OSINT : CADRE NORMATIF ET RESISTANCE AU CHANGEMENT

RAPHAËL LIOTIER

DIPLOME UNIVERSITAIRE CYBERCRIMINALITES : ENJEUX ET DEFIS HUMAINS - UNIVERSITE BORDEAUX MONTAIGNE

Résumé

Cet article examine les raisons de la résistance institutionnelle au recours à des civils spécialisés dans la réalisation d'opérations d'OSINT (renseignement en sources ouvertes) au sein des enquêtes pénales françaises. À travers une analyse doctrinale et normative, il identifie deux principales sources de résistance : l'incertitude procédurale quant au statut juridique des civils intervenants, et les risques liés à la loyauté et à la recevabilité des preuves issues de sources numériques. En réponse, l'article plaide pour une clarification procédurale, la reconnaissance d'une expertise spécifique et un encadrement éthique et technique rigoureux.

Abstract

This paper analyzes the institutional resistance to engaging civilian experts in Open Source Intelligence (OSINT) operations within French criminal investigations. Through a doctrinal and normative analysis, it identifies two main factors of resistance: procedural uncertainty concerning the legal status of civilian contributors, and the risks associated with the integrity and admissibility of digital evidence derived from open sources. To address these issues, the paper advocates clarifying procedural frameworks, formally recognizing OSINT expertise, and establishing rigorous ethical and technical guidelines.

Mots clés / Keywords

OSINT ; Résistance au changement / Resistance to change ; Procédure pénale / Criminal procedure ; Encadrement juridique / Legal framework ; Expertise civile / Civilian expertise ; Sources ouvertes / Open sources ; Intelligence artificielle / Artificial intelligence.

Introduction

Le recours aux sources ouvertes dans le cadre d'enquêtes judiciaires ne constitue plus une hypothèse marginale, mais une réalité croissante. Dans ce contexte, le projet VIDOCQ, porté par un consortium basé à Bordeaux, vise à renouveler les approches d'investigation numérique en s'appuyant sur une coopération intersectorielle réunissant forces de sécurité, magistrats, acteurs économiques, chercheurs et citoyens. Les investigations en sources ouvertes, ou OSINT (de l'anglais « open source investigations ») y sont utilisées à la fois comme outils d'appui aux enquêtes et comme instruments de veille technologique. Cette dynamique collaborative permet la co-construction de solutions intégrant notamment l'intelligence artificielle, dans le but d'automatiser certaines phases de traitement de l'information et d'anticiper l'évolution des pratiques délictueuses. Le choix du nom « VIDOCQ » est opportun : il fait écho à une tradition française d'ouverture de l'enquête aux acteurs civils. Dès 1811, la brigade de la sûreté générale de Paris, dirigée par Eugène-François Vidocq, mobilisait déjà des profils extérieurs aux institutions, préfigurant les logiques collaboratives qui fondent aujourd'hui ce projet.

Le recours, par les services enquêteurs, à l'expertise technique de civils spécialisés en OSINT soulève plusieurs difficultés. Ces pratiques visent à exploiter des informations librement accessibles en ligne, susceptibles d'apporter un appui concret à des investigations judiciaires.

Toutefois, deux obstacles majeurs sont régulièrement identifiés. D'une part, l'absence d'un cadre juridique clairement défini pour encadrer ce type de dispositif entretient l'incertitude sur la valeur procédurale des données collectées. D'autre part, la participation de professionnels extérieurs au champ institutionnel, notamment issus du monde juridique, est perçue comme un risque, dans la mesure où les connaissances acquises pourraient être mobilisées pour contester la régularité de preuves obtenues dans des conditions similaires.

Ces réserves révèlent une difficulté structurelle : la persistance d'une méfiance institutionnelle à l'égard de pratiques encore jugées insuffisamment encadrées juridiquement, et dont l'intégration pourrait fragiliser l'équilibre procédural existant.

Cette résistance au changement, loin de relever uniquement d'une opposition de principe, découle de plusieurs facteurs : incertitude sur le statut procédural du recours à des tiers spécialisés en OSINT, crainte d'une mise en péril de la procédure, auxquelles s'ajoute un réflexe protecteur propre aux institutions judiciaires, structurellement peu encline à intégrer une nouvelle pratique sans procédure préalable formalisée.

Les enjeux soulevés par l'intégration de l'OSINT dans la procédure pénale touchent à la fois aux fondements de l'action publique et aux capacités opérationnelles des institutions judiciaires face à la criminalité contemporaine. Dans un contexte de surcharge informationnelle et de mutation numérique, comprendre les freins à l'intégration d'expertises extérieures dans le champ pénal devient une nécessité.

En quoi précisément le recours aux services de civils pour la réalisation des opérations d'OSINT suscite-t-il une forte résistance de la part des acteurs de la chaîne pénale ?

Deux hypothèses guident cette étude :

- l'absence de certitude sur l'intégration dans un cadre procédural du recours à des tiers civils pour la réalisation d'opérations OSINT constitue un frein majeur à leur intégration

dans les enquêtes judiciaires, en raison des risques pesant sur la recevabilité des preuves et sur le respect des droits fondamentaux ;

- la mise en œuvre de l'OSINT en contexte pénal rencontre une résistance institutionnelle liée à des incertitudes techniques, juridiques et déontologiques, nécessitant la création d'un cadre normatif strict pour garantir la fiabilité, la loyauté et la valeur probatoire des éléments collectés.

Ce travail entend ainsi contribuer à une meilleure compréhension des logiques de résistance à l'innovation dans le secteur judiciaire. Il vise à éclairer les conditions d'un usage encadré de l'OSINT par les autorités, tout en identifiant les leviers possibles pour favoriser une conduite du changement respectueuse des droits fondamentaux.

Cette étude s'appuie sur une méthodologie descriptive et documentaire. Cette recherche repose cependant sur une observation empirique. En 2025, dans le cadre de mon activité professionnelle d'avocat, j'ai constaté pour la première fois l'inclusion de rapports d'OSINT dans des dossiers d'enquête.

Le choix d'un design descriptif permet d'analyser un phénomène encore émergent, en structurant l'analyse autour de matériaux théoriques, normatifs et doctrinaux. Ce design présente l'avantage d'articuler une analyse rigoureuse avec une réflexion prospective sur l'évolution du cadre procédural de l'OSINT.

L'étude s'articule autour de trois axes principaux. Dans un premier temps, elle précise le périmètre de l'OSINT et son utilisation croissante dans les enquêtes judiciaires, en soulignant les compétences spécifiques nécessaires. Ensuite, elle identifie les facteurs organisationnels, culturels, juridiques et procéduraux à l'origine des réticences institutionnelles actuelles. Enfin, l'étude propose des solutions concrètes, visant à lever ces résistances par une clarification juridique des sources employées, l'élaboration d'un cadre opérationnel rigoureux, la reconnaissance officielle de l'expertise OSINT et un encadrement spécifique de l'utilisation de l'intelligence artificielle.

1 Pertinence de l'OSINT dans la conduite des enquêtes judiciaires

C'est à l'occasion de dossiers traités en 2025, dans le cadre de mon activité d'avocat, que j'ai pour la première fois constaté la présence de rapports d'OSINT dans des procédures pénales. Mon secret en couvre le contenu en raison du secret professionnel, cependant certaines caractéristiques générales peuvent être évoquées. Ces caractéristiques sont les suivantes :

- les opérations d'OSINT observées ont été menées directement par des membres des forces de sécurité intérieure (policiers ou gendarmes), sans mention d'un tiers requis, et documentées dans des procès-verbaux ;
- ces opérations reposaient sur des outils accessibles en ligne ou plateformes de réseaux sociaux, et portaient principalement sur l'environnement de personnes mises en cause ;
- si une traçabilité des actions menées était mentionnée, elle demeurait sommaire ;
- dans tous les cas, les résultats issus de ces recherches ont influencé les suites de l'enquête.

Ces constats rejoignent ceux formulés par Cyril L. (2025), qui, à partir d'une analyse qualitative de 66 dossiers judiciaires traités entre 2020 et 2024 par une unité régionale spécialisée dans les affaires complexes, met en évidence l'utilité opérationnelle de l'OSINT. Selon lui, ces méthodes peuvent contribuer de manière significative à l'identification de pistes, de co-auteurs, de témoins ou d'éléments contextuels utiles à la manifestation de la vérité.

