Georges LECUR

OSINT &
SOUVERAINETE NATIONALE

Université BORDEAUX MONTAIGNE | Cyber criminalités

Promotion 2024-2025

Résumé

Alors que la souveraineté numérique devient un enjeu majeur pour les États dans un contexte géopolitique plus que tendu, la montée en puissance des plateformes OSINT étrangères pose de nouveaux défis à la France en matière de sécurité, de législation et d'autonomie stratégique.

Cette étude a été menée dans le but d'analyser l'impact que peut avoir l'utilisation massive d'outils OSINT non-français sur la souveraineté nationale, en s'appuyant sur un cadre juridique, technique et sociopolitique.

Nous tenterons de répondre à ces questions à travers des analyses comparatives, une revue de la législation en vigueur, une étude de cas concrets ainsi qu'une recherche sur les usages réels dans le cadre institutionnel et privé.

Les résultats de ce sujet d'étude ont pu démontrer que même si des solutions françaises émergent, la dépendance aux plateformes étrangères expose la France à une perte de contrôle sur ses données sensibles, à des risques juridiques accrus et à une influence stratégique défavorable.

Introduction

L'OSINT (Open Source Intelligence), ou ROSO en français (renseignement d'origine source ouverte), englobe différentes techniques de recherche dans le domaine public et accessible publiquement, déployées dans le cadre de la surveillance, de la recherche, de la collecte d'informations et des enjeux géopolitiques.
L'usage croissant des outils OSINT soulève des questions cruciales quant à la souveraineté numérique et à la protection des données sensibles. Le recours aux plateformes OSINT, qui permettent de collecter, analyser et exploiter des informations issues de sources publiques, s'est largement démocratisé au cours de ces dernières années. Que ce soit pour la sécurité nationale, la défense ou même dans des secteurs privés tels que la veille concurrentielle, ou les médias, les sources ouvertes deviennet une technique de recherche incontournable.
Toutefois, ce développement rapide n'est pas sans poser des défis significatifs. L'un des plus importants concerne la dépendance croissante de la France à l'égard de plateformes de recherche étrangères, principalement américaines, ce qui pourrait mettre en péril la souveraineté nationale du pays.

L'OSINT repose sur l'exploitation d'une grande variété d'informations disponibles en sources ouvertes et accessibles publiquement à tous, telles que les réseaux sociaux, les bases de données publiques, les images satellites ou encore différents types de publications en ligne. Ces informations, bien qu'accessibles légalement, peuvent être sensibles, en particulier lorsqu'elles concernent des données personnelles ou stratégiques.
Ce phénomène, amplifié par la globalisation numérique, entraîne une prolifération de plateformes OSINT basées en dehors de l'Union européenne.
Dans ce contexte, les autorités françaises se trouvent confrontées à des défis inédits, notamment la gestion du respect des législations nationales en matière de protection des données personnelles, et la question de la dépendance vis-à-vis des outils et services principalement américains.

Plusieurs problématiques découlent de ces usages :
- Pourquoi cette dépendance envers des outils extérieurs à la France s'est-elle installée ? Les régulations françaises, notamment les textes de lois, le Règlement Général sur la Protection des Données (RGPD) et la Commission Nationale de l'Informatique et des Libertés (CNIL), interagissent-elles avec les pratiques d'OSINT ?
- En quoi cette dépendance à des outils non français menace-t-elle la souveraineté numérique du pays ? Ce phénomène a des répercussions sur plusieurs aspects de la sécurité nationale, notamment en ce qui concerne la protection des données sensibles et la capacité de la France à contrôler l'exploitation de ces informations.

Les hypothèses de cet article pour répondre à ces questions se centreront sur :
- La législation française, notamment en matière de protection des données personnelles (texte de lois, RGPD, CNIL), limite l'utilisation de l'OSINT, ce qui pourrait nuire à la compétitivité des services

de renseignement et des entreprises françaises, notamment dans un contexte international où les régulations sont moins strictes, comme aux États-Unis ou au Royaume-Uni.
- La dépendance croissante de la France à des plateformes OSINT non-françaises constitue un risque pour la souveraineté nationale, particulièrement en ce qui concerne la gestion et l'analyse des données sensibles. En effet, ces outils, souvent dominés par des entreprises américaines, exposent la France à des risques liés à la collecte, à l'exploitation et à la gestion de données stratégiques par des acteurs extérieurs (notamment le stockage), sans possibilité de contrôle ou de régulation locale.

Cet article sera organisé en trois parties.
Dans un premier temps, une revue de la littérature permettra d'explorer les concepts fondamentaux de l'OSINT, de la souveraineté numérique et des régulations françaises en matière de données. Cette partie mettra en lumière ce qu'est l'OSINT et ses différents champs d'application.
Ensuite, une méthodologie de recherche sera présentée, décrivant les principales plateformes OSINT utilisées à l'échelle mondiale, et plus particulièrement en France. Cette approche comprendra une analyse qualitative et comparative des pratiques en France et dans d'autres pays.
Enfin, une analyse des résultats permettra de confronter les hypothèses aux données collectées et de proposer des pistes d'amélioration dans le cadre de sa souveraineté numérique.
Ce travail vise à apporter une réflexion approfondie sur l'impact des plateformes OSINT non-françaises et des régulations nationales sur la souveraineté numérique de la France, et à envisager des solutions pour renforcer cette souveraineté face à des enjeux géopolitiques et technologiques croissants.

