

REVUE

ISSN: 2737-8152

DROIT & SOCIETE

DOI: <https://doi.org/10.5281/zenodo.158475>

Vol, 6 N°17- Avril /Juin 2025

**L' « OPEN SOURCE INTELLIGENCE »
A L'ERE NUMERIQUE : UN SPECTRE
ETHICO-POLITIQUE ENTRE
POUVOIR, PREUVES ET LIMITES
JUDICIAIRES**

**BENNANI Hniya
EL MAYSOUR
Mohammed Amine**





L' « OPEN SOURCE INTELLIGENCE » A L'ERE NUMERIQUE : UN SPECTRE ETHICO-POLITIQUE ENTRE POUVOIR, PREUVES ET LIMITES JUDICIAIRES

OPEN SOURCE INTELLIGENCE IN THE DIGITAL AGE: AN ETHICO-POLITICAL SPECTRUM BETWEEN POWER, EVIDENCE AND JUDICIAL LIMITS

BENNANI Hniya

*Doctorante-chercheuse affiliée au Laboratoire d'Études et de Recherches en Droit Privé,
Ingénierie Juridique et Développement Durable – Faculté des Sciences Juridiques,
Économiques et Sociales de Fès – Université Sidi Mohamed Ben Abdellah.*

EL MAYSOUR Mohammed Amine

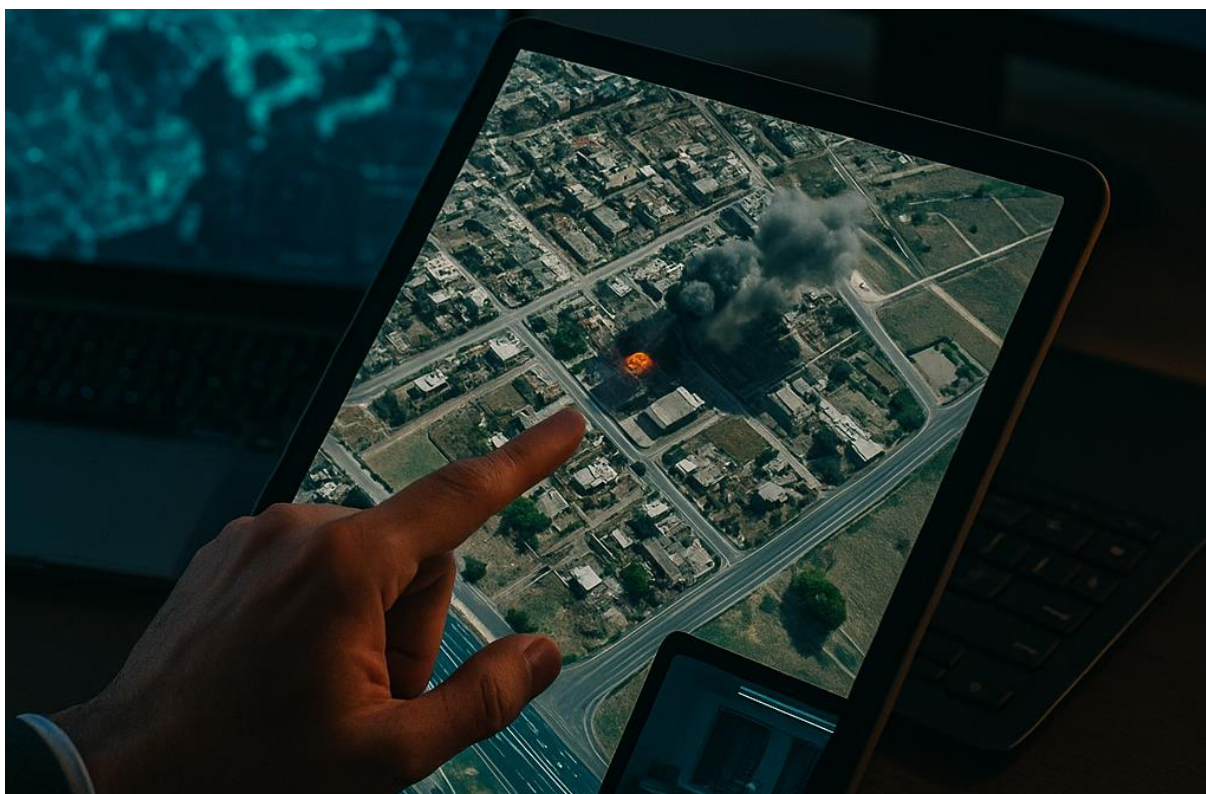
*Étudiant-chercheur inscrit au Master Gestion des Conflits et Alliance des Civilisations –
Université Euromed de Fès (UEMF).*



BENNANI, H., & EL MAYSOUR, M. A.
(2025). L' « OPEN SOURCE INTELLIGENCE » A L'ERE NUMERIQUE : UN SPECTRE
ETHICO-POLITIQUE ENTRE POUVOIR,
PREUVES ET LIMITES JUDICIAIRES.
REVUE DROIT ET SOCIÉTÉ, 6(17), 5-18.
<https://doi.org/10.5281/zenodo.15847508>



L' « OPEN SOURCE INTELLIGENCE » A L'ERE NUMERIQUE : UN SPECTRE ETHICO-POLITIQUE ENTRE POUVOIR, PREUVES ET LIMITES JUDICIAIRES