1.1 Qu'est ce que l'Osint ?

L'OSINT (de l'anglais « open source intelligence »), qui peut prendre en français le sigle ROSO (pour « renseignement d'origine sources ouvertes »), correspond à la collecte, l'analyse et le traitement d'informations accessibles publiquement. L'OSINT n'a pas, à ce jour, en droit français, de définition légale.

Van Puyvelde et Tabárez Rienzi (2025) définissent l'OSINT comme un ensemble de pratiques consistant à collecter, valider et exploiter des données accessibles au public afin de répondre à un besoin informationnel[1].

L'Osint repose ainsi sur l'emploi de sources ouvertes, définies au sein du rapport d'activités 1996 du Comité permanent de contrôle des services de renseignement (1996, p. 198) comme « toute information à laquelle le public peut accéder de manière légale, peu importe qu'il y ait une contrepartie financière ou non ».

Par définition, ces pratiques se limitent donc à l'exploitation d'informations accessibles à tout internaute, sans fraude.

[1] « OSINT is a set of practices involving the collection, validation, and exploitation of publicly available data and information to meet informational needs ».

Au regard du caractère très évolutif de l'OSINT, il est impossible de classifier toutes les composantes et tous les outils qui en sont le support, ainsi que les ressources que nécessitent les opérations d'OSINT.

Toute présentation par l'exemple est donc forcément datée au regard de l'évolution extrêmement rapide des techniques dans ce domaine. Les exemples ci-après sont ainsi imparfaits et non exhaustifs, et ont pour seule vocation d'illustrer des possibilités de recherche offertes par l'OSINT.

Les techniques d'OSINT les plus répandues consistent notamment en une :

- analyse des résultats de moteurs de recherche (dorking, advanced search operators) ;
- recherche inversée d'images à l'aide d'outils dédiés (tels que TinEye, Yandex Images ou Google Image) pour identifier des lieux, objets ou personnes ;
- consultation d'archives en ligne (comme Wayback Machine ou Archive.today) ;
- exploration de publications sur des services en ligne, notamment sur les réseaux sociaux ;
- schématisation automatisée d'identités, d'alias et de relations via des services et plateformes spécialisés, pour une clientèle institutionnelle ou civile, telles que Shadowdragon, Palantir, OsintLab, Chapsvision, Maltego, Pipl ou Social Links ;
- extraction des métadonnées de fichiers numériques (données contenues dans des images et photographies, propriétés intégrées dans les documents) ;
- géolocalisation basée sur des indices contextuels, consultation et recherche sur des images satellites, et analyse visuelle et géographique assistée par des outils comme SunCalc, Sentinel Hub, Mapillary, GeoLocator ou Terrapattern, permettant de croiser orientation solaire, caractéristiques topographiques et éléments urbains ;
- analyse de registres pour identifier les propriétaires de sociétés, de noms de domaine ou d'actifs matériels ou immatériels, et exploitation des données publiques de registres d'entreprises et d'administrations (bases brevets et marques, registres publics, plateformes d'agrégation de données en open data telles que Pappers) ;
- utilisation de systèmes d'exploitation et de navigateurs donc le paramétrage limite les traces numériques et possibilité d'identification.

Des méthodes dont la licéité peut être sujet à interprétation, voire à controverse, existent en OSINT. Parmi celles-ci figurent notamment :

- le recours à des identités d'emprunt (« sock puppets » ou faux profils), et leur utilisation active pour interagir directement avec des tiers ou pénétrer des communautés fermées afin d'y obtenir des informations ;
- le « web scraping », « harvesting » ou en français « moissonnage », pratique qui recouvre l'ensemble des techniques consistant à extraire de façon automatisée et indifférenciée un volume important de données d'un service ;
- l'analyse d'images par reconnaissance faciale ;
- l'accès en ligne à des diffusions ou données de terminaux connectés, tels que des webcam, par le biais de services tels que shodan.io ;
- l'utilisation de données issues de fuites de données et/ou d'attaques informatiques.

1.2 Champs d'application

En raison de la qualité et de la pertinence des données qu'elle permet d'obtenir, l'OSINT tend à s'imposer comme une méthode couramment mobilisée dans de nombreux domaines d'application.

Ainsi, l'OSINT est employé depuis toujours par les services de renseignement, Oudet (2021, p. 63) expliquant à son sujet que :

- « Durant la guerre froide, le recours aux savoirs extérieurs est peu institutionnalisé. Cette tendance est étroitement liée à la relégation de l'OSINT au rang de discipline marginale du renseignement. C'est au cours des années 1990 et plus encore après le 11 septembre 2001 que l'OSINT connaît une phase de réhabilitation théorique et pratique bien que ses usages ne fassent pas l'objet d'un consensus ».

L'OSINT constitue également un fondement méthodologique pour de nombreuses enquêtes journalistiques, notamment dans le cadre du journalisme d'investigation.

À titre d'exemple, le média Bellingcat a mené une enquête approfondie en OSINT sur le crash du vol MH17 de la Malaysia Airlines, survenu en Ukraine le 17 juillet 2014. Grâce à l'analyse de sources ouvertes, leurs travaux ont permis d'établir une reconstitution détaillée des faits. Dans la conclusion de leur rapport, ils affirment ainsi[2] :

- « Sur la base des informations ci-dessus, on peut conclure que le 17 juillet 2014, un lanceur de missiles Bouk, provenant de la 53e brigade près de Koursk, en Russie, a été acheminé de Donetsk à Snijné. Il a ensuite été déchargé et a roulé de manière autonome jusqu'à un champ au sud de Snijné, où, vers 16h20, il a lancé un missile sol-air qui a touché le vol Malaysia Airlines 17 alors qu'il survolait l'Ukraine. Le matin du 18 juillet, le lanceur de missiles Bouk a été transporté de Louhansk, en Ukraine, vers la Russie en traversant la frontière. Les scénarios alternatifs présentés par le ministère russe de la Défense et Almaz-Antey sont, au mieux, profondément erronés, et au pire, montrent une tentative délibérée de tromper en utilisant des preuves fabriquées ».

Schwartz (2021) illustre également la mobilisation de l'OSINT dans le cadre d'enquêtes journalistiques en revenant sur l'identification rapide de plusieurs participants à l'envahissement du Capitole, le 6 janvier 2021. Il montre comment des journalistes, dont Ronan Farrow, ont utilisé des traces numériques accessibles en ligne pour établir, de manière rigoureuse, l'identité de certains individus impliqués, démontrant ainsi l'efficacité des techniques OSINT dans des contextes d'investigation à fort enjeu démocratique.

---

[2] "Based on the information above, it can be concluded that on July 17, 2014 a Buk missile launcher, originating from the 53rd Brigade near Kursk, Russia, travelled from Donetsk to Snizhne. It was then unloaded and drove under its own power to a field south of Snizhne, where at approximately 4:20 pm it launched a surface-to-air missile that hit Malaysia Airlines Flight 17 as it flew over Ukraine. On the morning of July 18, the Buk missile launcher was driven from Luhansk, Ukraine, across the border to Russia. Alternative scenarios presented by the Russian Ministry of Defense and Almaz-Antey are at best deeply flawed, and at worst show a deliberate attempt to mislead using fabricated evidence". https://www.bellingcat.com/app/uploads/2015/10/MH17-The-Open-Source-Evidence-EN.pdf

L'OSINT est mobilisé dans la recherche de preuves relatives aux crimes de guerre et aux crimes contre l'humanité. Limonier et Audinet (2022, p. 6) soulignent que la communauté OSINT, composée de journalistes, d'enquêteurs indépendants ou encore de militants, tend à jouer un rôle central dans ce domaine. Dans la même perspective, Aumaître et Letoqueux (2022, p. 49) identifient la collecte et l'analyse de données en sources ouvertes comme un nouveau paradigme dans les méthodes d'enquête appliquées aux crimes internationaux.