1 – Généralité de la souveraineté numérique à travers l'OSINT

En introduction, il est essentiel de comprendre que la souveraineté numérique ne se résume pas à une simple question de technologie ou d'accès aux données. Elle renvoie à une capacité stratégique, à une maîtrise des infrastructures, des données, des normes et des usages du numérique.
Plusieurs définitions et approches de la souveraineté numérique ont été formulées à travers différents articles, par des institutions et penseurs français, selon les angles juridiques, sociopolitiques ou technologiques.
Étudions quelques-unes de ces définitions :

- Pauline Türk (2020)[1] définit la souveraineté numérique comme la capacité pour un État de faire prévaloir ses normes, ses intérêts et sa sécurité sur les infrastructures et les flux numériques relevant de sa juridiction.
- François Pellegrini (2021)[2] se positionne autour de l'importance du logiciel libre pour garantir une indépendance technologique, condition immuable pour une véritable souveraineté numérique. Pour lui, "celui qui maîtrise le code, maîtrise la norme et le pouvoir d'agir".
- Julien Nocetti (2023)[3] propose une lecture géopolitique : la souveraineté numérique est "un instrument politique" permettant aux États de sécuriser leurs données stratégiques et de résister à la domination technologique des GAFAM ou des États concurrents.
- Pierre Bellanger (2011)[4], fondateur de Skyrock, il est le premier à introduire cette notion en France, affirmant que la souveraineté numérique est la condition de la souveraineté nationale, et insistant sur la nécessité de maîtriser les réseaux, les données et les plateformes comme biens stratégiques.

Plusieurs éléments communs émergent ; toutes les définitions s'accordent sur l'idée que la souveraineté numérique vise à assurer une autonomie de décision, de contrôle et de sécurité face à la dépendance croissante à l'égard d'acteurs numériques étrangers (notamment les GAFAM).
Elle encourage dans la capacité à héberger, traiter, protéger et gouverner les données et les systèmes de manière autonome vis à vis des géants de la tech étrangers.

---

1 Pauline Türk (2020) - *La souveraineté numérique européenne, vers une troisième voie ?* - https://shs.cairn.info/publications-de-pauline-turk--42254?lang=fr

2 François Pellegrini (2021) - *Open source, pour un numérique souverain ?* - https://www.librealire.org/open-source-pour-un-numerique-souverain

3 Julien Nocetti (2023) - *La souveraineté numérique : dix ans de débats, et après ?* - https://stm.cairn.info/revue-enjeux-numeriques-2023-3?lang=fr

4 Pierre Bellanger (2011) - *La souveraineté numérique* - *https://www.institutdiderot.fr/wp-content/uploads/2019/12/Diner-La-Souverainete%CC%81-nume%CC%81rique-Page.pdf*

On peut donc définir la souveraineté numérique comme la capacité pour un État à contrôler ses propres infrastructures, ses données et les règles qui s'y appliquent, sans dépendre de juridictions étrangères ou d'acteurs extérieurs .

Cette souveraineté s'applique à différents domaines :

- Les infrastructures (centres de données, réseaux, systèmes de communication)
- Les données (hébergement, chiffrement, localisation des *data-centers*)
- Les logiciels (plateformes, code)
- La législation
- Les capacités humaines (compétences, éducation, recherche).

Nous nous intéresserons à la souveraineté numérique à travers le prisme de l'OSINT.
Avant de définir qu'est ce que l'OSINT, il est important de distinguer l'information ouverte (OSINF) du renseignement en sources ouvertes (OSINT). L'OSINF désigne simplement des données accessibles au public, tandis que l'OSINT implique une analyse approfondie de ces données pour produire des renseignements pertinents. Cette distinction est essentielle pour comprendre le processus de transformation de l'information brute en renseignement stratégique.

Maintenant, étudions différentes définitions données à l'OSINT :

- U.S. Department of Defense (2010) : R*elevant information derived from the systematic collection, processing, and analysis of publicly available information in response to known or anticipated intelligence requirements*[5].
- NATO : Open Source Intelligence (OSINT) : *OSINT is information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience, generally the commander and their immediate staff, in order to address a specific question. OSINT, in other words, applies the proven process of intelligence to the broad diversity of open sources of information, and creates intelligence*[6].
- ComCyberGend (2024) : Méthode qui permet de collecter des informations accessibles à tous sur le web, dans le respect du cadre légal[7].
- CNIL (2024) : Le Renseignement d'Origine Source Ouverte (ROSO), aussi appelé OSINT en anglais (Open Source INTelligence), consiste à identifier des individus ou des entités, en utilisant des informations publiquement disponibles[8].
- Marlène Dulaurans et Jean-Christophe Fedherbe : Ensemble de technologies permettant de collecter et d'analyser en temps réel des données issues de sources accessibles au public.

5 U.S. Department of Defense (2010) - DoD Dictionary of Military and Associated Terms *U.S. Department of Defense* - https://irp.fas.org/doddir/dod/jp1_02.pdf

6 North Atlantic Treaty Organization (NATO) (2001) - NATO Open Source Intelligence Handbook - https://archive.org/details/NATOOSINTHandbookV1.2

7 ComCyberGend (2024) - *Une nuit de recherche en sources ouvertes (OSINT) pour les nouveaux cybercombattants* - https://www.defense.gouv.fr/comcyber/actualites/nuit-recherche-sources-ouvertes-osint-nouveaux-cybercombattants

8 CNIL (2024) - *Recoupement d'informations en ligne : ce que vous publiez peut dévoiler votre vie privée* - https://www.cnil.fr/fr/recoupement-dinformations-en-ligne-ce-que-vous-publiez-peut-devoiler-votre-vie-privee

L'utilisation stratégique de l'OSINT soutient les enquêtes criminelles en identifiant des pistes inédites tout en offrant une veille proactive pour détecter les innovations technologiques, les vulnérabilités émergentes et protéger les infrastructures critiques[9].

