em explorar mais detidamente como OSINT pode ser estruturado no fazer jornalístico, não apenas em termos técnicos, mas também enquanto prática metodológica integrada às rotinas de redações. Isso inclui, por exemplo, investigar modelos de colaboração entre jornalistas e profissionais especializados em OSINT, a fim de superar limitações técnicas e ampliar o impacto social das apurações.

Outra possibilidade reside no próprio grau de maturação do uso de OSINT em outras áreas, principalmente na cibersegurança. Constatou-se que uma variedade de tipos de dados coletados em fontes públicas são utilizados na cibersegurança, principalmente no contexto de CTI e na condução de *pentests*. Muitos desses dados são de natureza mais técnicas, como DNS, IPs, registro de domínios e WHOIS, logs, *pastes sites*, hashes de *malware*, cabeçalho HTTP e certificados TLS. Entretanto, esta pesquisa não identificou o uso desses tipos de dados em investigações jornalísticas que

usaram OSINT, que predominantemente usam mais dados governamentais, de redes sociais e de satélite, e em alguns casos, análise de metadados de ficheiros. Desse modo, esta ampliação de possibilidade de tipos de dados coletados e analisados via OSINT como fonte jornalística é um caminho promissor a ser explorado.

Por fim, outro campo ainda pouco explorado para futuras pesquisas é a própria dark web e as suas possibilidades de contribuição para o jornalismo. Seria relevante analisar, por exemplo, qual é a extensão dessa dimensão escondida da internet e quais são as suas várias possibilidades que podem ser exploradas pelo jornalismo. Esse tipo de investigação permitiria trazer luz ao vasto espectro da *web* que é desconhecida pela maior fatia da população, os tipos de informações que podem ser encontrados, bem como os desafios éticos e legais que o jornalista se depararia com uma investigação jornalística do gênero.

Referências Bibliográficas

Al Jazeera Media Institute. (2019). *Open-source investigation: A guide for journalists*. Al Jazeera Media Institute. https://institute.aljazeera.net/sites/default/files/2023/Open%20Source%20Investigation%20Handbook.pdf?title=Open+Source+Investigation+Handbook

Al Jazeera Media Institute. (2025). *Ethics and safety in OSINT – can you believe what you see?*. Al Jazeera Media Institute. https://institute.aljazeera.net/en/ajr/article/2275

Alqudah, R., Al-Qaisi, M., Ammari, R., & Ta'a, Y. A. (2023). OSINT-Based Tool for Social Media User Impersonation Detection Through Machine Learning. In *2023 International Conference on Information Technology (ICIT)* (pp. 752-757). IEEE. https://www.psut.edu.jo/uploads/2024/05/osint-basedtoolforsocialmediauserimpersonationdetectionthroughmachinelearning.pdf?language=ar

Ameno, F. (2024). Polícia: sistema vasculha redes, dados sigilosos e de crédito. *Intercept Brasil*. https://www.intercept.com.br/2024/03/12/uso-de-ferramenta-que-cruza-conexoes-do-facebook-e-dados-da-policia-explode-no-pais/

Antonopoulos, N., Konidaris, A., Polykalas, S., & Lamprou, E. (2020). Online journalism: Crowdsourcing, and media websites in an era of participation. *Studies in Media and Communication, 8*(1), 25-36. https://redfame.com/journal/index.php/smc/article/view/4734

Artigo 19. (2023). *As práticas de Inteligência de Fontes Abertas (OSINT) são amigas ou inimigas dos direitos humanos?*. ARTIGO 19 Brasil e América do Sul. https://artigo19.org/wp-content/blogs.dir/24/files/2023/09/DIGITAL_OSINT_20-09-2023_ARTIGO_19.pdf

Baack, S. (2015). Datafication and empowerment: How the open data movement re-articulates notions of democracy, participation, and journalism. *Big Data & Society, 2*(2), 1-11. DOI: 10.1177/2053951715594634

Bazzell, M. (2019). *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information* (7th ed.). Independently published.

Bazzell, M. (s.d.). *IntelTechniques OSINT Tools*. IntelTechniques.