En septembre 2023, le Bureau du Procureur de la Cour pénale internationale a présenté un projet de politique générale mettant en avant l'importance croissante des preuves numériques issues de sources ouvertes. Dans un contexte marqué par la prolifération des contenus produits au cœur des conflits, l'OSINT est désormais considérée comme un levier central pour améliorer l'efficacité, la rapidité et l'objectivité des enquêtes. Pour accompagner cette évolution, la CPI a engagé des investissements dans des technologies avancées de collecte, de traitement et de diffusion à grande échelle de ces données numériques.

Jouette (2024) confirme cette évolution. Il note que le conflit en Ukraine a fortement contribué à la reconnaissance de l'OSINT comme source de preuve crédible, au point d'inciter le Bureau du Procureur à mettre en place une plateforme dédiée au signalement d'informations par le public. Cette évolution s'inscrit dans un processus plus large de légitimation juridique : Jouette cite notamment la décision de la CPI dans l'affaire Ahmad Al Faqi Al Mahdi (2024), où des preuves numériques ont été utilisées pour établir la culpabilité de l'accusé.

L'OSINT est également mise en œuvre par certaines administrations publiques dans le cadre de missions de contrôle et de lutte contre la fraude. A titre d'exemple, depuis la loi de finances pour 2020 (article 154 de la loi n°2019-1479 du 28 décembre 2019), l'administration fiscale et l'administration des douanes et droits indirects sont autorisées à collecter et exploiter, par des traitements informatisés et automatisés (excluant tout recours à la reconnaissance faciale), les contenus manifestement rendus publics par leurs auteurs sur les plateformes en ligne, y compris lorsque l'accès à ces contenus nécessite la création d'un compte.

Ce dispositif a été étendu par la loi de finances pour 2024 (article 112 de la loi n°2023-1322 du 29 décembre 2023). Elle permet désormais à certains agents spécialement habilités de procéder, dans des conditions encadrées, à des opérations de recherche de manquements réalisées sous pseudonyme.

L'OSINT ne constitue pas seulement une méthode d'enquête ou de renseignement : elle s'inscrit également dans une logique de marché. Comme le souligne Oudet (2021, p. 65), il s'agit désormais d'un espace où interagissent les services de renseignement, les acteurs du big data, de l'intelligence artificielle, ainsi que les fournisseurs de services spécialisés dans le traitement de l'information.

Chopin et Oudet (2023) soulignent par ailleurs le développement d'une offre structurée de formation et de diffusion des savoirs en OSINT à l'échelle internationale. Des institutions publiques et privées, comme des centres de formation spécialisés, des services de police ou encore des plateformes indépendantes, proposent aujourd'hui des contenus pédagogiques, des outils pratiques ou des guides méthodologiques accessibles en ligne. Cette dynamique contribue à la professionnalisation du secteur et à la standardisation progressive des pratiques.

1.3 Professionnalisation du secteur et opportunité du recours aux compétences de civils

Renault, Charon et Laurençon (2022) identifient une double dynamique à l'origine du déploiement actuel de l'OSINT : d'une part, la multiplication des sources ouvertes disponibles en ligne, et d'autre part, la professionnalisation croissante des méthodes d'exploitation de ces données.

L'usage généralisé d'internet rend aujourd'hui accessible à un très large public des pratiques relevant de l'OSINT, souvent sans que celles-ci soient nommées comme telles. En effet, quelques données éparses suffisent à reconstituer des informations complémentaires sur une personne, un lieu ou une activité, grâce à des recherches non structurées mais efficaces. Qu'il s'agisse de mettre un visage sur un nom, de retracer un parcours professionnel, d'identifier des relations, ou encore de visualiser un lieu précis via des outils cartographiques, l'OSINT s'inscrit de plus en plus dans les pratiques courantes, bien au-delà des seuls cercles spécialisés.

Cependant, les techniques d'OSINT ne peuvent être exploitées à leur plein potentiel que par des professionnels disposant d'une expertise approfondie. Van Puyvelde et Tabárez Rienzi (2025) rappellent que, bien que l'OSINT soit souvent perçue comme une pratique ouverte et accessible, elle repose en réalité sur des compétences techniques, des ressources spécialisées et des outils technologiques qui ne sont ni universellement maîtrisés, ni aisément mobilisables. La maîtrise des outils d'analyse, l'accès à certaines bases de données payantes, ainsi que l'expertise thématique indispensable à une interprétation rigoureuse des informations, requièrent un haut niveau de compétences.

Dans le champ du renseignement, Oudet (2021, p. 64) rappelle que le recours à des experts extérieurs n'est pas une pratique nouvelle pour les services français : dès 1995, Claude Silberzahn, alors directeur de la DGSE, évoquait déjà des collaborations ponctuelles avec des spécialistes civils. Néanmoins, ces interactions restaient informelles.

Ce qui se joue aujourd'hui, selon Oudet, c'est la formalisation progressive de dispositifs durables intégrant les savoirs extérieurs au fonctionnement des institutions de renseignement. Cette logique de partenariat s'observe également dans d'autres domaines : Schwartz (2021) souligne les effets fructueux de la coopération entre acteurs civils et journalistes, tandis que dans le champ judiciaire, Cyril L. (2025) précise que « la source civile d'un élément n'en disqualifie pas l'usage, pourvu que sa production respecte les standards d'enquête ».

2 Resistance au changement causée par la pratique actuelle de l'Osint

2.1 Les causes organisationnelles et culturelles de la résistance

Pesqueux (2020) rappelle que la résistance au changement n'est ni aberrante ni irrationnelle, mais consubstantielle à tout processus de transformation. Elle traduit une tension entre les injonctions au changement et les routines stabilisatrices d'un système. Loin d'être un simple obstacle, elle peut révéler des contradictions internes, une perte de repères, voire une contestation légitime.

L'importance des dimensions cognitives (dissonance), sociales (logiques d'adhésion ou de rejet) et politiques (structures de pouvoir) est ainsi à prendre en compte dans les comportements de résistance.

Le cadre théorique proposé par Pesqueux (2020) permet en ce sens d'éclairer les raisons des réticences institutionnelles à l'intégration de ressources civiles réalisant des opération d'OSINT au support des investigations pénales.

Loin d'être une opposition irrationnelle ou conservatrice, cette résistance s'inscrit dans une logique organisationnelle plus profonde. L'introduction de nouvelles méthodes d'investigations, mobilisant des compétences techniques de tiers et remettant en question les monopoles professionnels traditionnels, perturbe les compromis sur lesquels repose la stabilité de l'institution. L'OSINT engage un déplacement des savoirs et des pouvoirs en matière d'investigation, rendant visibles les tensions entre innovation technique et procédurale et culture judiciaire.

Dans ce contexte, la résistance apparaît moins comme un refus que comme un mécanisme de régulation d'un changement perçu comme trop rapide, trop peu encadré, et susceptible d'éroder les garanties fondamentales du procès pénal.

L'analyse de Diaz et Desbiens (2011), à partir de l'exemple québécois de l'implantation de la police communautaire, met en lumière les dynamiques classiques de résistance au changement au sein de la police. Leur étude montre que les blocages ne tiennent pas nécessairement au rejet des objectifs du changement, mais à la remise en cause des routines, des identités professionnelles et des rapports de pouvoir. Transposée au champ de l'OSINT, cette grille de lecture permet de comprendre pourquoi son intégration dans les pratiques judiciaires et policières suscite des résistances : elle déstabilise les savoir-faire traditionnels, fait émerger de nouvelles formes de légitimité experte, et oblige à redéfinir les modes d'enquête et les rapports à l'information. Ainsi, l'OSINT ne se heurte pas uniquement à une inertie technique ou juridique, mais à une transformation plus profonde des équilibres organisationnels.

2.2 Les contraintes juridiques et procédurales

Dans le cadre d'une enquête diligentée par le parquet, les actes d'investigation ont pour objectif la constatation des infractions, la réunion des preuves et l'identification de leurs auteurs, conformément aux dispositions de l'article 14 du code de procédure pénale. Lorsqu'une information judiciaire est ouverte, le juge d'instruction procède, en application de l'article 81, alinéa 1er du même code, à tous les actes utiles à la manifestation de la vérité.

Les résultats d'opérations d'OSINT peuvent, dès lors, contribuer à l'établissement de la vérité judiciaire : ils peuvent fonder une décision de poursuite, servir de support à une condamnation ou, au contraire, conduire à une relaxe ou à un acquittement. Inversement, leur usage inapproprié ou leur interprétation erronée peut provoquer l'échec d'une procédure, voire conduire à une erreur judiciaire.