Malgré la diversité des contextes institutionnels ou académiques, les définitions de l'OSINT partagent plusieurs éléments communs.
Toutes s'accordent sur le fait qu'il s'agit d'un processus dans le but de collecter et d'analyser des informations accessibles au public.
Les définitions du Département de la Défense américain et de l'OTAN insistent sur l'importance de la finalité du renseignement : transformer des données disponibles en information stratégique. Cette dimension stratégique se retrouve également dans la définition de Marlène Dulaurans et Jean-Christophe Fedherbe, qui soulignent l'utilité de cette exploitation en temps réel, notamment dans le domaine judiciaire, permettant d'ajouter une nouvelle dimension de recherche pour les enquêteurs.
Du côté des structures françaises, la CNIL et le ComCyberGend insistent sur l'accessibilité publique des données et le respect du cadre légal, mais reconnaissent aussi leur utilité pour l'identification d'acteurs ou de menaces.

Nous définirons l'OSINT comme la collecte, l'analyse et l'exploitation d'informations accessibles publiquement, dans le but de produire du renseignement exploitable. Ces informations peuvent provenir de sources variées comme :

- les réseaux sociaux (Facebook, X, LinkedIn, ...)
- les messageries (whatsapp, gmail, ...)
- les sites web, blogs et forums
- les bases de données publiques (brevets, entreprises, registres, WHOIS, …)
- les images satellites, photos et vidéos disponibles en ligne
- les articles de presse et publications officielles
- les documents indexés sur le web (PDF, ...)

L'OSINT est utilisé aussi bien par des journalistes, des enquêteurs, des forces de l'ordre, des analystes en cybersécurité que par des entreprises (veille concurrentielle, audit, vérification diligente).
Sa force réside dans l'exploitation d'informations déjà disponibles, sans intrusion ni piratage, ce qui le rend légal dans la majorité des cas à condition de respecter les lois sur la vie privée et la réutilisation des données.

Et les *leaks* ?

Les informations peuvent également provenir de leaks, parfois très importants[10].

9 Marlène Dulaurans et Jean-Christophe Fedherbe – *Projet Vidocq* - https://cyberneticproject.eu/vidocq

10 Cybermalveillance (2024) - *Violation de données personnelles de l'opérateur Free : situation, risques et recommandations* - https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/violation-de-donnees-personnelles-free-202410

Avant d'aller plus loin, il paraît important de différencier deux termes régulièrement utilisés en OSINT : les leaks et le scrapping :

- Le leak est une fuite de données, souvent d'origine illégale. Leur usage est assimilé à du recel.
- Le scraping est une technique consistant à aspirer des données accessibles (réseaux sociaux, annuaires, sites), est en principe légal, mais peut enfreindre les conditions d'utilisation d'un site. Ce n'est donc pas illégal mais peut engendrer un blocage de l'utilisateur par le site de manière permanente. Le glissement vers l'illégalité apparaît lorsque le scraping est massif, non déclaré, ou avec un stockage de données personnelles.

Nous nous intéresserons aux *leaks*, très controversés dans le milieu de l'OSINT, car ils utilisent, comme son nom l'indique, des fuites de données, donc par implication, au recours à des données « dérobées ».
Certaines plateformes hébergées principalement dans d'autres pays proposent pourtant des abonnement afin de consulter les *leaks*, y compris en France (ChapsVision avec leur outils BlackInt et Owlint).
Aux États-Unis il est légal d'accéder à une base de données de *leaks* déjà publiée publiquement (forum, plateformes,...) sans violer un mot de passe, sans piratage, sans accès non autorisé, de consulter uniquement des informations déjà indexées et d'utiliser ces données à des fins de cybersécurité ou de recherche, sans porter atteinte à la vie privée ni les republier [11].
En Angleterre il est interdit généralement la consultation de données issues de fuites, sauf exception spécifique et justifiée. L'accès à des données personnelles provenant d'un *leak* sans autorisation explicite, expose à des sanctions civiles et pénales sauf pour le journalisme d'intérêt public, les recherches universitaires et la protection de l'intérêt vital[12].
Mais que dit la loi en France ?

- Le mot de la CNIL [13] :

La réutilisation de données issues de fuites est illégale, même si elles sont techniquement accessibles sur Internet. La CNIL indique que toute base de données constituée ou mise en ligne de manière manifestement illicite ne peut être réutilisée, sous peine de sanctions, notamment pour recel de données volées: « En outre, la personne qui télécharge ou réutilise une base de données manifestement illégale risque de se rendre coupable du délit de recel. »

- Le mot du Code Pénal [14] :

- Article 321-1 : Le recel est le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit.

11 Legal Information Institute - *18 U.S.C. § 1030 – Computer Fraud and Abuse Act* - https://www.law.cornell.edu/uscode/text/18/1030

12 UK Public General Acts - *Data Protection Act 2018* - https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

13 CNIL (2025) - *Réutilisation de bases de données : les vérifications nécessaires pour respecter la loi* - https://www.cnil.fr/fr/reutilisation-de-bases-de-donnees-les-verifications-necessaires-pour-respecter-la-loi

14 Code Pénal - *Article 321-1* / Article 226-16 – https://www.legifrance.gouv.fr/

Constitue également un recel le fait, en connaissance de cause, de bénéficier, par tout moyen, du produit d'un crime ou d'un délit.
Le recel est puni de cinq ans d'emprisonnement et de 375 000 euros d'amende.

- Article 226-16
Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 3° du IV de l'article 20 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

- Le mot du Directeur du Cyber-Campus de Nouvelle Aquitaine :

C'est illégal !

2 – Méthodologie de recherche

Dans cette seconde partie, nous exposerons la méthode employée pour tester les hypothèses formulées en introduction, notamment les répercussions de la législation française sur l'usage de l'OSINT, ainsi que l'impact potentiel de la dépendance à des plateformes étrangères sur la souveraineté numérique française.

Lorsque nous évoquons OSINT, nous pensons au *Google Dorks* (combinaisons d'opérateurs et de mots-clés reconnus par les moteurs de recherche pour affiner et préciser les résultats d'une recherche), mais également à différentes plateformes gigantesques apportant un soutien non-négligeable dans les recherches menées en sources ouvertes comme :

- Shodan (USA):

Il s'agit d'un moteur de recherche pour appareils connectés. En France, largement utilisé pour scanner les infrastructures françaises et étudier les failles existantes ; étude de Trend Micro à partir des données Shodan début 2017 montre plus de 7 millions d'enregistrements pour la France, couvrant 2,1 millions d'adresses IP [15].