Bellingcat. (2016). *A brief history of open source intelligence*. Bellingcat. https://www.bellingcat.com/resources/2016/03/07/a-brief-history-of-open-source-intelligence/

Bellingcat. (2017). How a Werfalli Execution Site Was Geolocated. *Bellingcat, 3* October. https://www.bellingcat.com/resources/2017/10/03/how-a-werfalli-execution-site-was-geolocated/

Bellingcat. (2019). *Bellingcat's Online Investigation Toolkit*. Bellingcat. https://www.bellingcat.com/resources/2019/07/01/bellingcats-online-investigation-toolkit/

Bellingcat. (2023). *Identifying possible crater from Gaza hospital blast*. Bellingcat. https://www.bellingcat.com/resources/2023/05/15/identifying-possible-crater-from-gaza-hospital-blast/

Bellingcat. (2024a). *Strike that killed World Central Kitchen workers bears hallmarks of Israeli precision strike*. Bellingcat. https://www.bellingcat.com/resources/2024/01/15/strike-that-killed-world-central-kitchen-workers-bears-hallmarks-of-israeli-precision-strike/

Bellingcat. (2024b). "We've become addicted to explosions": The IDF unit responsible for demolishing homes across Gaza. *Bellingcat*. https://www.bellingcat.com/resources/2024/03/10/weve-become-addicted-to-explosions-the-idf-unit-responsible-for-demolishing-homes-across-gaza/

Bellingcat. (2025). *Satellite imagery shows schools and hospitals destroyed in northern Gaza*. Bellingcat. https://www.bellingcat.com/resources/2025/02/20/satellite-imagery-shows-schools-and-hospitals-destroyed-in-northern-gaza/

Berghel, H. (2014). Robert david steele on OSINT. *Computer*, *47*(7), 76-81. DOI: 10.1109/MC.2014.213

Bryman, A. (2012). *Social Research Methods*. Oxford University Press.

Cai, W. (2023). The Country That Bombs Its Own People. *The New York Times*. https://www.nytimes.com/2023/07/15/world/asia/china-bombs-own-people.html

Cardia, A. (2023). Evidence Suggests Ukrainian Missile Caused Market Tragedy. *The New York Times*. https://www.nytimes.com/2023/06/20/world/europe/ukraine-missile-market-tragedy.html

Cavaco, S. (2019). Confidencialidade da fonte em jornalismo: Perspectivas morais. *Mediapolis–Revista de Comunicação, Jornalismo e Espaço Público, (9)*, 57-72.

https://www.mediapolis-revista.com/2019/09/01/confidencialidade-da-fonte-em-jornalismo-perspectivas-morais/

Centre for Information Resilience. (s.d.). *How is OSINT used in armed conflict?*. Centre for Information Resilience. https://www.cir.org.uk/how-is-osint-used-in-armed-conflict/

CIR - Centre for Information Resilience. (2025). *How we found an RSF military camp in the Libyan desert* [Vídeo]. YouTube. http://www.youtube.com/watch?v=umaFPlwJUKM

Copernicus. (s.d.). *Copernicus Programme*. European Commission. https://copernicus.eu/en/about-copernicus

Creta, S., & Rees, P. (2023). *Open Source Investigations Handbook*. Al Jazeera Media Institute. https://institute.aljazeera.net/sites/default/files/2023/Open%20Source%20Investigations%20Handbook.pdf

Denis, M., Zena, C., & Hayajneh, T. (2016). Penetration testing: Concepts, attack methods, and defense strategies. In *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (pp. 1-6). IEEE. DOI: 10.1109/LISAT.2016.7472734

Department of Defense. (2011). *Joint Publication 2-0: Joint Intelligence*. DoD.

Dietrich, C., & Wetzling, T. (2022). *Disproportionate use of commercially and publicly available data: Europe's next frontier for intelligence reform?* interface (formerly Stiftung Neue Verantwortung). https://www.interface-eu.org/publications/disproportionate-use-commercially-and-publicly-available-data-europes-next-frontier

District 4. (s.d.). *Darkside*. District 4. https://www.district4.com/darkside

DomainTools. (s.d.). *Whois and Domain Intelligence*. DomainTools. https://whois.domaintools.com/

Eijkman, Q., & Weggemans, D. (2023). Open source intelligence and privacy dilemmas. *Centre for Terrorism and Counterterrorism, Leiden University–Campus The Hague*. https://www.ctc.leidenuniv.nl/publications/open-source-intelligence-and-privacy-dilemmas.pdf

Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA)*. Europol. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2023

European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679... (General Data Protection Regulation)*. *Official Journal of the European Union, L 119*, 1–88.