RESUME

A l'ère numérique, l'OSINT (Open Source Intelligence) émerge comme un outil polymorphe qui oscille entre révélation de réalités sociales et instrumentalisation stratégique. Employé par des acteurs aux motivations divergentes, il révèle pourtant des réalités sociales et politiques tout en reproduisant des fractures structurelles : asymétries technologiques, biais épistémologiques et impunité persistante. L'analyse de cas comme les frappes en Birmanie ou le mandat d'arrêt de la CPI contre Al-Werfalli démontre sa capacité à transformer des données brutes en preuves tangibles malgré des limites inhérentes. Au-delà d'une simple mécanique technique, l'OSINT

BENNANI Hniya

Doctorante-chercheuse en Droit Privé

*Université Sidi Mohamed Ben
Abdellah, Fès – Maroc*

EL MAYSOUR Mohammed Amine

*Étudiant-chercheur, Master Gestion
des Conflits et Alliance des
Civilisations –*

Université Euromed de Fès, Maroc

incarne un « spectre éthico-politique » où s'entremêlent innovation pouvoir et responsabilité.

Mots-clés : *OSINT, Spectre éthico-politique, Droit International Pénal, Asymétries Technologiques, Preuves numériques.*

OPEN SOURCE INTELLIGENCE IN THE DIGITAL AGE: AN ETHICO-POLITICAL SPECTRUM BETWEEN POWER, EVIDENCE AND JUDICIAL LIMITS

ABSTRACT

In the digital age, OSINT (Open Source Intelligence) emerges as a dual-edged tool, balancing between uncovering social realities and enabling strategic exploitation. Leveraged by actors with conflicting agendas, it uncovers social and political realities while perpetuating structural divides: technological asymmetries, epistemological biases, and enduring impunity. Case studies, such as airstrikes in Myanmar or the ICC's arrest warrant for Al-Werfalli, highlight its ability to convert raw data into actionable evidence, despite inherent limitations. Beyond technical processes, OSINT reflects an « ethico-political spectrum » where innovation, power dynamics and accountability collide.

BENNANI Hniya

PhD student-researcher in Private Law

*Sidi Mohamed Ben Abdellah University,
Fez - Morocco*

EL MAYSOUR Mohammed Amine

*Student-researcher, Master in Conflict
Management and Alliance of
Civilizations -*

Euromed University of Fez, Morocco

Keywords: *OSINT, Ethico-Political Spectrum, International Criminal Law, Technological Asymmetries, Digital Evidence.*

INTRODUCTION :

Dans un monde où l'information numérique prolifère à un rythme sans précédent, l'OSINT (Open Source Intelligence) s'impose comme une pratique incontournable¹ pour décrypter les réalités sociales², politiques³ et économiques⁴. Autrefois réservé aux agences de

¹ Glassman, M., & Kang, M. (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Comput. Hum. Behav.*, 28, p.674

² Charlton, T., Mayer, A., & Ohme, J. (2024). A Common Effort: New Divisions of Labor Between Journalism and OSINT Communities on Digital Platforms. *The International Journal of Press/Politics*, p.6

renseignement, ce processus de collecte et d'analyse de données ouvertes notamment sur la base de tweets⁵, images satellitaires⁶, publications en ligne⁷, est désormais mobilisé par une pluralité d'acteurs : journalistes traquant les crimes de guerre, entreprises anticipant les risques géopolitiques, ONG documentant les violations des droits humains, ou universitaires analysant les dynamiques de pouvoir. Cette démocratisation s'accompagne néanmoins de défis majeurs⁸, tant méthodologiques que juridiques, dans un cyberspace où les frontières entre public et privé se brouillent continuellement. Ainsi, la problématique centrale de cet article peut donc se formuler de la sorte : comment penser les usages contemporains de l'OSINT à travers la diversité de ses acteurs, la pluralité de ses domaines d'application et la complexité juridique des pratiques de collecte et d'analyse de données publiques dans un espace numérique aux frontières mouvantes, en intégrant un « spectre éthico-politique » ainsi que ses limites judiciaires ?

Afin d'y répondre, trois questions spécifiques guident cette réflexion : quels sont les motivations, méthodes et impacts différenciés des acteurs étatiques, économiques, médiatiques et académiques dans l'usage de l'OSINT ? Comment concilier l'exploitation de données « ouvertes » avec le respect de la vie privée et les cadres juridiques ? En quoi les outils automatisés redéfinissent-ils les pratiques traditionnelles du renseignement et de la recherche sans pour autant éliminer les biais humains et structurels ? De ces faits, trois hypothèses structurent cette étude :

1. La pluralité des acteurs génère des finalités contradictoires ;
2. L'absence de régulation spécifique favorise des pratiques à la limite de la légalité ;
3. L'automatisation des outils renforce l'objectivité des preuves OSINT mais ne supprime pas les biais humains.