- ShadowDragon (USA):

Il s'agit d'outils OSINT (notamment Horizon™ et SocialNet), axés sur veille médiatique, deep et dark web.

- Palantir (USA):

Il s'agit d'une plateforme de fusion de différentes données destinée aux agences de renseignement et forces de l'ordre. Sa présence en France est très importante notamment sur des domaines sensibles : Airbus, Stellantis, Forvia, DGSI[16]. Il a longtemps été critiqué en France pour son

15 Trend Micro (2017) - *French Cities Exposed* - https://documents.trendmicro.com/assets/wp/wp-french-cities-exposed.pdf

16 IntelligenceOnline (2025) – *France Palantir dans le renseignement français jusqu'à la fin de la présidence Macron ?* - https://www.intelligenceonline.fr/surveillanc-interception/2025/04/17/palantir-dans-le-renseignement-francais-jusqu-a-la-fin-de-la-presidence-macron,110412435-art

hébergement de données sensibles à l'étranger et ses liens avec les agences américaines (NSA, CIA) [17].

- Maltego (Allemagne):

Plateforme utilisée pour les investigations numériques, cartographie de réseaux, transformations. Régulièrement utilisé par les services judiciaires Français. Il respecte le RGPD, mais bénéficie d'un droit allemand parfois perçu comme plus "souple".

- Osint-Indiustries (Angleterre) :

Plateforme pour effectuer des recherches à partir de sélecteur technique (téléphone, email, ...).

Malgré ces plateformes des solutions françaises se positionnent également sur le marché :

- OSINTLab (Thales), outil d'analyse des réseaux sociaux, extrait les tendances, les signaux faibles et les informations pertinentes pour la veille, l'investigation ou l'alerte stratégique.
- ChapsVision : fondé en 2019 et axé sur l'analyse de données pour des clients institutionnels (DGSI, Police nationale, Ministère des Armées) et privés, rival potentiel à Palantir [18].

Étudions les différents cas concrets attribués aux solutions qui ont pu être reportés médiatiquement :

- Palantir (2019)[19] :

  La DGSI a utilisé Palantir Gotham pour fusionner des données afin de surveiller et identifier des menaces terroristes. Malgré la controverse autour de l'hébergement aux États-Unis, le contrat initial passé en 2016 a été renouvelé en 2019 faute de solution française prête.

- Shodan (2014)[20] :

  Le Monde et Rue89 démontrent qu'il est possible de prendre le contrôle de webcams privées et industrielles en quelques clics via Shodan révélant la vulnérabilité des réseaux français.

- Maltego (2025)[21] :

  La Police Nationale française a démantelé une escroquerie aux cryptomonnaies d'un montant de 1,2 million d'euros impliquant 200 agents et Rexxfield. Maltego a joué un rôle clé dans la résolution de cette affaire.

17 Le Monde - *Palantir, l'embarrassant poisson-pilote du big data* - https://www.lemonde.fr/pixels/article/2018/10/09/palantir-l-embarrassant-poisson-pilote-du-big-data_5366568_4408996.html

18 Le Journal du Dimanche (2022) - INFO JDD. Spécialisé dans la cyberintelligence, le français ChapsVision muscle son offre régalienne - https://www.lejdd.fr/Economie/info-jdd-specialise-dans-la-cyberintelligence-le-francais-chapsvision-muscle-son-offre-regalienne-4139546

19 Siècle Digital - *La DGSI prolonge son contrat avec Palantir, société américaine spécialisée dans les logiciels de cybersécurité* - https://siecledigital.fr/2019/11/28/la-dgsi-prolonge-son-contrat-avec-palantir-societe-americaine-specialisee-dans-les-logiciels-de-cybersecurite/

20 Le Monde (2014) - *INTRUSION 2.0 - Avec Shodan, contrôlez des webcams et imprimez chez les autres*. - https://www.lemonde.fr/big-browser/article/2014/06/10/intrusion-2-0-avec-shodan-controlez-des-webcams-et-imprimez-chez-les-autres_6000060_4832693.html

21 x.com – Maltego - https://x.com/MaltegoHQ/status/1886365145083060530

Et les leaks?

Dans le domaine de l'OSINT, certaines plateformes se sont spécialisées dans la collecte, l'indexation et la mise à disposition de données compromises, issues de fuites.

Ces outils, bien que variées dans leur fonctionnement et leur origine géographique, partagent un objectif commun : permettre à leurs utilisateurs de rechercher des informations personnelles
(adresses e-mail, mots de passe, numéros de téléphone, identifiants, ...) dans des bases de données ayant fuité à la suite d'intrusions, de négligences, ou de mise à disposition..

Quelques exemples non-exhaustifs de ces plateformes :

- IntelX (Autriche) : payante, plateforme d'OSINT avancée, proposant l'accès à des leaks, à des documents indexés sur le dark web, ou à des métadonnées. Elle propose des fonctions puissantes de recherche multi-source.
- Snusbase (États-Unis) : payante, spécialisée dans l'indexation rapide des fuites de données.
- DeHashed (États-Unis) : payante, axée sur la recherche de sélecteurs (IP, noms, username,...).
- Leak-Lookup (Royaume-Uni) : propose une interface gratuite mais limitée, avec des abonnements pour des recherches plus poussées.
- Owlint (France) : payante, propose l'analyse de données exposées tout en revendiquant une conformité légale.
- Bots Telegram (Russie) : nombreux bots non officiels proposent des recherches dans des bases de leaks, souvent à des tarifs très accessibles mais dans un cadre légal très flou.
- Zhenhua Data leak (Chine) : recherche dans les fuites de bases de données contenant des profils d'individus étrangers suivis par des entités chinoises .