Face à ces enjeux, magistrats, enquêteurs et avocats doivent faire preuve d'une rigueur particulière dans l'appréciation de chaque information recueillie.

Ainsi, outre la question même de la preuve, la réticence institutionnelle à l'intégration des opérations d'OSINT, notamment lorsqu'elles impliquent des ressources civiles, trouve son origine dans la nécessité de garantir trois exigences fondamentales : le respect des droits fondamentaux, l'inscription de l'acte dans un cadre procédural clair, et l'absence de commission d'infractions

pénales au cours des opérations. Ces conditions sont indispensables à la sécurisation des pratiques et à l'acceptabilité de leur emploi.

2.2.1 Principe de liberté de la preuve pénale et principe de loyauté

En matière pénale, le principe de liberté de la preuve est consacré par l'article 427 du code de procédure pénale. Celui-ci prévoit que, sauf disposition contraire, les infractions peuvent être établies par tout mode de preuve, le juge statuant d'après son intime conviction et sur la base d'éléments débattus contradictoirement.

En conséquence, des parties privées peuvent produire des éléments de preuve obtenus de manière déloyale (Cass. crim., 31 janvier 2007, n° 06-82.383, CEDH, 12 juillet 1988, req. n° 10862/84) à condition que l'administration n'ait pas participé à leur obtention et que les droits de la défense soient garantis (Cass. crim., 11 mai 2006, n° 05-84.837 ; Cass. crim., 27 novembre 2013, n° 13-85.042).

En effet, les autorités publiques sont tenues de respecter un principe de loyauté dans l'obtention de la preuve. En ce sens elles ne peuvent pas participer à l'obtention de preuves par un moyen frauduleux (Cass. crim., 11 mai 2006, n° 05-84.837 ; Cass. crim., 27 novembre 2013, n° 13-85.042) être l'instigateur du délit support de son obtention (Cass. crim,28 octobre 1991, n° 90-83.692), ou provoquer à la commission d'une infraction (CEDH, Teixeira de Castro c. Portugal, 9 juin 1998, req. n° 44/1997/828/1034, Cass. ass. plén., 9 décembre 2019, n° 18-86.767).

Elles peuvent en revanche provoquer à la preuve, c'est à dire recourir à un stratagème pour obtenir la démonstration d'une infraction déjà réalisée.

Audibert (2025, p. 2) rappelle cependant que « le stratagème employé par un agent de l'autorité publique pour la constatation d'une infraction ou l'identification de ses auteurs ne constitue pas en soi une atteinte au principe de loyauté », sauf s'il porte atteinte à un droit essentiel ou une garantie fondamentale. Ce critère permet d'admettre certains procédés, comme le recours à des pseudonymes par les enquêteurs sur des plateformes en ligne où l'usage de l'anonymat est courant (Cass. crim., 25 octobre 2000, n° 00-80.829). A ce sujet, il est à noter que les conditions générales des services existants actuellement en ligne écartent presque systématiquement la possibilité de recourir à un pseudonyme. Dans un tel cas, l'utilisation d'un pseudonyme pourrait caractériser un manquement contractuel qui pourrait être mobilisé au support de la caractérisation du caractère frauduleux de l'opération.

Cette dissymétrie entre la liberté probatoire reconnue aux parties privées et les contraintes déontologiques imposées aux autorités publiques crée une tension structurelle dans l'intégration des outils d'OSINT aux pratiques judiciaires.

2.2.2 Respect des droits fondamentaux

Les techniques d'OSINT, qu'elles soient mobilisées par des acteurs publics ou privés, doivent impérativement respecter les droits fondamentaux garantis par les normes constitutionnelles, européennes et internationales. Ce respect constitue un fondement juridique essentiel pour apprécier la licéité et la légitimité de leur usage dans un contexte judiciaire.

L'exploitation de résultats issus de l'OSINT dans une procédure juridictionnelle doit notamment s'inscrire dans le respect des garanties offertes par l'article 6 de la Convention européenne des droits de l'homme (CEDH), qui consacre le droit à un procès équitable, incluant notamment le

principe du contradictoire (également consacré à l'article préliminaire du code de procédure pénale). Par ailleurs, l'article 8 de cette même Convention protège le droit à la vie privée, auquel il ne peut être porté atteinte que si l'ingérence est prévue par la loi, poursuit un but légitime, et demeure proportionnée à l'objectif visé.

La protection des données personnelles, en tant que droit fondamental autonome, est expressément consacrée par l'article 8 de la Charte des droits fondamentaux de l'Union européenne (JOUE 2000/C 364/01), l'article 16 du Traité sur le fonctionnement de l'Union européenne (TFUE), et réaffirmée par l'article 8 de la CEDH tel qu'interprété par la jurisprudence de la Cour européenne des droits de l'homme. Ainsi, les opérations d'OSINT ne peuvent être mises en œuvre que dans le strict respect des normes applicables en matière de protection des données, à savoir le Règlement (UE) 2016/679 du 27 avril 2016 (RGPD) et la loi n° 78-17 du 6 janvier 1978 modifiée, lorsqu'elles sont conduites à titre privé ; ainsi que la directive (UE) 2016/680 du 27 avril 2016 relative aux traitements à des fins répressives, combinée à la même loi nationale dans sa version applicable, lorsque ces opérations sont menées dans le cadre d'enquêtes judiciaires.

2.2.3 Absence de commission d'infraction

Les opérations d'OSINT doivent impérativement être menées dans le respect des règles de droit pénal, afin d'éviter que les techniques utilisées ne constituent elles-mêmes des infractions.

En particulier, les articles 323-1 et suivants du code pénal répriment les atteintes aux systèmes de traitement automatisé de données (STAD), en sanctionnant notamment l'accès, le maintien ou l'atteinte frauduleuse à un système ou aux données qu'il contient. La jurisprudence admet que l'infraction soit constituée même en l'absence de contournement de sécurité, dès lors que l'accès est réalisé en méconnaissance de la volonté du responsable du système (CA Paris, 11e ch. A, 5 avr. 1994, n° 93/01603).

L'exploitation de vulnérabilités, le contournement de dispositifs de sécurité, l'utilisation de techniques de forçage ou l'usage de données issues d'un accès frauduleux relèvent ainsi d'infractions pénalement sanctionnées. Il en va de même pour l'utilisation d'outils permettant d'intercepter ou d'extraire des données à partir de terminaux numériques.

Par ailleurs, l'article 223-1-1 du Code pénal incrimine la pratique du doxing, c'est-à-dire la diffusion de données personnelles permettant d'identifier ou localiser une personne, lorsqu'elle l'expose à un risque direct d'atteinte.

S'y ajoutent d'autres qualifications susceptibles d'être caractérisées : atteinte à l'intimité de la vie privée (art. 226-1 et s.), usurpation d'identité (art. 226-4-1), escroquerie (art. 313-1), faux et usage de faux (art. 441-1 et s.), recel (art. 321-1).

En matière de données à caractère personnel, l'article 226-18 du code pénal réprime tout traitement opéré de manière frauduleuse, déloyale ou illicite. À ce titre, la Cour de cassation a récemment jugé, dans un arrêt du 30 avril 2024 (Cass. crim., 30 avr. 2024, n° 23-80.962), qu'une collecte en accès libre sur Internet pouvait être qualifiée de déloyale si elle était réalisée à des fins de profilage et d'investigation dans la vie privée, à l'insu des personnes concernées.

L'extraction massive de données peut porter atteinte aux droits des producteurs de bases de données, protégés par l'article L.342-1 du code de la propriété intellectuelle.

Les agents des forces de sécurité intérieure sont également soumis à des obligations spécifiques, dont le non-respect peut engager leur responsabilité pénale : non-dénonciation de crime (art.

434-1 du code pénal), complicité (art. 121-6 et 121-7 du code pénal), violation du secret de l'enquête ou de l'instruction (art. 11, al. 3 du code de procédure pénale, en lien avec les art. 226-13 et 226-14 du code pénal).