L'objectif principal de cette étude est d'analyser les dynamiques contemporaines de l'OSINT en proposant un cadre théorique intégrant son spectre éthico-politique (articulé autour des finalités, de la légalité et de l'épistémologie), ses enjeux juridiques ainsi que son impact dans la sphère judiciaire. Pour ce faire, nous allons mobiliser une méthodologie hybride en combinant des données qualitatives telles que les enquêtes du collectif Bellingcat, puis,

³ Kumar, N. (2024). OSINT (OPEN SOURCE INTELLIGENCE) Exploring the Power of Open Source Intelligence in Modern Decision-Making. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, p.2

⁴ 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*, 1, p.1409

⁵ Pastor-Galindo, J., Nespoli, P., Mármol, G., & Pérez, M. (2020). The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. *IEEE Access*, 8, p.10289

⁶ Paglia, M. (2022). Open-source intelligence (OSINT) et journalisme d'investigation : l'art de faire savoir un savoir-faire ou le renouvellement d'une profession ? *Sciences de l'information et de la communication*, p.9

⁷ Deneuille, A. (2024). (Contre-)enquêtes Osint. Publicationnaire, p.3

⁸ Voir notamment : Pastor-Galindo, J., Nespoli, P., Mármol, G., & Pérez, M. (2020). The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. *IEEE Access*, 8 ; Kumar, N. (2024). OSINT (OPEN SOURCE INTELLIGENCE) Exploring the Power of Open Source Intelligence in Modern Decision-Making. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*. ; 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*. ; Van Puyvelde, D., & Rienzi, F. (2025). The rise of open-source intelligence. *European Journal of International Security*. ; Qusef, A., & Al-Kilani, H. (2022). The effect of ISO/IEC 27001 standard over open-source intelligence. *PeerJ Computer Science*, 8. ; Chaudhary, M., & Bansal, D. (2022). Open source intelligence extraction for terrorism-related information: A review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 12.

quantitatives, via les bases de données satellitaires issues de Sentinel Hub ou d'outils comme NASA FIRMS.

Pour cela, cet article s'articule autour de quatre axes complémentaires. Le premier cerne la définition et les usages de l'OSINT, entre processus technique (input/output) et spectre éthico-politique. Le deuxième explore les méthodes de collecte des données hybrides (manuelles et automatisées) et les ambiguïtés juridiques qu'elles soulèvent. Le troisième analyse la transformation des données brutes en connaissances exploitables et ce à travers des outils tels que NASA FIRMS ou Sentinel Hub en montrant comment l'expertise humaine et les biais cognitifs influencent l'interprétation. Enfin, le quatrième évalue l'impact de l'OSINT dans le domaine judiciaire en examinant son rôle dans des procédures pénales internationales notamment à l'image du mandat d'arrêt de la CPI contre Al-Werfalli.

1- L'OSINT : un concept polymorphe aux acteurs pluriels

Donner corps à une définition intégrale et exhaustive à la notion de l'OSINT (Open Source Intelligence) ou le ROSO (le Renseignement d'Origine Sources Ouvertes) s'avère être une tâche relativement difficile, d'une part en raison de l'absence d'une littérature académique suffisamment large et constituée en rapport avec cette discipline, notamment parce que l'intérêt qui y est porté par le champ académique (surtout francophone) est relativement récent, et d'une autre part, en raison de sa nature évolutive qui s'inscrit dans un développement, des mutations et des changements permanents et continus.

Cette difficulté conceptuelle ne tient pas seulement à la jeunesse du champ académique mais aussi et surtout à la nature fondamentalement contradictoire de l'OSINT : outil de transparence pour les uns, il devient un instrument de contrôle pour les autres. De ce fait et pour dépasser ce dilemme, nous proposons de conceptualiser l'OSINT comme étant un « spectre éthico-politique » structuré autour de trois axes : la finalité, la légalité et l'épistémologie.

Une autre difficulté conceptuelle réside également dans la diversité des domaines d'usage de l'OSINT. En effet, le renseignement d'origine sources ouvertes fait l'objet d'un usage courant par des acteurs diversifiés et notamment sécuritaires, comme c'est le cas des agences de sécurité étatiques qui sous-traitent leurs données à des entreprises privées comme Palantir pour en soustraire des informations dédiées à des finalités sécuritaires. Cette même soustraction peut avoir des finalités économiques tout comme le cas de certaines sociétés privées comme le groupe Eurasia, Oxford Analytica, IHS Global Insight ou Maplecroft (pour ne citer que les plus connues), qui font de la veille stratégique⁹. Cette dernière, aux côtés de la protection et de l'influence, est l'un des trois piliers du renseignement économique ou de l'intelligence économique¹⁰. Ces exemples rentrent en adéquation avec le premier axe du spectre éthico-politique, à savoir la finalité. L'OSINT sert tantôt des logiques sécuritaires et tantôt des intérêts économiques. Pourtant, ces usages peuvent coexister avec des finalités démocratiques tout comme le montre le travail de Bellingcat en documentant les crimes de guerre en Syrie. Ainsi, cette tension entre sécurité, profit et justice prouve pourquoi toute définition univoque de l'OSINT rentre impossible.

⁹ La veille stratégique consiste en l'observation, le recueil, le traitement et l'analyse des données émanant des sources d'information ouvertes dans le but de construire une connaissance qui aide les entités publiques et privées dans le processus de prise de décisions.

¹⁰ A. BENCHRIF, F. MERAND. « L'Analyse du Risque Politique », Les Presses de l'Université de Montréal, 2023, p : 60

Un autre domaine d'usage de l'OSINT est celui du champ journalistique et surtout celui du journalisme d'investigation, où on peut affirmer que cette méthode a atteint un certain degré de maturité dans la mesure où depuis la première guerre du golfe (1990-1991), les journalistes confrontés aux défis de l'hyperréalité¹¹ et à la désinformation, ont été contraints d'emprunter des méthodes propres aux services de renseignements pour révéler des informations grises grâce à l'agrégation et le croisement de sources ouvertes¹², sans avoir nécessairement un accès direct ni à des témoins ou à des témoignages, ni à des zones ou territoires sur lesquels ils enquêtent. Cette usage journalistique et analysé par Paglia¹³ comme étant un « art du faire-savoir », incarne le second axe du spectre : la légalité. Les journalistes d'investigation naviguent dans des zones grises juridiques afin de révéler des crimes ; cependant, cette pratique et bien que justifiée par l'intérêt public, questionne le respect des données et de la vie privée.