L'existence et l'usage de ces plateformes soulèvent plusieurs problématiques majeures :

- La légalité de la détention et de l'accès à ces données, qui, dans de nombreux pays, notamment au sein de l'Union européenne, posséder ou utiliser des données personnelles issues de fuites est considéré comme illégal, notamment si ces données n'ont pas été obtenues avec le consentement des personnes concernées, ce qui, il faut le dire, est le cas... Toutefois, certaines plateformes affirment se conformer à la législation locale en n'hébergeant pas directement les données, mais en ne proposant qu'un index de recherche ou un hash anonymisé.
- L'éthique de l'usage car ces données proviennent d'atteintes à la vie privée. Leur usage, même à des fins de veille ou de cybersécurité, pose la question de l'équilibre entre protection et exploitation de l'information.
- La souveraineté des données qui sont généralement hébergées, consultables, voire monétisées depuis des pays hors de la France, interroge la capacité à protéger les données de leurs citoyens et à réguler ce type d'activité.

Le cas particulier de Owlint constitue un exemple atypique. Enregistrée sous juridiction française, cette entreprise affirme respecter le RGPD (Règlement général sur la protection des données) et la législation française. Sur son interface, l'utilisateur peut choisir de désactiver l'utilisation des données issues de leaks dans ses requêtes. Ce paramètre pose question : s'agit-il d'une fonctionnalité destinée à se conformer à la loi française, notamment dans le cadre d'un usage professionnel ou institutionnel (journalisme, cybersécurité, etc.) ? Ou d'une simple précaution juridique face à un cadre encore flou ?

La question centrale demeure : la seule détention de telles données, même si l'accès est contrôlé, est-elle conforme à la loi française ? À ce jour, la législation reste ambiguë, notamment en ce qui concerne l'usage à des fins d'enquête privée, de cybersécurité ou de vérification d'atteintes personnelles.

3 – Résultats et analyse des hypothèses

L'analyse des outils majoritairement utilisés par les acteurs français (forces de l'ordre, cybersécurité, journalistes...) montre une dépendance significative à l'égard de plateformes OSINT étrangères, principalement américaines (Palantir, Shodan, ShadowDragon…). Ces plateformes sont devenues des piliers dans les stratégies d'enquête ou de veille numérique, alors même qu'elles échappent à tout encadrement législatif français.
Les plateformes françaises, bien que présentes (ChapsVision, OSINTLab, Owlint), restent marginales ou en cours de développement. Elles ne couvrent ni l'étendue fonctionnelle ni la réputation internationale de leurs concurrentes étrangères, créant ainsi une forme de monopole technologique dans le domaine de l'OSINT .
Cette dépendance soulève plusieurs risques majeurs :

- La perte de souveraineté numérique, via l'exploitation de données sensibles françaises par des outils hébergés à l'étranger expose ces données à des accès non contrôlés par l'État français, notamment par les agences américaines comme la NSA ou autre agences de renseignement.
- Le risques juridiques et politiques à travers les décisions concernant l'accès, la suppression ou la conservation des données, échappant à toute juridiction nationale.
- La vulnérabilité stratégique, car il suffirait d'une coupure d'accès, d'un changement de politique tarifaire ou d'un litige international entraînant le blocage des outils OSINT utiles pour des services français et une paralysie.

Certaines initiatives européennes émergent pour contrer cette dépendance : l'Agence de l'Union européenne pour la cybersécurité (ENISA) se tourne vers la création d'un OSINT souverain, notamment par le soutien et des financements par Horizon Europe de développement de plateformes, comme Trustee[22] ou encore AI-driven data operations and compliance technologies[23]. Toutefois, la maturité de ces projets reste encore insuffisante face à l'urgence opérationnelle.

D'autre part, la législation française, particulièrement avec le RGPD et les directives de la CNIL, encadre fortement l'exploitation des données personnelles, ce qui freine l'utilisation d'outils OSINT dans certaines techniques.

Et les leaks ?

22 Cordis europa - *TRUST AND PRIVACY PRESERVING COMPUTING PLATFORM FOR CROSS-BORDER FEDERATION OF DATA* - https://cordis.europa.eu/project/id/101070214/reporting/

23 Horizon Europe - *AI-driven data operations and compliance technologies (AI, data and robotics partnership) (IA)* - https://www.horizon-europe.gouv.fr/ai-driven-data-operations-and-compliance-technologies-ai-data-and-robotics-partnership-ia-32590

En France, comme vu précédemment dans notre première partie, la législation interdit la réutilisation de données issues de fuites, même accessibles publiquement. Mais explicitement, rien n'est indiqué concernant la consultation de plateformes référencées dans notre 2nde partie. Nous pouvons tout de même observer qu'il s'agit d'utiliser « des biens provenant d'un vol », entrant ainsi dans la définition du recel. Ce vide juridique engendre un paradoxe : les acteurs français sont dépendants de services privés étrangers, parfois à des fins légitimes (vérification de compromission, cybersécurité, enquêtes), mais dans un cadre juridiquement incertain, voire interdit. Cette situation peut s'apparenter à une perte de souveraineté numérique, car les données françaises compromises circulent sur des plateformes étrangères, échappant à tout contrôle institutionnel ou judiciaire national. De plus, certains services français (entreprises privées de cybersécurité, journalistes, analystes) admettent, de manière non officielle, avoir recours à ces outils.

Dans d'autres pays, comme les États-Unis, le cadre légal est plus souple : la consultation de leaks publiquement disponibles n'est pas forcément illégale (notamment dans les domaines judiciaires).
L'e Royaume Uni interdit l'accès sauf pour des motifs d'intérêt public (journalisme, recherches universitaires).
Ce contraste révèle une fracture opérationnelle entre les pays. La France applique un principe de restriction total, pouvant freiner l'innovation et limiter les capacités d'enquête dans les milieux publics ou privés tandis que d'autres pays adoptent une logique d'efficacité : tant que l'accès est passif et qu'aucune intrusion n'a lieu l'exploitation des données peut être tolérée.
Cela crée un désavantage significatif pour les acteurs français, qui doivent contourner ou éviter certains outils, tandis que d'autres pays y recourent ouvertement, notamment dans le domaine de la cybersécurité, de l'enquête et la vérification de compromission.