Enfin, au-delà des poursuites pénales, les membres des forces de l'ordre sont tenus au respect des obligations déontologiques fixées par le code de déontologie de la police nationale et de la gendarmerie nationale (Décret n° 2014-1253 du 27 octobre 2014), notamment : respect de la légalité (art. R.434-5), devoir d'intégrité (art. R.434-11), devoir de loyauté et de réserve (art. R.434-12).

2.2.4 Inscription dans un cadre procédural

La présente analyse porte sur les conditions dans lesquelles des personnes extérieures aux services d'enquête – notamment des civils – peuvent être associées à la réalisation d'opérations d'OSINT dans le cadre d'une procédure pénale. Sont ainsi exclues du champ d'étude les techniques spéciales d'enquête telles que l'enquête sous pseudonyme ou la cyberinfiltration (articles 230-46 et suivants du code de procédure pénale), l'infiltration (article 706-81 du Code de procédure pénale et article 67 bis du code des douanes), ou encore les interceptions de communications électroniques ou les captations de données de connexion. Ces actes sont en effet réservés aux agents habilités et ne peuvent être confiés à des intervenants extérieurs.

La voie de la réquisition judiciaire est le moyen procédural permettant de recourir à des tiers.

La réquisition judiciaire constitue un acte contraignant émanant de l'autorité judiciaire, permettant de contraindre une personne physique ou morale à fournir des informations ou à accomplir une prestation utile à la conduite d'une procédure pénale.

Trois catégories principales de réquisitions sont prévues par le Code de procédure pénale :

- les réquisitions à professionnel, dites aussi « à manouvrier », visent l'obtention d'un concours matériel ou manuel indispensable à la réalisation de constatations ou d'investigations. Elles peuvent concerner, par exemple, l'ouverture d'une porte, le déplacement d'objets ou le développement de photographies ;
- les réquisitions à personne qualifiée, ou « à sachant », permettent de solliciter l'intervention de personnes disposant de compétences spécifiques afin d'effectuer des constatations, examens techniques ou scientifiques. La Cour de cassation a précisé que les missions confiées dans ce cadre peuvent être de même nature que celles prévues à l'article 156 pour les experts judiciaires (Cass. crim., 14 septembre 2005, n° 05-84021). La seule condition est l'existence d'une ou plusieurs questions d'ordre technique que le magistrat ne peut trancher seul. Les personnes qualifiées doivent prêter serment, sauf si elles sont inscrites sur une liste d'experts judiciaires. Leur rémunération est fixée soit forfaitairement soit par taxation ;
- Les réquisitions aux fins de remise d'informations comprennent deux sous-catégories :
    - les réquisitions générales, qui visent la remise d'informations utiles à l'enquête, quels qu'en soient la nature ou le support ;
    - Les réquisitions informatiques qui concernent l'accès à des données numériques, non couvertes par un secret protégé, auprès d'organismes publics ou privés, via la Plateforme nationale des interceptions judiciaires (PNIJ).

Ce dernier type de réquisition suppose que la personne requise détienne déjà les informations sollicitées. Or, dans le cadre de l'OSINT, les données doivent être activement recherchées, collectées et analysées. La réquisition aux fins de remise d'informations ne paraît donc pas adaptée à la mobilisation d'un tiers chargé de réaliser des opérations d'OSINT.

À l'inverse, le recours à un intervenant extérieur spécialisé dans l'investigation numérique en sources ouvertes pourrait être envisagé dans le cadre :

- des réquisitions à professionnel, si la tâche requise est manuelle ou matérielle et ne présente pas de complexité technique ;
- ou des réquisitions à personne qualifiée, si l'opération nécessite une expertise particulière pour effectuer des constatations ou analyses.

Se pose ainsi la question de savoir si les actes réalisés par un tiers spécialisé en OSINT peuvent être assimilés à ceux pouvant être confiés à un expert judiciaire au sens des articles 77-1 et 156 du Code de procédure pénale. L'absence de qualification juridique explicite de ces intervenants crée une incertitude quant au fondement procédural applicable, ce qui tend à limiter leur recours dans les enquêtes.

Dans ce contexte, on peut constater que les compétences et ressources mobilisées en matière d'OSINT présentent des caractéristiques proches de celles exigées des personnes qualifiées ou des experts judiciaires. Van Puyvelde et Tabárez Rienzi (2025) soulignent que l'OSINT repose sur une technicité qui n'est ni aisément accessible ni universellement maîtrisée[3], ce qui renforce la spécificité de ces savoir-faire. Ce constat peut être regardé, à ce stade, comme allant dans le sens d'une reconnaissance possible de cette expertise dans les pratiques judiciaires.

3 Solution

Au regard de l'impact opérationnel croissant des résultats obtenus par le recours à l'OSINT, il apparaît indispensable de permettre aux services enquêteurs de s'appuyer, de manière encadrée, sur des compétences extérieures spécialisées. La conduite d'investigations en sources ouvertes requiert en effet des savoir-faire techniques, que les enquêteurs ne maîtrisent pas toujours pleinement.

Permettre à des collaborateurs civils d'y contribuer constituerait une avancée pragmatique. Avancée qui s'inscrirait dans le sens de ce qu'exposait le commissaire divisionnaire Paul Bousquet lors de son intervention en 2025 au DU Cybercriminalités : enjeux et défis humains, « les enquêtes les plus réussies sont souvent celles qui sont réalisées en collaboration avec le privé ».

Afin de lever les résistances identifiées, plusieurs pistes d'amélioration peuvent être proposées :

- la création d'un cadre opérationnel ;
- la clarification du rapport aux sources employées dans le cadre des opérations d'OSINT;

[3] "Extensive subject knowledge is crucial for understanding and prioritising information on complex security developments. […] OSINT demands skills and resources that are not easily acquired or universally available. The rise of OSINT is not 'democratising intelligence'."

- l'encadrement du recours à l'intelligence artificielle.

3.1 La création d'un cadre opérationnel

En matière pénale, les modalités d'obtention de la preuve par les forces de l'ordre font l'objet d'un encadrement légal strict et d'un contrôle régulier tout au long de la procédure. À l'inverse, les opérations d'OSINT reposent sur l'exploitation de sources en ligne accessibles à tous, issues d'un environnement décentralisé. Cette architecture propre à Internet rend particulièrement complexe l'identification fiable du chemin d'accès ayant conduit à une information donnée, dès lors que la même donnée peut être obtenue par des moyens licites ou illicites.

Dans ce contexte, il est particulièrement difficile de vérifier a posteriori la licéité des moyens utilisés pour accéder à une information. L'ambiguïté des chemins d'accès rend possible un risque : celui de présenter une information comme issue d'une source licite, alors qu'elle aurait été obtenue à l'origine par un procédé illicite, dans le but d'en sécuriser la recevabilité procédurale. Ce décalage entre la réalité de l'accès et sa présentation déclarative interroge la loyauté de la preuve, l'intégrité des procès-verbaux, et plus largement, la sincérité du procès.

Cette problématique n'est pas inédite. Aux origines de la police moderne la loyauté des pratiques d'enquête était déjà questionnée.

Vidocq, ancien bagnard devenu chef de la brigade de sûreté, avait lui-même institué une mesure symbolique pour désamorcer les accusations portées contre ses agents, qui étaient suspectés de vol par d'autres services de police : il leur imposait le port de gants en daim afin de prévenir toute mise en cause en lien avec des vols commis dans la foule. Ce geste visait à « paralyser le membre qui peut être l'instrument du péché » et à couper court aux soupçons (Vidocq, *Mémoires*, livre 3, chap. X, p. 21-22).

Or, à la différence des gants de daim de Vidocq, les opérations OSINT ne peuvent s'appuyer sur un artefact aussi visible. Elles reposent sur des pratiques numériques, discrètes par nature. Mais ce caractère numérique offre en contrepartie une opportunité précieuse : l'horodatabilité des actions.

À défaut d'un signe visible, ce sont donc les métadonnées, les traces numériques, et la documentation structurée des actes d'enquête qui peuvent servir à établir la licéité de la démarche. Cette traçabilité constitue la condition première pour apprécier le respect du principe de loyauté et garantir la recevabilité de la preuve.