FaceCheck.ID. (s.d.). *Face Recognition Search Engine*. FaceCheck. https://www.facecheck.id/

Faidin, F., Rimbawa, H. D., & Saputro, J. W. (2025). Exploration of Tactics, Techniques, and Procedures (TTP) in Cyber Attacks on Government Infrastructure. https://www.researchgate.net/publication/369000000_Exploration_of_TTP_in_Cyber_Attacks_on_Government_Infrastructure

Feedly. (n.d.). *Feedly: Agregador de notícias*. https://feedly.com

Fenza, G., Loia, V., Mainardi, P. M., & Stanzione, C. (2023). OSINT Knowledge Graph for Fact-Checking: Google Map Hacks Debunking. In *ITASEC*. https://www.itasec-conference.org/2023/papers/osint-knowledge-graph-google-map-hacks.pdf

Flipboard. (n.d.). *Flipboard: Agregador de notícias e redes sociais*. https://flipboard.com

Forensic OSINT. (s.d.). *Forensic OSINT*. Forensic OSINT. https://www.forensic-osint.com/

Ganguly, M. (2022). *The Future of Investigative Journalism in the Age of Automation, Open-Source Intelligence (OSINT) and Artificial Intelligence (AI)* (Doctoral dissertation). University of Westminster. https://westminsterresearch.westminster.ac.uk/item/q5v0y/the-future-of-investigative-journalism-in-the-age-of-automation-open-source-intelligence-osint-and-artificial-intelligence-ai

Gehrke, M., & Mielniczuk, L. (2017). Philip Meyer, the outsider who created Precision Journalism. *Intexto*, 4-13. https://www.intexto.com.br/index.php/intexto/article/view/1234

Gioti, A. (2024). *Advancements in Open Source Intelligence (OSINT) Techniques and the role of artificial intelligence in Cyber Threat Intelligence (CTI)* (Master's thesis). Πανεπιστήμιο Πειραιώς. https://www.repository.piraeus.gr/handle/123456789/gioti_osint_ai_cti

GitHub. (2019). *Blackbird*. GitHub Repository. https://github.com/blackbird-project/blackbird

GitHub. (2020). *Maigret*. GitHub Repository. https://github.com/soxoj/maigret

Google. (s.d.). *Google Earth*. Google. https://www.google.com/earth/

Google. (s.d.). *Google Maps*. Google. https://www.google.com/maps/

Gray, J., Bounegru, L., & Chambers, L. (Eds.). (2012). *The Data Journalism Handbook*. O'Reilly Media / European Journalism Centre.

Hamouda, H. A. (2023). Authenticating citizen journalism videos by incorporating the view of archival diplomatics into the verification processes of open-source investigations (OSINT). In *2023 IEEE International Conference on Big Data (BigData)* (pp. 2036-2046). IEEE.

Higgins, E. (2021). *We Are Bellingcat: An Intelligence Agency for the People*. Bloomsbury.

Hoffmann, S., & de la Rocha Ladeira, R. (2024). Aplicação de Técnicas de Hashing e Redes Neurais Convolucionais na Busca Reversa de Imagens. In *Escola Regional de Redes de Computadores (ERRC)* (pp. 160-165). SBC.

Hutchins, E., Cloppert, M., & Amin, R. (2011). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Lockheed Martin. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Hypestat. (s.d.). *Website statistics and analytics*. Hypestat. https://www.hypestat.com

International Center for Journalists (ICFJ). (2018). *A reporter's guide to using open source information*. ICFJ. https://www.icfj.org/resources/reporters-guide-using-open-source-information

ICIJ. (2016). *Panama Papers*. International Consortium of Investigative Journalists. https://www.icij.org/investigations/panama-papers/

Internet Archive. (s.d.). *Wayback Machine*. Internet Archive. https://web.archive.org

Jota, L. M. G. (2022). *A informação como elemento de difusão de poder no espaço cibernético: O uso de inteligência de fontes abertas (OSINT) no conflito entre Rússia e Ucrânia*. Repositório Institucional da UFSC. https://repositorio.ufsc.br/handle/123456789/233328

Jusbrasil. (n.d.). *Jusbrasil: Plataforma jurídica*. https://www.jusbrasil.com.br

Khan, S. A., Furuly, J. G., Vold, H. B., Tahseen, R., & Dang-Nguyen, D. T. (2023). Online multimedia verification with computational tools and osint: Russia-ukraine conflict case studies. *arXiv preprint arXiv:2310.01978*. https://doi.org/10.48550/arXiv.2310.01978

Kovach, B., & Rosenstiel, T. (2007). *The elements of journalism: What newspeople should know and the public should expect*. Three Rivers Press.