L'OSINT est également une technique très répandue chez les chercheurs universitaires, surtout chez les géopoliticiens, car elle leur confère des procédés ou encore des outils et des méthodes pour rassembler des informations leur permettant de mieux analyser pour mieux comprendre les soubassements des relations internationales. C'est par exemple le cas des géopoliticiens qui s'intéressent à la dissuasion navale américaine et qui peuvent tracer leurs trajets maritimes à travers des newsletters envoyées fréquemment par certaines sociétés privées comme Stratfor. Certes, ces trajets peuvent apparaître superflus dans certains cas, mais avec un processus de contextualisation et d'analyse, ils peuvent servir aux géopoliticiens comme moyen d'analyser, de déterminer et de comprendre les rapports de force et de négociation dans une zone géographique déterminée. Finalement, le cas académique renvoie au troisième axe qui est l'épistémologie. En effet, si l'OSINT combine des outils technologiques et une interprétation humaine, cette hybridité ne garantit pas pour autant l'objectivité : les biais cognitifs telle que la surreprésentation des sources anglophones ou structurels comme l'accès inégal aux outils dits premium, peuvent persister.

De tout ce qui précède, il apparaît que toute définition de l'OSINT reste inévitablement partielle et incomplète en raison de la pluralité de ses méthodes, de la multiplicité de ses finalités et de la diversité des acteurs étatiques, paraétatiques et privés qui en font appel. Toutefois, il est primordial de mettre de l'ordre dans toute cette complexité et de la réduire à des éléments simples pour la saisir. De cette sorte et en regroupant la logique même de cette pluralité, il apparaît que l'OSINT peut être défini comme étant un processus séquentiel de transformation des données dites « brutes » en informations « raffinées », prêtes à être déployées à des finalités d'intelligence (au sens anglais du terme). Ce processus se structure en deux phases distinctes : la première étape, appelée « input » (entrée), correspond à la collecte de données brutes qui proviennent de sources ouvertes (par exemple des photos publiques, des tweets, des commentaires, des posts sur les réseaux sociaux, des statistiques ou encore des enregistrements audio ou vidéos, etc.). La deuxième étape quant à elle, nommée « output » (sortie), consiste à analyser ces informations. En effet, les données recueillies, bien que massives et omniprésentes dans notre quotidien, restent cependant inutilisables en l'état :

¹¹L'hyperréalité est un concept philosophique développé par le philosophe post-moderniste Jean Baudrillard. Elle peut être définie comme étant un état produit par la société où la réalité a été remplacée par des simulations. V. notamment : Baudrillard, J. (1981). *Simulacres et simulation*. Paris : Éditions Galilée, p.10

¹²M. PAGLIA. « Open-source intelligence (OSINT) et journalisme d'investigation : l'art de faire savoir un savoir-faire ou le renouvellement d'une profession ? » *Sciences de l'information et de la communication*. 2022, p.10

¹³*Ibid.*

elles doivent être traitées, interprétées et transformées lors de cette phase d'analyse (output) pour acquérir une valeur concrète et opérationnelle.

Cette définition processuelle doit être complétée cependant par notre grille du « spectre éthico-politique » car réduire l'OSINT à une mécanique technique (input/output) occulte ses dimensions conflictuelles : les mêmes données « brutes » servent autant à documenter des crimes de guerre qu'à exploiter des ressources naturelles. Cette dualité révèle ainsi que l'OSINT est moins un outil neutre qu'un miroir des rapports de pouvoir.

2- L'OSINT et la collecte de données : l'illusion de la transparence

La phase initiale de collecte (input) en OSINT s'inscrit également dans le spectre éthico-politique où s'entrelacent des tensions fondamentales. Cette phase, souvent perçue comme étant une simple mécanique technique, révèle pourtant en réalité une construction politique où chaque choix méthodologique, juridique ou éthique engage une perspective différente. Le rassemblement de données peut être réalisé par le biais de deux méthodes : la première renvoie à la collecte manuelle qui repose sur une recherche directe dans les réseaux sociaux, blogs ou bases de données publiques, permettant ainsi de contextualiser des éléments subtils ; cependant, cette méthode, chronophage et limitée en volume, se voit être vulnérable aux biais cognitifs du chercheur telle que la sélection arbitraire de hashtags ou encore l'invisibilisation des crises hors des radars médiatiques. La seconde méthode quant à elle, qualifiée de semi-automatisée, utilise des outils comme Maltego¹⁴, RSS Reader, Feeder ou encore TweetDeck et permet d'agréger des masses de données tels que les métadonnées ou la géolocalisation, promettant une certaine objectivité algorithmique. Pourtant, cette promesse reste illusoire car ces outils reproduisent des asymétries structurelles à l'aune de la sous-représentation des langues minoritaires ou, comme précédemment soulevé, la domination des plateformes anglo-saxonnes. Plus encore, l'extraction de métadonnées (heure, lieu, appareil) d'une photo d'arme dans un groupe Telegram (à titre d'exemple) fermé, et bien que techniquement précise, devient une interprétation située car elle peut être lue comme une menace sécuritaire par un analyste occidental mais peut également être perçue comme étant un symbole culturel par un observateur local. Cette tension épistémologique illustre la dualité du spectre : l'OSINT oscille entre rationalité technicienne et herméneutique critique.