Ce flou autour des pratiques OSINT accentue les risques pour les acteurs français :

- Soit ils respectent strictement le droit national, mais renoncent à des sources précieuses accessibles à leurs concurrents étrangers.
- Soit ils utilisent certains outils en toute discrétion, pouvant se mettre en difficulté pénalement ou être à l'origine d'un scandale en cas de divulgation.

Conclusion

Les résultats tendent à confirmer nos deux hypothèses :

- La France dépend structurellement d'outils OSINT non-français, voire non-européen, ce qui compromet sa souveraineté numérique.
- La législation française, bien qu'éthique, limite l'efficacité opérationnelle des utilisateurs de l'OSINT par rapport aux régulations plus souples d'autres pays.

Pour contrer cette situation, plusieurs possibilités sont à envisager, notamment favoriser soutenir et accompagner le développement de plateformes souveraines, clarifier juridiquement l'usage des plateformes de leaks, adapter la législation à la réalité des pratiques (par un encadrement à certains acteurs).

La législation française, notamment le RGPD et les interventions de la CNIL, peut être plus contraignante pour des entreprises françaises comme OSINTLab (Thales) et ChapsVision, comparativement à des acteurs étrangers comme Palantir (USA) ou Maltego (Allemagne). Voici une analyse juridique et sociopolitique de cette asymétrie :

Les entreprises européennes comme ChapsVision ou Thales sont directement soumises à un contrôle étroit par leurs autorités nationales (CNIL, DGFIP, ANSSI...).

Les entreprises extra-européennes (comme Palantir) peuvent sous-traiter la responsabilité juridique à des filiales européennes, mais les sanctions sont plus longues à mettre en œuvre et les contrôles sont plus difficiles à appliquer (juridiction, diplomatie, négociations transatlantiques).

Par exemple, en 2020, la CNIL a condamné Google et Amazon pour des violations liées aux cookies, mais cela a pris des années d'enquêtes complexes avec des obstacles de juridiction.
En revanche, une société française peut être sanctionnée en quelques mois, car la CNIL a un accès direct à ses documents, locaux et personnels.

De plus, les acteurs français dans le domaine de l'OSINT sont bien plus jeunes que ceux présentés précédemment outre France.
La préférence pour des outils plus « matures » peut expliquer cette large adoption d'outils étrangers.
La théorie de la Construction sociale des technologies de Trévor Pinch et Wiebe Bijker (1984)[24] expliquent que les technologies ne se diffusent pas seulement parce qu'elles sont techniquement supérieures, mais parce que différents groupes sociaux notamment des experts, utilisateurs, décideurs, les valident et les adaptent à leurs normes et valeurs.
Une seconde théorie de Pascal Plantard (2012)[25], décrit comment les usages technologiques s'inscrivent dans des "techno-imaginaires" : les représentations sociales alimentent des normes

24 Trévor Pinch et Wiebe Bijker (1984) - *The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology might Benefit Each Other* - https://journals.sagepub.com/doi/10.1177/030631284014003004

25 Pascal Plantard (2012) - *Anthropologie des usages du numérique* - https://shs.hal.science/tel-01164360

d'usage qui favorisent les outils connus, éprouvés, rassurants plutôt que des nouveaux sur lesquels il faudrait se reformer.

Il existe une dualité française : le discours public est souverainiste (promouvoir l'autonomie numérique), mais les acteurs publics utilisent malgré tout des solutions étrangères (Palantir, Maltego), car ces solutions sont jugées plus "matures", "interopérables", ou "prêtes à l'emploi".
Cela crée une forme d'asymétrie stratégique car les acteurs français doivent respecter à la lettre la doctrine RGPD et la législation française, tandis que les acteurs étrangers bénéficient d'une tolérance politique liée à leur efficacité perçue ou à leur réputation.

Néanmoins, une réflexion semble en marche pour réguler et mettre « au même niveau» les techniques françaises notamment autour des fuites de données : des professionnels et députés se sont assemblés afin d'étudier et autoriser la récupération de leaks [26].
Ces mesures, bien que « nécessaire » pour établir une souveraineté nationale dans la gestion de ces données, ne sont pas saluées par l'ensemble des professionnels agissant autour de la cybersécurité ; en effet, Maître Marc-Antoine LEDIEU, Avocat au Barreau de Paris, critique une proposition visant à encadrer juridiquement la pratique de l'OSINT, notamment la collecte et le stockage de données issues de leaks, même à des fins de cybersécurité. Il considère que, malgré de bonnes intentions, cette initiative ouvre la voie à de nombreux problèmes juridiques, soulève des enjeux éthiques et commerciaux et appel à la prudence aux professionnels exerçant l'OSINT. Son alternative serait d'assouplir la juridiction exclusivement aux forces de l'ordre et à la justice, via une loi ciblée[27].

Nous avons pu voir que des plateformes existent depuis plusieurs années afin de pouvoir consulter les leaks via un abonnement à ces dernières, de nombreux bots Telegram payants sont également capables de répondre à ce genre de requêtes, mais d'autres plateformes ont existé sur un principe de gratuité et de libre consultation, mais se sont retrouvées fermées, notamment via les forces de l'ordre locales (illiciteservice, search-0t-rocks).