Ainsi, pour que les résultats d'une opération d'OSINT puissent valablement nourrir l'intime conviction du juge, il est indispensable de disposer d'un enregistrement précis, daté et inaltéré du cheminement suivi, de la réalisation de l'acte d'enquête jusqu'à la preuve obtenue. Ce cheminement doit répondre à des standards documentaires élevés, reposant notamment sur la chronologie, la conservation et l'authenticité.

Des méthodes et protocoles techniques existent pour assurer cette traçabilité, mais leur efficacité repose sur un impératif fondamental : la supervision par un OPJ. Si l'OPJ n'a pas nécessairement à réaliser lui-même les actions techniques, il doit en comprendre la logique, en maîtriser les étapes, et avoir la capacité d'en garantir la régularité.

En effet, dans un environnement où l'accès à des sources illégales peut être techniquement simple et peu traçable, seule une supervision rigoureuse permet d'éviter les dérives – notamment le contournement des règles d'obtention ou l'usage de techniques de « blanchiment » de la preuve.

La traçabilité stricte des opérations d'OSINT devient ainsi une condition essentielle de la valeur probatoire des éléments collectés. Comme le rappelle Ghernaouti (2024, p. 206), toute chaîne de conservation doit pouvoir répondre à des questions fondamentales : qui a recueilli la preuve ? comment et où a-t-elle été collectée ? comment a-t-elle été stockée, protégée, analysée ? par qui a-t-elle été manipulée ? dans quelles conditions a-t-elle été transmise ? Ce sont ces réponses qui fondent l'intégrité probatoire.

Or, comme le souligne Sottas (2022, p. 9), les juridictions pénales, y compris internationales, ne disposent pas encore de principes contraignants clairs spécifiquement dédiés aux preuves numériques collectées en sources ouvertes. En l'absence d'un référentiel légal stabilisé, l'établissement de règles procédurales rigoureuses – internes à la chaîne pénale – apparaît comme une exigence incontournable pour garantir la validité de ces preuves dans un cadre judiciaire.

3.1.1 Respect d'une norme technique

La mise en œuvre d'une norme technique constitue un préalable indispensable à la recevabilité d'un élément de preuve OSINT, dans la mesure où elle permet d'en garantir la traçabilité, l'intégrité et l'authenticité à chaque étape de sa collecte et de sa conservation.

Letoqueux et Aumaître (2022, p. 61) rappellent en ce sens que que « la production de l'élément de preuve doit être distinguée de son admission en tant que preuve ».

Face à ces enjeux, plusieurs référentiels techniques peuvent être mobilisés pour structurer la démarche probatoire dans le domaine de l'OSINT. Deux normes présentent un intérêt particulier :

- la norme AFNOR NF Z67-147, adoptée le 11 septembre 2010, fixe un « mode opératoire de procès-verbal de constat sur Internet effectué par un commissaire de justice ». Bien que conçue initialement pour des officiers ministériels, cette norme offre un cadre utile pour documenter et tracer rigoureusement les actions réalisées sur Internet ;
- la norme ISO 9001, relative au management de la qualité, peut être transposée à la gestion des procédures OSINT. Elle permet d'assurer une cohérence méthodologique dans les opérations réalisées, en structurant les démarches, en formalisant les étapes, et en garantissant un haut niveau de traçabilité et de contrôle.

Dans une optique de sécurisation procédurale, l'intégration de telles normes dans le travail des tiers spécialisés en OSINT pourraient permettre d'établir une chaîne de confiance entre la collecte de la donnée et son usage judiciaire et de réduire le niveau de résistance au changement existant.

3.1.2 Respect d'une norme déontologique

Au-delà de la conformité technique, l'exploitation de sources ouvertes dans un cadre judiciaire ou quasi-judiciaire suppose le respect de principes éthiques rigoureux. Comme le souligne le rapport The Gray Spectrum (Stanley Center, 2019), les analystes mobilisant des données géospatiales ou OSINT sont régulièrement confrontés à des dilemmes éthiques liés à la production, la publication ou l'exploitation d'informations sensibles. Ces activités s'inscrivent dans une « zone grise », où les effets indirects – sur la vie privée, la sécurité d'opérations ou des dynamiques sociales – peuvent s'avérer préjudiciables.

Ce constat plaide pour une formalisation des pratiques : codes de conduite clairs, formation déontologique des professionnels, mécanismes de relecture par les pairs. Le Markkula Center for Applied Ethics propose à cet égard un cadre d'analyse éthique structuré autour de cinq axes : utilité, justice, respect des droits, vertu et bien commun. Le Code of Ethics de la Society of Professional Journalists met, quant à lui, l'accent sur la rigueur, la prudence et l'intégrité dans le traitement de l'information.

Hanham et Shin (2020) insistent sur le besoin de règles spécifiques à l'analyse OSINT, incluant notamment des processus de relecture par les pairs, garants de la robustesse méthodologique et éthique des investigations.

Les efforts d'encadrement ne relèvent pas uniquement des institutions publiques. Van Puyvelde et Tabárez Rienzi (2025) rappellent que la communauté OSINT elle-même a vocation à se réguler. À titre d'exemple, l'OSINT Foundation a élaboré un code de conduite traitant notamment de pratiques controversées. De même, Loehrke et al. (2019) relèvent qu'un tel code peut contribuer à la responsabilisation des praticiens, tout en les protégeant contre des pressions extérieures ou injonctions déviantes.

Dans une perspective internationale, le Berkeley Protocol on Digital Open Source Investigations, publié en 2020 par le Human Rights Center de l'Université de Californie à Berkeley en partenariat avec le Haut-Commissariat des Nations unies aux droits de l'homme, constitue une tentative structurée d'encadrement déontologique et procédural des enquêtes OSINT.

Décrit par Sottas (2022, p. 6) comme « la première ligne directrice mondiale pour l'utilisation d'informations en ligne publiquement disponibles », ce protocole identifie six étapes fondamentales dans le cycle d'une enquête numérique ouverte : (1) la recherche en ligne, (2) l'évaluation préliminaire, (3) la collecte, (4) la conservation, (5) la vérification, et (6) l'analyse. Ces phases doivent être systématiquement documentées, notamment pour assurer la traçabilité des opérations, la transparence méthodologique et la collaboration interdisciplinaire.

Le protocole distingue aussi clairement les pratiques licites – comme la consultation de contenus publics sous identité virtuelle – de celles qui, telles que l'interaction sous fausse qualité ou l'accès à des espaces protégés, contreviennent aux standards éthiques et juridiques.

Enfin, dans les procédures judiciaires internationales, le protocole recommande un triple test d'admissibilité de la preuve fondé sur sa pertinence, sa valeur probante et l'absence d'effet disproportionné sur l'équité du procès. Pour les enquêtes non judiciaires, une grille d'évaluation similaire – fondée sur la fiabilité, la pertinence et la valeur informative – est également préconisée.

3.1.3 Reconnaissance de l'expertise

Le recours à des professionnels de l'OSINT dans un cadre judiciaire pose la question de la reconnaissance institutionnelle de leur compétence. En France, le statut d'expert judiciaire est encadré par le décret n° 2004-1463 du 23 décembre 2004, dont l'article 1er renvoie à une

nomenclature des spécialités d'expertise fixée par l'arrêté du 10 juin 2005. Cette nomenclature, établie par arrêté du garde des Sceaux, est organisée en branches générales (de A à H), subdivisées en rubriques et spécialités, et vise à répondre aux besoins des juridictions.

À ce jour, aucune spécialité ne correspond spécifiquement aux activités liées à l'OSINT. Toutefois, deux rubriques pourraient s'en approcher fonctionnellement :

- E-01 : Électronique et informatique ;
- G-13 : Supports numériques.

Dans ce contexte, la création d'une spécialité autonome dédiée aux opérations d'OSINT pourrait présenter un double intérêt. D'une part, elle permettrait aux juridictions de désigner, en toute sécurité juridique, des professionnels dont l'expertise serait spécifiquement adaptée aux enjeux techniques et déontologiques liés aux sources ouvertes. D'autre part, elle contribuerait encadrer ce recours par les garanties attachées au statut d'expert judiciaire (serment, obligation d'impartialité, contrôle de compétence).