Lowenthal, M. M. (2017). *Intelligence: From Secrets to Policy* (7th ed.). CQ Press.

Maltego. (2023). *Maltego use cases for law enforcement [Documentation]*. Maltego. https://docs.maltego.com

Maltego Technologies. (s.d.). *What is Maltego?*. Maltego Technologies. . https://www.maltego.com

Mouton, F., Leenen, L., & Venter, H. S. (2014). Social engineering attack examples, templates and scenarios. *Computers & Security, 59*, 186–209. https://doi.org/10.1016/j.cose.2016.03.004

Müller, N. C., & Wiik, J. (2021). From Gatekeeper to Gate-opener: Open-Source Spaces in Investigative Journalism. *Journalism Practice*, 1–20. https://doi.org/10.1080/17512786.2021.1919171

Nelliyullathil, M. (2020). Teaching Open Source Intelligence (OSINT) Journalism: Strategies and Priorities. *COMMUNICATION & JOURNALISM RESEARCH, 61*.

NIST. (2008). *Special Publication 800-115: Technical Guide to Information Security Testing and Assessment*. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-115/final

Niu, J., Stillman, M., & Kruspe, A. (2025). OSINT or BULLSHINT? Exploring Open-Source Intelligence tweets about the Russo-Ukrainian War. *arXiv preprint arXiv:2508.03599*. https://doi.org/10.48550/arXiv.2508.03599

OCCRP. (s.d.). *Aleph*. Organized Crime and Corruption Reporting Project. https://aleph.occrp.org

Oerlemans, J. J., & Langenhuijzen, S. (2025). Balancing national security and privacy: examining the use of commercially available information in OSINT practices. *International journal of intelligence and CounterIntelligence*, *38*(2), 579-597. https://doi.org/10.1080/08850607.2025.2331672

OHCHR. (2022). *Berkeley Protocol on Digital Open Source Investigations*. OHCHR. https://www.ohchr.org/en/documents/tools-and-resources/berkeley-protocol-digital-open-source-investigations

Omand, D., Bartlett, J., & Miller, C. (2012). Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security, 27*(6), 801–823. https://doi.org/10.1080/02684527.2012.716965

OpenCorporates. (s.d.). *OpenCorporates Database*. OpenCorporates. https://opencorporates.com

OpenSanctions. (s.d.). *OpenSanctions Database*. OpenSanctions. https://www.opensanctions.org

OSINT Foundation. (2024). *Standards*. OSINT Foundation. https://www.osintfoundation.com/standards

OSINT Framework. (n.d.). *OSINT Framework: Ferramenta de coleta de inteligência*. https://osintframework.com

OSINT Industries. (n.d.). *OSINT Industries*. OSINT Industries. https://www.osintindustries.com

OSINT Industries. (2025). *OSINF vs OSINT: How Data Becomes Open-Source Intelligence*. OSINT Industries. https://www.osintindustries.com/osinf-vs-osint

OSINT-Brazuca. (s.d.). *OSINT-Brazuca*. GitHub Repository. https://github.com/OSINT-Brazuca

Osint.rocks. (s.d.). *OSINT Tools Directory*. Osint.rocks. https://osint.rocks

Paliscope. (2024). *Paliscope solutions for open-source investigations*. Paliscope. https://www.paliscope.com

Perondi, A. B., Viana, J. F. R., de Morais, J. E. V., & Tonieto, M. T. (2022). Processo de mineração de dados e análise de sentimentos em redes sociais. *Revista de Tecnologia da Informação da Faculdade Lourenço Filho*, *3*(1). https://revistas.lourencofilho.edu.br/RTI/article/view/78

Pipl. (s.d.). *People Search*. Pipl. https://pipl.com

Polglase, K., Mezzofior, G., Doherty, L., & Mankarious, S. (2022). Mariupol hospital attack: Examining how Russian forces hit a Ukraine maternity and children's hospital. *CNN*. https://edition.cnn.com/2022/03/11/europe/ukraine-mariupol-hospital-attack-intl/index.html

Pournis, S. (2022). *School of Journalism and Mass Communications Faculty of Economic and Political Sciences*.

Quivy, R., & Campenhoudt, L. van. (2019). *Manual de investigação em ciências sociais* (J. M. Marques, M. A. Mendes & M. Carvalho, Trad.). Lisboa: Gradiva.