Les questions suivantes peuvent alors se poser :
Est-ce l'argent et les principes commerciaux peuvent réguler à ce point l'utilisation de données très controversées comme les leaks au dépit de l'éthique et de la législation ?
Pourquoi des plateformes payantes « sans plus de vérifications que celle de la carte bancaire » peuvent prétendre être plus légitimes et attirer moins l'attention des pouvoirs publics que des plateformes libres ?
Est ce que la puissance et les finances peuvent être un passe droit sur les législations ?
Les travaux de Frank Pasquale (2016)[28] montre que les grandes entreprises technologiques possèdent des systèmes opaques appelés « boîtes noires » leur permettant de contrôler

26 Journaldunet (2025) - *Osint : des professionnels et députés veulent autoriser la récupération de leaks* - https://www.journaldunet.com/cybersecurite/1541623-osint-des-professionnels-et-deputes-veulent-autoriser-la-recuperation-de-leaks/

27 Marc-Antoine LEDIEU (2025) – *Linkedin* - https://fr.linkedin.com/posts/marc-antoine-ledieu-a040917_osint-des-professionnels-et-d%C3%A9put%C3%A9s-veulent-activity-7331248372969787392-ezCG

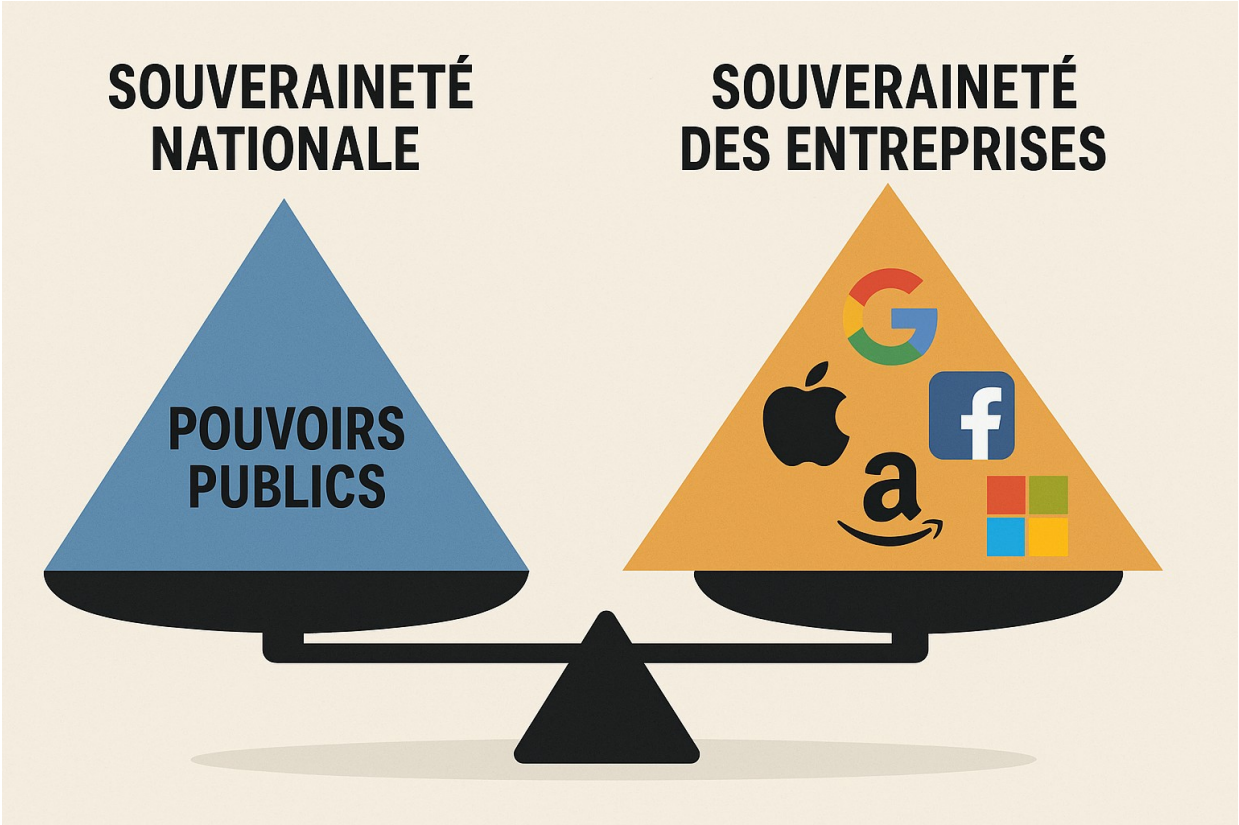
l'information et d'influencer discrètement le public et les régulateurs. Trop puissantes, elles

échappent ainsi à une surveillance effective, tandis que de plus petits acteurs sont plus régulièrement sanctionnés.

Entre États, citoyens et entreprises, la souveraineté nationale (légitime, juridique et territoriale) est mise à l'épreuve par l'essor des GAFAM.

En 2019, le Sénat lance l'alerte face à l'emprise des GAFAM, notamment sur le fait que l'État français doit préserver "l'autonomie informationnelle" [29].

Selon Christian Byk (2022)[30], ces plateformes exercent une forme de "souveraineté 2.0", redéfinissant les rapports de pouvoir dans l'espace numérique.