Cependant, force est de relever que cette dualité interprétative où la perception d'une même donnée varie entre menace et symbole, se répercute directement sur l'ambiguïté des frontières numériques : la vie privée, déjà vulnérable aux subjectivités culturelles, devient dès lors un terrain juridique et éthique instable où la transparence et la confidentialité s'affrontent sans cadre unifié. L'ambiguïté des limites de la vie privée peut se cristalliser si l'on se repose sur l'exemple précédemment évoqué où une photo publiée dans un groupe Telegram fermé et initialement destinée à un cercle restreint, devient par la suite accessible au grand public suite à une fuite ou à une ingérence du chercheur. Cette situation soulève par conséquent une question : un espace numérique est-il public dès qu'il est techniquement accessible, même sans consentement explicite ? Ici le flou normatif transforme la vie privée en une zone grise où chaque acteur arbitre discrétionnairement entre transparence et confidentialité et questionne également l'éthique de la proportionnalité en se posant la question de savoir jusqu'où peut-on violer la vie privée d'un individu pour servir l'intérêt public.

¹⁴ Pastor-Galindo, J., Nespoli, P., Mármol, G., & Pérez, M. (2020). The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. *IEEE Access*, 8, p.10294

Ainsi, l'OSINT révèle que la vie privée dans le cyberspace n'a pas de limites claires : elle est constamment redéfinie par des acteurs aux motivations contradictoires. La méthode de l'image inversée ou l'extraction de métadonnées et bien que techniquement neutres, deviennent des instruments de cette redéfinition. A titre d'exemple, une photo partagée dans un compte personnel et même restreint, peut être indexée par des moteurs de recherche, transformant ainsi un espace privé en ressource publique. En somme, cette perméabilité des frontières ouvre la voie à une autre interrogation relative à la notion même de consentement : une donnée est-elle ouverte dès lors qu'elle est techniquement accessible ou doit-elle respecter l'intention initiale de son auteur ?

3- L'OSINT : entre objectivité technologique et subjectivité humaine

La deuxième étape d'analyse, de contextualisation et de transformation des données¹⁵ « brutes » dépend fondamentalement des finalités poursuivies par le chercheur ; qu'il s'agisse d'un analyste de risque évaluant des indicateurs macroéconomiques, d'un universitaire étudiant les stratégies navales ou encore d'un juge confronté à des preuves numériques dans un procès pénal. De cette sorte, la diversité des objectifs révèle une tension entre rationalité technique et interprétation contextuelle : un même ensemble de données satellitaires sur les déploiements militaires sera analysé différemment selon qu'il sert à anticiper des risques géopolitiques ou à documenter des crimes de guerre. Pour illustrer cette dynamique, prenons l'exemple des frappes aériennes en Birmanie en 2024. Face à la difficulté d'accéder physiquement aux zones de conflits, la chercheuse Pooja Chaudhuri, associée à l'ONG Bellingcat s'est appuyée sur des photos publiées sur la page Facebook de Western News. Ces images révélaient des attaques aériennes ciblant des civils et les locaux de Médecins Sans Frontières (MSF) dans le village de Buthidaung.