Une telle reconnaissance offrirait également un levier pour encadrer l'intervention des tiers spécialisés en OSINT dans le cadre de réquisitions ou d'analyses techniques confiées par l'autorité judiciaire, en assurant que leurs contributions respectent les exigences de traçabilité, de loyauté et de fiabilité probatoire attendues en procédure pénale.

3.2 Nécessité de clarifier le rapport aux sources employées

L'exploitation de données issues de fuites peut, dans certains cas, constituer une ressource précieuse pour l'identification d'acteurs, de réseaux ou d'éléments techniques dans le cadre d'enquêtes numériques. Toutefois, leur emploi soulève des enjeux juridiques majeurs.

En effet, conformément au principe de liberté de la preuve, alors que les données accessibles en ligne, y compris lorsqu'elles proviennent de fuites ou de piratages, peuvent être mobilisées par des tiers, leur usage par les enquêteurs est susceptible de contrevenir au principe de loyauté.

Dès 1996, le Comité permanent de contrôle des services de renseignement soulignait déjà la complexité de la qualification des sources issues de fuites : « l'information qui, à l'origine, n'est pas obtenue légalement, mais qui est devenue publique par la suite, peut également être considérée comme source ouverte » (Rapport annuel, 1996, p. 198). Cette ambiguïté persiste, en particulier en l'absence de consensus normatif sur ce qui constitue, en pratique, une « source ouverte licite ».

Le recours à des bases issues de fuites soulève donc une série de questions juridiques, notamment au regard des infractions suivantes :

- Article 323-3 du code pénal, qui réprime l'extraction, la détention, la reproduction ou la transmission frauduleuse de données issues d'un système de traitement automatisé, même sans accès frauduleux préalable ;
- Article 321-1 du code pénal, relatif au recel, applicable à la détention ou à l'usage de données obtenues illégalement, en connaissance de leur origine délictueuse ;
- Article 226-18 du code pénal, qui sanctionne le traitement de données personnelles effectué de manière déloyale ou illicite.

Ce dernier fondement a été mobilisé par la Cour de cassation dans un arrêt du 30 avril 2024 (Cass. crim., 30 avril 2024, n° 23-80.962), pour confirmer la condamnation d'un enquêteur privé ayant procédé à une collecte de données à des fins de profilage sans en informer les personnes concernées. La Cour a estimé que l'accessibilité libre des données en ligne ne suffisait pas à neutraliser l'exigence de loyauté imposée par la législation.

D'un point de vue procédural, la jurisprudence française admet que des données issues de fuites peuvent être recevables comme preuve dès lors que les autorités publiques ne sont pas à l'origine de leur obtention et que les garanties procédurales sont respectées (Cass. crim., 11 mai 2006, n° 05-84.837 ; Cass. crim., 27 nov. 2013, n° 13-85.042). Dans ce dernier arrêt, la Cour a admis la recevabilité de fichiers informatiques volés à l'administration, dans la mesure où l'autorité publique ne les avait ni sollicités ni extraits elle-même, mais en avait pris connaissance dans le cadre d'une perquisition régulière.

Par analogie, une utilisation judiciaire de données issues de fuites de données publiquement accessibles sur Internet peut être envisagée, à condition que l'autorité publique n'ait pas participé activement à leur collecte illégitime (v. Cass. ass. plén., 10 nov. 2017, n° 17-82.028 ; Cass. crim., 20 sept. 2016, n° 16-80.820).

Cette approche a été confirmée plus récemment dans une décision du 12 mars 2025 (Cass. crim., 12 mars 2025, n° 23-80.407), qui valide l'usage de données personnelles collectées par un logiciel étranger (CPS), dès lors que leur exploitation respecte les règles encadrant les enquêtes pénales et les normes en matière de protection des données (directive (UE) 2016/680, loi n° 78-17 du 6 janvier 1978, Code de procédure pénale).

En l'absence de cadre juridique spécifique à l'OSINT, ces décisions participent à dessiner des lignes directrices implicites. Toutefois, cette zone grise demeure problématique. Séjean (2023) appelle à un encadrement normatif explicite, soulignant que ni les logiques contractuelles, ni la seule utilité opérationnelle ne suffisent à fonder la licéité des pratiques. Dans cette perspective, une consultation parlementaire a été lancée en 2024 à l'initiative du député Philippe Latombe, en vue d'un éventuel texte législatif sur l'encadrement de l'exploitation de données issues d'infractions.

Se pose enfin la question des plateformes supports de ces fuites. Certaines de ces plateformes se sont développées autour de l'indexation et de la mise à disposition de données compromises. Comme l'explique Lecur (2025), elles permettent la recherche d'informations personnelles (adresses électroniques, identifiants, mots de passe, numéros de téléphone, etc.) extraites de bases exposées à la suite d'intrusions, de négligences ou de mises en ligne illégales. Ces outils, bien que divers dans leur implantation géographique ou leur modèle économique, partagent une finalité commune : faciliter l'exploitation de fuites à des fins de renseignement. Lecur (2025) mentionne notamment :

- IntelX (Autriche), plateforme payante à fonctions avancées, incluant l'indexation du dark web ;
- Snusbase (États-Unis), spécialisée dans l'indexation rapide de bases compromises ;
- DeHashed (États-Unis), orientée vers les requêtes sur des sélecteurs techniques ;
- Leak-Lookup (Royaume-Uni), proposant une version gratuite avec options étendues sous abonnement ;

- Owlint (France), revendiquant une conformité légale dans l'analyse des données exposées ;

ainsi que plusieurs bots Telegram (principalement hébergés en Russie), permettant des recherches automatisées à bas coût, dans un environnement juridiquement incertain.

3.3 L'encadrement du recours à l'intelligence artificielle dans l'OSINT

L'intégration de l'intelligence artificielle (IA) dans les pratiques d'enquête a franchi un seuil normatif en France avec l'introduction, par la loi du 13 juin 2025, d'une disposition spécifique au sein du code de procédure pénale (art. 260-46), consacrant pour la première fois l'usage de l'IA comme moyen d'investigation encadré.

Dans le champ de l'OSINT, le recours à l'IA s'inscrit dans une dynamique visant à optimiser l'exploitation de volumes massifs de données numériques. Van Puyvelde et Tabárez Rienzi (2025) rappellent que le développement de logiciels d'analyse automatique constitue l'une des réponses les plus prometteuses à la surcharge informationnelle rencontrée par les analystes. L'IA permet en effet de faciliter certaines tâches comme la détection d'anomalies, le tri d'informations ou l'identification de patterns à partir de données ouvertes, notamment sur les réseaux sociaux, les bases de données publiques ou le dark web.

Néanmoins, cette automatisation ne saurait être assimilée à une substitution complète de l'humain. Comme le souligne Fressin (2021, p. 77), aucune analyse totalement automatisée ne peut actuellement — ni probablement à l'avenir — se substituer à l'expertise humaine, que ce soit pour le traitement, la contextualisation ou l'interprétation de données issues de sources ouvertes. L'intervention humaine demeure indispensable pour donner sens aux corrélations, évaluer la fiabilité contextuelle des sources, et articuler les résultats dans une logique d'enquête ou d'instruction.

Dès lors, la légitimité de l'usage de l'IA dans un cadre judiciaire repose sur deux conditions fondamentales :

- la maîtrise technique de l'outil par l'opérateur, capable d'en comprendre le fonctionnement, les biais potentiels et les limites d'application ;
- la capacité à justifier et expliciter devant le juge les méthodes utilisées, les paramètres retenus, et la validité des résultats produits.

Sur le plan normatif, l'IA mobilisée dans les opérations d'OSINT devra également satisfaire aux exigences du règlement européen sur l'intelligence artificielle (AI Act), qui distingue les systèmes à usage interdit, les usages autorisés sous conditions, et les systèmes à haut risque. Les technologies employées à des fins judiciaires sont, en principe, classées dans cette dernière catégorie. Elles sont donc soumises à des obligations strictes de documentation, de transparence, de traçabilité et de contrôle humain.

Dans ce contexte, le développement des pratiques d'OSINT assistées par IA impose une montée en compétence continue des praticiens, qu'ils soient agents publics ou experts tiers. Il ne s'agit pas seulement de maîtriser des outils, mais aussi d'adopter une démarche critique sur les résultats générés par les algorithmes, afin de garantir la fiabilité, la loyauté et la recevabilité des éléments collectés.