SANS Institute. (2023). *What is Open-Source Intelligence?*. SANS Institute. https://www.sans.org/blog/what-is-open-source-intelligence

Sawant, P. B. (2003). Accountability in journalism. *Journal of Mass Media Ethics*, *18*(1), 16-28. https://doi.org/10.1207/S15327728JMME1801_2

Schaurer, F., & Störger, J. (2010). *The Evolution of Open Source Intelligence (OSINT Report 3/2010)*. ETH Zürich. https://css.ethz.ch/en/publications/css-osint.html

Sindicato dos Jornalistas. (2017). *Código Deontológico dos Jornalistas*. Sindicato dos Jornalistas. https://jornalistas.eu/codigo-deontologico/

Shere, A. (2020). Reading the Investigators their Rights: A review of literature on the General Data Protection Regulation and open-source intelligence gathering and analysis. *The New Collection*, *3*, 3-21. https://doi.org/10.24877/tnc.65

Sherlock Project. (s.d.). *Sherlock*. GitHub Repository. https://github.com/sherlock-project/sherlock

Shodan. (s.d.). *Shodan Search Engine*. Shodan. https://www.shodan.io

Silverman, C. (Ed.). (2014). *Verification handbook: An essential guide to verifying digital content for emergency coverage*. European Journalism Centre. https://verificationhandbook.com

Social Links. (s.d.). *Social Links for Maltego*. Social Links. https://sociallinks.io/integrations/maltego

SockPuppet. (s.d.). *Alias*. https://github.com/ghostinthewires/sockpuppet

Spyros, A., Koritsas, I., Papoutsis, A., Panagiotou, P., Chatzakou, D., Kavallieros, D., & Kompatsiaris, I. (2025). AI-based holistic framework for cyber threat intelligence management. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3344552

Stalder, F., & Hirsh, J. (2002). Open Source Intelligence. *First Monday, 7*. https://doi.org/10.5210/fm.v7i6.961

StealthMole. (s.d.). *StealthMole OSINT Platform*. StealthMole. https://www.stealthmole.com

Steele, R. D. (1995). The Importance of Open Source Intelligence to the Military. *International Journal of Intelligence and Counter Intelligence, 8*(4), 457–470. https://doi.org/10.1080/08850609508435291

Steele, R. D. (2007). Open Source Intelligence. In L. Johnson (Ed.), *Handbook of Intelligence Studies* (pp. 129–147). Routledge. . https://doi.org/10.4324/9780203945623

Tounsi, W., & Rais, H. (2018). A survey on cyber threat intelligence. *Computers & Security, 72*, 212–233. https://doi.org/10.1016/j.cose.2017.11.001

UNESCO. (2018). *Journalism, fake news & disinformation: Handbook for journalism education and training*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000265552

Van Puyvelde, D., & Rienzi, F. T. (2025). The rise of open-source intelligence. *European Journal of International Security*. https://doi.org/10.1017/eis.2024.25

Vaughan, A. (2024). *The role of OSINT in criminal investigations: Leveraging open-source data to combat cybercrime and organized criminal activities*. Old Dominion University. https://digitalcommons.odu.edu/ugresearch/OSINT

Vortimo. (2023). *Vortimo OSINT Browser (V1/V2) — Investigative features and workflows [Docs]*. Vortimo. https://docs.vortimo.com

WeVerify. (s.d.). *WeVerify Project*. European Commission. https://weverify.eu

WhatsMyName. (s.d.). *Username Search Tool*. WhatsMyName. https://github.com/WebBreacher/WhatsMyName

Willis, H. (2022). Dead Lay Out in Bucha for Weeks, Refuting Russian Claim, Satellite Images Show. *The New York Times*. https://www.nytimes.com/2022/04/04/world/europe/bucha-bodies-russia-ukraine.html

Yadav, A., Kumar, A., & Singh, V. (2023). Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security.

Artificial Intelligence Review, 56(11), 12407-12438. https://doi.org/10.1007/s10462-023-10595-8

Yadav, T., & Rao, A. M. (2015). Technical aspects of cyber kill chain. In *International symposium on security in computing and communication* (pp. 438-452). Springer. https://doi.org/10.1007/978-3-319-22915-7_41

Zubiaga, A. (2019). Mining social media for newsgathering: A review. *Online Social Networks and Media*, *13*, 100049. https://doi.org/10.1016/j.osnem.2019.100049

Zureik, E. (2020). "Settler Colonialism, Neoliberalism and Cyber Surveillance: The Case of Israel." *Middle East Critique, 29*(2), 219–235.