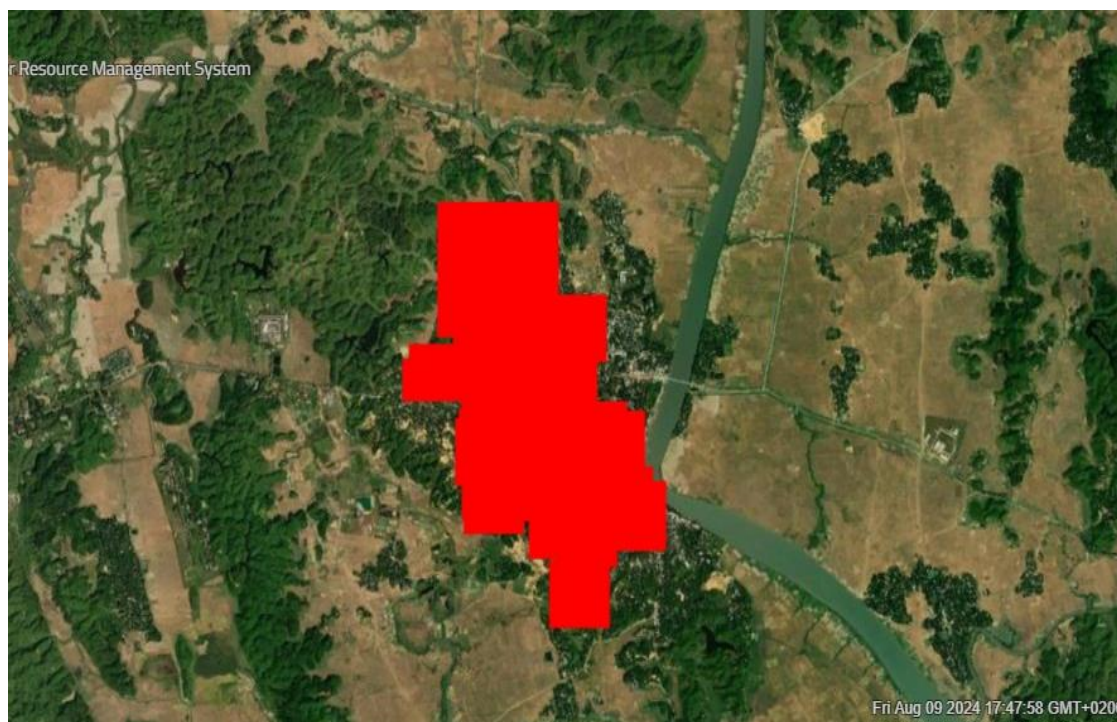


¹⁵ M. DALE, *The OSINT Handbook*. Birmingham, Packt Publishing, 2024, p.29



Photos publiées le Mercredi 24 avril 2024 à 05:30 (heure locale) sur la page Facebook de Western News

Sur la base de ces dernières, la chercheuse a mobilisé des outils comme NASA FIRMS afin de détecter des « hotspots » d'incendies pour localiser les attaques.



NASA FIRMS May 17, 2024. The red shapes reflect a 'fire hotspot' in these areas

Cette approche incarne la promesse d'objectivité technique : les données satellitaires qui sont accessibles publiquement, semblent fournir une preuve irréfutable de violations du droit humanitaire. Cependant, cette objectivité est immédiatement confrontée à un défi épistémologique : un incendie détecté par NASA FIRMS peut résulter d'une frappe aérienne

mais aussi d'un feu de forêt ou d'une combustion accidentelle. Pour dépasser cette ambiguïté, la chercheuse a recoupé ces données avec des images Sentinel Hub, utilisant des bandes spectrales (8-4-3) pour distinguer les destructions causées par des explosions de celles issues de phénomènes naturels.



Photo soustraite du satellite d'observation « Sentinel-2 » accessible sur la plateforme de Sentinel-Hub

Ainsi, ce processus hybride (à savoir technique et humain) souligne la dualité de l'OSINT : si les outils automatisés identifient des patterns, l'expertise humaine reste cruciale pour interpréter les causes et les responsabilités. Par exemple, la visualisation en *timelapse* a permis de confirmer que les incendies coïncidaient avec les frappes aériennes du 17 avril 2024.

Cependant, cette rigueur méthodologique ne suffit pas à éliminer certains biais structurels :

- Des biais techniques : les satellites Sentinel et bien que publics, sont contrôlés par l'Agence Spatiale Européenne qui signifie que l'accès à leurs données brutes, à la fréquence d'imagerie ou encore à certaines résolutions peut être à la fois limité ou encadré. Par conséquent, ceci crée une certaine forme d'asymétrie technologique dans la mesure où ces données et bien que théoriquement ouvertes, la capacité à les exploiter de manière efficace reste concentré dans certaines régions ou institutions.
- Des biais juridiques : la qualification des crimes internationaux repose sur des conventions comme la convention de Genève ou encore le Statut de Rome. Toutefois, l'application du droit international pénal reste profondément marquée par des rapports de force politiques. A titre d'exemple, des preuves OSINT qui documentent des crimes en Birmanie contre les Rohingyas ou d'autres minorités sont nombreuses et certes crédibles, mais ne garantissent pas pour autant l'ouverture d'enquêtes ou d'inculpations par la CPI¹⁶, se trouvant souvent freinées par des questions de compétence ou encore de coopération des États.
- Des biais éthiques : bien que cité plus haut, l'usage de photos, vidéos ou encore de données personnelles soulève des enjeux éthiques majeurs et ce même dans un but légitime de justice ou de documentation de crimes. Plusieurs victimes ou de proches n'ont pas consenti à l'utilisation de ces images ; leur diffusion peut donc entraîner des risques supplémentaires tels que la stigmatisation, les représailles ou pire, la réouverture des traumatismes. Ce qui soulève un dilemme important : comment concilier la transparence et la justice avec le respect de la dignité et des droits des victimes ?

Si les défis méthodologiques et éthiques de l'analyse OSINT révèlent les fractures entre objectivité promise et réalités politiques, il n'en demeure pas moins important d'interroger l'impact concret de ces preuves dans l'arène judiciaire.

4- L'OSINT devant les tribunaux : l'exemple du cas d'Al-Werfalli

Aujourd'hui, il est de plus en plus fréquent que des juridictions pénales nationales ou internationales prennent en compte des éléments de preuve collectés à partir de sources ouvertes et analysés à l'aide d'outils accessibles au public. En effet, les mutations qu'ont connues les technologies de l'information et de la communication ont renforcé cette tendance vers l'utilisation de données issues de sources ouvertes comme éléments de preuve dans les juridictions pénales.