L’IA constitue ainsi un levier puissant pour améliorer l’efficacité des investigations en sources ouvertes, mais son déploiement dans un cadre pénal exige un encadrement strict, fondé sur des compétences techniques, une capacité de justification procédurale, et une vigilance constante face aux risques de dérive algorithmique.

Conclusion

La résistance au changement générée par le recours à des tiers spécialisés en OSINT n'est pas le signe d'un conservatisme ou d'un rejet du progrès, mais la manifestation d'un besoin légitime : celui de rattacher tout acte d'enquête à un cadre procédural clair, garant, in fine, d'un procès équitable.

C'est précisément la perception actuelle de l'absence de cadre formalisé qui alimente une résistance au changement, d'autant plus forte que les opérations d'OSINT bousculent les frontières classiques entre enquête pénale diligentée par les membres des forces de l'ordre et, savoir technique privé.

La réponse à cette défiance n'est donc pas seulement normative, elle est aussi épistémique. Seule une connaissance fine des enjeux techniques, juridiques et éthiques de l'OSINT permettra de lever les incertitudes, de sécuriser les pratiques, et de restaurer la confiance entre les acteurs.

Plusieurs pistes peuvent être dégagées. Il est impératif que les membres de la chaîne pénale soient formés, de manière approfondie, aux spécificités du numérique, tant pour garantir l'efficacité des opérations que pour assurer la protection des droits fondamentaux. Si la collaboration avec des acteurs privés s'avère précieuse, notamment pour pallier certaines lacunes de compétences internes, elle ne peut être envisagée sans un effort structurel de maintien, voire de renforcement, des savoir-faire au sein des institutions publiques.

Comme le suggère Schwartz (2021, p. 39), la coopération entre différentes sphères – ici, le public, le privé, et même les citoyens – peut favoriser une dynamique de confiance, à condition que chacun reste à sa place et que les règles du jeu soient clairement établies :

- « La confiance peut être retrouvée : elle se construit sur les fondations mêmes de cette collaboration qui reconnaît à chacun sa valeur. »

Pour autant, même à supposer qu'un encadrement juridique abouti soit mis en place, deux zones de friction subsisteront probablement, nourrissant une résistance latente : celle des sources et celle de l'intelligence artificielle.

Sur le premier point, Bertran (2022) alerte sur les risques d'instrumentalisation politique, géopolitique ou économique des sources disponibles en ligne, notamment lorsque celles-ci proviennent de fuites ou d'actions offensives. La manipulation ou l'intentionnalité dissimulée des données peut affecter la fiabilité des éléments produits, et donc leur recevabilité.

Sur le second, Lecur (2025) attire l'attention sur la dépendance des acteurs français à des plateformes OSINT étrangères, majoritairement américaines. Il évoque ainsi un enjeu de souveraineté numérique, encore peu maîtrisé, alors même que certains outils sont devenus incontournables dans les pratiques d'enquête ou de veille. Malgré l'émergence de projets européens portés notamment par l'ENISA, tels que Trustee ou AI-driven Data Operations, la maturité de ces initiatives reste encore insuffisante pour répondre à l'urgence opérationnelle.

Enfin, s'agissant de l'intelligence artificielle, l'enjeu est aussi celui de la maîtrise intellectuelle et technique. Pour que les outils d'IA déployés dans l'OSINT puissent être admis comme supports probatoires, encore faut-il que leurs logiques de fonctionnement soient comprises par leurs utilisateurs. À défaut, comme le rappelait Lawrence Lessig, « code is law » : ce qui n'est pas compris dans le code devient incontrôlé dans le droit. Sans une telle maîtrise, aucune conviction judiciaire fondée sur l'analyse automatisée ne saurait être valablement formée.

Bibliographie

Audibert, M. (2025). La preuve numérique au cœur des enquêtes judiciaires : quels enjeux et quelles perspectives en procédure pénale ? Les notes du Centre de Recherche de la Gendarmerie Nationale, (114). https://hal.science/hal-05023029v1

Bellingcat. (s.d.). MH17: The Open Source Evidence. Bellingcat. https://www.bellingcat.com/resources/2020/10/08/mh17-the-open-source-evidence/

Berkeley Human Rights Center. (2020). Berkeley Protocol on Digital Open Source Investigations: A Methodological Framework for Human Rights Fact-Finding. United Nations Human Rights Office & UC Berkeley. https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source

Bertran, M.-G. (2022). Illustration des apports et limites de l'usage des sources ouvertes à travers le cas de la Russie. Hérodote, 186(3), 85–98. https://doi.org/10.3917/her.186.0085

Chopin, O., & Oudet, B. (2023). Sources ouvertes, cyber, data : le renseignement et la révolution de l'information. In Renseignement et sécurité (3e éd., pp. 187–214). Dunod.

Comité permanent de contrôle des services de renseignement. (1996). Rapport d'activités 1996. Bruxelles : Parlement belge.

Cyril, L. (2025). OSINT et procédure pénale : vers une collaboration possible entre civils et enquêteurs ?

Diaz, F., & Desbiens, D. (2011). Résistance au changement de l'institution policière et criminalité évolutive : un paradoxe. Champ pénal/Penal field, 8. https://doi.org/10.4000/champpenal.7982

Ghernaouti, S. (2024). Criminalistique informatique et investigation numérique. In Cybercriminalité (pp. 198–222). Vuibert.

Hanham, M., & Shin, J. (2020). Ethics in the Age of OSINT Innocence. Courier, Summer 2020. Stanley Center for Peace and Security. https://stanleycenter.org/publications/ethics-in-the-age-of-osint-innocence/

Jouette, P. (2024). Quelle politique pénale pour le procureur près la Cour pénale internationale ? Revue de science criminelle et de droit pénal comparé, 2024(2), 263–277.

Lecur, G. (2025). OSINT et souveraineté nationale.

Letoqueux, H., & Aumaître, A. (2022). La contribution de l'OSINT aux enquêtes portant sur des crimes internationaux. Hérodote, 186(3), 57–68. https://www.cairn.info/revue-herodote-2022-3-page-57.htm

Limonier, K., & Audinet, M. (2022). De l'enquête au terrain numérique : les apports de l'OSINT à l'étude des phénomènes géopolitiques. Hérodote, 186(3), 5–17. https://www.cairn.info/revue-herodote-2022-3-page-5.htm

Loehrke, B., Rockwood, L., Hanham, M., & Kenausis, L. (2019). The Gray Spectrum: Ethical Decision Making with Geospatial and Open Source Analysis. Stanley Center for Peace and Security. https://stanleycenter.org/publications/the-gray-spectrum/

Pesqueux, Y. (2020). La résistance au changement. HAL-SHS. https://halshs.archives-ouvertes.fr/halshs-02876103

Renault, C., Charon, P., & Laurençon, F. (2022). Renseigner autrement ? Trajectoires de l'OSINT dans les services de renseignement. Hérodote, (186), 19–30. https://www.cairn.info/revue-herodote-2022-3-page-19.htm

Roumanos, R., & Le Deuff, O. (2021). L'enquête OSINT : Des traces ouvertes au récit journalistique fermé. Revue Intelligibilité du Numérique, (2). https://intelligibilite-numérique.openedition.org/178

Schwartz, A. (2021). Journalistes et citoyens, main dans la main ? L'exemple du Capitol Hill Project, fondé sur les méthodes de l'Open Source Intelligence. I2D - Information, données & documents, 57(1), 36–39. https://doi.org/10.3917/i2d.211.0036

Sottas, P. (2022). Enquêter en ligne : La justice internationale face aux défis des preuves numériques en sources ouvertes. Éclairage du GRIP, 8 septembre 2022. https://hal.science/hal-03822203

Thierry, G. (2022, 4 juillet). Comment la justice travaille avec les recherches en sources ouvertes. Dalloz actualité. https://www.dalloz-actualite.fr

Van Puyvelde, D., & Tabárez Rienzi, F. (2025). The rise of open-source intelligence. European Journal of International Security, à paraître. https://doi.org/10.1017/eis.2024.61

Vidocq, E.-F. (1828–1829). Mémoires (Livre 3, Chapitre X, p. 22).