Pour une meilleure contextualisation, prenons l'exemple de la guerre civile libyenne. Cette dernière, déclenchée à la suite du soulèvement populaire de 2011 contre le régime de Mouammar Kadhafi, a plongé le pays dans une instabilité chronique, marquée par l'effondrement de l'Etat central et l'émergence de multiples factions armées concurrentes. Après la chute de Kadhafi, le vide politique laissé a donné lieu à une fragmentation du

¹⁶ Il est important de souligner que la CPI a ouvert une enquête en 2019 mais sa compétence repose uniquement sur le fait que le Bangladesh où les Rohingyas ont été déplacés, est membre du Statut de Rome. Parallèlement, la Birmanie, non membre, ne reconnaît pas l'autorité de la CPI ce qui limite par conséquent la portée de l'enquête aux crimes transfrontaliers ou partiellement commis sur le territoire bangladais. De ce fait, malgré la crédibilité des preuves, la juridiction restrictive de la CPI constitue ici un obstacle majeur.

pouvoir entre gouvernements rivaux, notamment le Gouvernement d'Union nationale (GNA), reconnu par l'ONU et l'Armée Nationale Libyenne (ANL), dirigée par le maréchal Khalifa Haftar. Ce contexte chaotique a favorisé l'émergence de milices locales exerçant un contrôle territorial et sécuritaire sur diverses régions du pays et ce souvent en dehors de tout cadre juridique et légal. C'est dans ce contexte de conflit prolongé et de violations massives du droit international humanitaire que s'inscrit l'affaire Mahmoud Al-Werfalli, commandant au sein de la brigade Al-Saiqa, affiliée à l'ANL, accusé d'avoir ordonné et exécuté sommairement des prisonniers à Benghazi. La Cour Pénale Internationale (CPI) qui prévoit une évaluation libre des modes de preuve utilisés¹⁷, avait délivré le 15 août 2017 un mandat d'arrêt à l'encontre de Mahmoud Al-Werfalli, sur la base de 20 vidéos¹⁸ qui documentent des exécutions rendues publiques sur les réseaux sociaux pendant la période s'étendant du 3 Juin 2016 au 17 juillet 2017. L'une de ces vidéos d'exécution impliquant Al-Werfalli a fait l'objet d'une analyse approfondie par Bellingcat¹⁹ et grâce à des méthodes combinant l'étude d'images satellitaires, la comparaison de repères géographiques visibles sur les enregistrements et l'examen des ombres, les chercheurs ont pu déterminer avec précision l'emplacement et la date exacts où Al-Werfalli a ordonné l'acte, confirmant ainsi sa responsabilité directe.

De cette manière, l'OSINT s'est ainsi imposé comme une preuve clé dans le mandat d'arrêt délivré par la CPI en 2017. Ce dernier, précise que les charges reposent à la fois sur des témoignages de victimes et sur un corpus numérique inédit²⁰, contenant des vidéos montant Al-Werfalli donnant l'ordre de tirer, des publications Facebook de la brigade Al-Saiqa revendiquant les actes ainsi que des rapports d'ONG corroborant les faits. Cette approche plurielle marque un tournant : pour la première fois, des données open source ont été jugées suffisamment fiables pour inculper un commandant en exercice.

Cependant, ce succès technique contraste avec l'échec judiciaire ; malgré deux mandats d'arrêt (en 2017 et 2018)²¹, Mahmoud Al-Werfalli n'a jamais été transféré à la CPI. Les autorités de l'Armée Nationale Libyenne ont systématiquement ignoré les requêtes internationales²², puis, le 24 mars 2021, la mort du commandant à Benghazi a définitivement clos le dossier. Conformément au Statut de Rome, la CPI a dû abandonner les poursuites illustrant ainsi les limites de l'OSINT face à l'impunité politique. Ce cas donc soulève une question fondamentale : l'OSINT peut-il réellement faire justice dans des conflits où le droit international est instrumentalisé ? Si les outils techniques ont permis d'établir des vérités factuelles, leur impact cependant reste tributaire de volontés politiques souvent absentes. La mort d'Al-Werfalli et loin de clore le débat, rappelle que la transparence numérique ne suffit pas à elle seule à dépasser les réalités géopolitiques.

¹⁷ La règle 63 des dispositions générales en matière d'administration de la preuve du Règlement de procédure et de preuve de la CPI dispose dans son deuxième paragraphe que : Les Chambres sont habilitées, en vertu du pouvoir discrétionnaire visé au paragraphe 9 de l'article 64, à évaluer librement tous les moyens de preuve présentés en vue d'en déterminer la pertinence ou l'admissibilité comme le prévoit l'article 69.

¹⁸ ICC-01/11-01/17-2 15-08-2017 12/17 NM PT

¹⁹ Bellingcat « Bushes, buildings, and blood stains. Geolocating the Werfalli executions », 21 septembre 2017, YouTube, <https://www.youtube.com/watch?v=mPrxMn655lg>

²⁰ ICC-01/11-01/17-2 15-08-2017 4/17 NM PT

²¹ ICC-CPI-20170815-PR1328

²² M. OSMAN, « ICC Suspect Al-Werfalli "Escapes" from Prison in Libya », International Justice Monitor, 2018

Conclusion

À l'issue de cette analyse, il apparaît que l'OSINT, loin d'être un simple outil technique, se déploie comme un champ éminemment politique, éthique et stratégique, où se croisent finalités contradictoires, pratiques juridiquement ambiguës et interprétations marquées par des biais structurels. Ce constat permet de répondre à la problématique centrale posée : comment penser les usages contemporains de l'OSINT à travers la diversité de ses acteurs, la pluralité de ses domaines d'application et la complexité juridique des pratiques de collecte et d'analyse de données publiques dans un espace numérique aux frontières mouvantes, en intégrant un « spectre éthico-politique » ainsi que ses limites judiciaires ?

Premièrement, l'analyse des motivations, des méthodes et des effets différenciés selon les acteurs (États, entreprises, ONG, journalistes, universitaires) confirme l'hypothèse H1, selon laquelle la pluralité des acteurs engendre des finalités parfois antagonistes : protection des droits humains vs. contrôle sécuritaire, intérêt public vs. logiques de marché, transparence vs. opacité. L'OSINT apparaît dès lors comme un champ de tension, où chaque acteur négocie sa propre éthique d'usage.

Deuxièmement, les pratiques de collecte de données, qu'elles soient manuelles ou automatisées, ont mis en lumière un vide juridique persistant concernant la définition des espaces publics et privés numériques. L'absence d'un encadrement clair alimente une zone grise juridique, donnant lieu à des pratiques qui, bien qu'efficaces sur le plan opérationnel, peuvent être discutables sur le plan éthique et légal. Cela confirme l'hypothèse H2, à savoir que l'absence de régulation spécifique favorise des pratiques à la limite de la légalité.

Troisièmement, l'examen des cas empiriques – qu'il s'agisse des frappes en Birmanie ou du mandat d'arrêt contre Al-Werfalli – montre que l'automatisation des outils OSINT renforce effectivement la capacité à produire des preuves factuelles, mais ne permet pas d'évacuer les biais humains, cognitifs et structurels. L'objectivité algorithmique reste conditionnée par l'interprétation humaine, les rapports de pouvoir géopolitiques, l'accès inégal aux technologies, et les limites du droit international. Ce constat valide l'hypothèse H3, soulignant que l'automatisation n'abolit ni les subjectivités, ni les asymétries.

En réponse aux questions secondaires, cette étude a démontré que :

- les acteurs utilisent l'OSINT selon des finalités très variées qui traduisent des rapports de force hétérogènes ;
- l'utilisation de données ouvertes soulève des défis considérables en matière de respect de la vie privée, d'éthique de la recherche et de protection juridique ;
- les outils automatisés, bien qu'efficaces pour traiter de grands volumes de données, n'éliminent pas la nécessité d'un regard critique et contextualisé.

Ainsi, l'OSINT incarne à la fois un levier de justice et un risque d'instrumentalisation, un outil de dévoilement et un mécanisme de contrôle, un symbole d'innovation technologique et une source de tensions normatives. Son efficacité en matière de transparence et de production de vérité ne garantit pas son impact judiciaire, comme en témoigne l'affaire Al-Werfalli, où la preuve numérique n'a pu surmonter les obstacles politiques à l'arrestation et au jugement.

En définitive, si l'OSINT porte en lui une promesse puissante de démocratisation de l'information, cette promesse ne pourra être tenue que sous certaines conditions : la mise en

place d'un cadre juridique international cohérent, l'adoption de standards éthiques partagés, et la reconnaissance des limites cognitives et politiques inhérentes à tout traitement de données. À cette condition seulement, l'OSINT cessera d'être un spectre pour devenir un vecteur durable d'intelligence, de responsabilité et de justice dans l'ère numérique.

Bibliographie :

Ouvrages et articles scientifiques

Benchrif, A., & Mérand, F. (2023). *L'analyse du risque politique*. Les Presses de l'Université de Montréal.

Charlton, T., Mayer, A., & Ohme, J. (2024). A common effort: New divisions of labor between journalism and OSINT communities on digital platforms. *The International Journal of Press/Politics*.

Chaudhary, M., & Bansal, D. (2022). Open-source intelligence extraction for terrorism-related information: A review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 12(1).

Deneuve, A. (2024). (Contre-)enquêtes Osint. *Publictionnaire*.

Glassman, M., & Kang, M. J. (2012). Intelligence in the Internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior*, 28(2), 673–682.

Baudrillard, J. (1981). *Simulacres et simulation*. Paris : Éditions Galilée.

Kumar, N. (2024). OSINT (Open Source Intelligence): Exploring the power of open source intelligence in modern decision-making. *International Journal of Scientific Research in Engineering and Management*.

Dale, M. (2024). *The OSINT handbook*. Birmingham, UK: Packt Publishing.

Osman, M. (2018). ICC suspect Al-Werfalli “escapes” from prison in Libya. *International Justice Monitor*.

Paglia, M. (2022). Open-source intelligence (OSINT) et journalisme d'investigation : l'art de faire savoir un savoir-faire ou le renouvellement d'une profession ? *Sciences de l'information et de la communication*, (6).

Pastor-Galindo, J., Nespoli, P., Mármol, G., & Pérez, M. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *IEEE Access*, 8, 1–22

Qusef, A., & Al-Kilani, H. (2022). The effect of ISO/IEC 27001 standard over open-source intelligence. *PeerJ Computer Science*, 8, e945.

Van Puyvelde, D., & Rienzi, F. (2025). The rise of open-source intelligence. *European Journal of International Security*.

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*.

Documents juridiques – Cour pénale internationale

Cour pénale internationale. (2017). *ICC-01/11-01/17-2 15-08-2017 4/17 NM PT*.

Cour pénale internationale. (2017). *ICC-01/11-01/17-2 15-08-2017 12/17 NM PT*.

Cour pénale internationale. (2017). *ICC-CPI-20170815-PR1328*.

Ressources en ligne

Bellingcat. (2017, September 21). *Bushes, buildings, and blood stains. Geolocating the Werfalli executions* [Video]. YouTube. <https://www.youtube.com/watch?v=mPrxMn655Ig>

NASA FIRMS. (n.d.). *Fire Information for Resource Management System*. <https://firms.modaps.eosdis.nasa.gov/>