28 Frank Pasquale (2016) - *Black Box Society* - https://raley.english.ucsb.edu/wp-content/Engl800/Pasquale-blackbox.pdf

29 Sénat (2019) - Le devoir de souveraineté numérique - https://www.senat.fr/rap/r19-007-1/r19-007-1_mono.html

30 Christian Byk (2022) - L'ère du numérique conduit-elle à l'émergence de nouveaux acteurs et formes de souveraineté ? - https://journals.openedition.org/cdst/6859

Bibliographie

- Pauline Türk (2020)

La souveraineté numérique européenne, vers une troisième voie ?
https://shs.cairn.info/publications-de-pauline-turk--42254?lang=fr

- François Pellegrini (2021)

Open source, pour un numérique souverain ?
https://www.librealire.org/open-source-pour-un-numerique-souverain

- Julien Nocetti (2023)

La souveraineté numérique : dix ans de débats, et après ?
https://stm.cairn.info/revue-enjeux-numeriques-2023-3?lang=fr

- Pierre Bellanger (2011)

La souveraineté numérique
https://www.institutdiderot.fr/wp-content/uploads/2019/12/Diner-La-Souverainete%CC%81-nume%CC%81rique-Page.pdf

- Steele, R. D. (2007)

Open source intelligence (OSINT): What is it? Why is it important to the military? Military Review
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2762766/

- U.S. Department of Defense (2010)

DoD Dictionary of Military and Associated Terms U.S. Department of Defense
https://irp.fas.org/doddir/dod/jp1_02.pdf

- North Atlantic Treaty Organization (NATO) (2001)

NATO Open Source Intelligence Handbook
https://archive.org/details/NATOOSINTHandbookV1.2

- Recorded Future (2024)

What is open source intelligence (OSINT)?
https://www.recordedfuture.com/blog/open-source-intelligence-definition

- OSINT Time Project (2021)

Introduction to Open Source Intelligence (OSINT)
https://medium.com/@osinttimeproject/introduction-to-open-source-intelligence-osint-824a1c2138ac

- Marlène Dulaurans et Jean-Christophe Fedherbe

Projet Vidocq
https://cyberneticproject.eu/vidocq

- ComCyberGend (2024)

Une nuit de recherche en sources ouvertes (OSINT) pour les nouveaux cybercombattants
https://www.defense.gouv.fr/comcyber/actualites/nuit-recherche-sources-ouvertes-osint-nouveaux-cybercombattants

- CNIL (2024)

Recoupement d'informations en ligne : ce que vous publiez peut dévoiler votre vie privée
https://www.cnil.fr/fr/recoupement-dinformations-en-ligne-ce-que-vous-publiez-peut-devoiler-votre-vie-privee

- Cybermalveillance (2024)

Violation de données personnelles de l'opérateur Free : situation, risques et recommandations
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/violation-de-donnees-personnelles-free-202410

- CNIL (2025)

Réutilisation de bases de données : les vérifications nécessaires pour respecter la loi
https://www.cnil.fr/fr/reutilisation-de-bases-de-donnees-les-verifications-necessaires-pour-respecter-la-loi

- Legal Information Institute

18 U.S.C. § 1030 – Computer Fraud and Abuse Act
https://www.law.cornell.edu/uscode/text/18/1030

- UK Public General Acts

Data Protection Act 2018
https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

- Trend Micro (2017)

French Cities Exposed
https://documents.trendmicro.com/assets/wp/wp-french-cities-exposed.pdf

- IntelligenceOnline (2025)

France Palantir dans le renseignement français jusqu'à la fin de la présidence Macron ?
https://www.intelligenceonline.fr/surveillanc-interception/2025/04/17/palantir-dans-le-renseignement-francais-jusqu-a-la-fin-de-la-presidence-macron,110412435-art

- x.com

Maltego
https://x.com/MaltegoHQ/status/1886365145083060530

- Le Journal du Dimanche (2022)

INFO JDD. Spécialisé dans la cyberintelligence, le français ChapsVision muscle son offre régalienne
https://www.lejdd.fr/Economie/info-jdd-specialise-dans-la-cyberintelligence-le-francais-chapsvision-muscle-son-offre-regalienne-4139546

- Le Monde

Palantir, l'embarrassant poisson-pilote du big data
https://www.lemonde.fr/pixels/article/2018/10/09/palantir-l-embarrassant-poisson-pilote-du-big-data_5366568_4408996.html

- Siècle Digital

La DGSI prolonge son contrat avec Palantir, société américaine spécialisée dans les logiciels de cybersécurité
https://siecledigital.fr/2019/11/28/la-dgsi-prolonge-son-contrat-avec-palantir-societe-americaine-specialisee-dans-les-logiciels-de-cybersecurite/

- Le Monde (2014)

INTRUSION 2.0 - Avec Shodan, contrôlez des webcams et imprimez chez les autres.
https://www.lemonde.fr/big-browser/article/2014/06/10/intrusion-2-0-avec-shodan-controlez-des-webcams-et-imprimez-chez-les-autres_6000060_4832693.html

- Cordis europa

TRUST AND PRIVACY PRESERVING COMPUTING PLATFORM FOR CROSS-BORDER FEDERATION OF DATA
https://cordis.europa.eu/project/id/101070214/reporting/

- Horizon Europe

AI-driven data operations and compliance technologies (AI, data and robotics partnership) (IA)
https://www.horizon-europe.gouv.fr/ai-driven-data-operations-and-compliance-technologies-ai-data-and-robotics-partnership-ia-32590

- Trévor Pinch et Wiebe Bijker (1984)

The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology might Benefit Each Other
https://journals.sagepub.com/doi/10.1177/030631284014003004

- Pascal Plantard (2012)

Anthropologie des usages du numérique
https://shs.hal.science/tel-01164360

- Journaldunet (2025)

Osint : des professionnels et députés veulent autoriser la récupération de leaks
https://www.journaldunet.com/cybersecurite/1541623-osint-des-professionnels-et-deputes-veulent-autoriser-la-recuperation-de-leaks/

- Marc-Antoine LEDIEU (2025)

Linkedin
https://fr.linkedin.com/posts/marc-antoine-ledieu-a040917_osint-des-professionnels-et-d%C3%A9put%C3%A9s-veulent-activity-7331248372969787392-ezCG

- Frank Pasquale (2016)

Black Box Society
https://raley.english.ucsb.edu/wp-content/Engl800/Pasquale-blackbox.pdf

- Sénat (2019)

Le devoir de souveraineté numérique
https://www.senat.fr/rap/r19-007-1/r19-007-1_mono.html

- Christian Byk (2022)

L'ère du numérique conduit-elle à l'émergence de nouveaux acteurs et formes de souveraineté ?
https://journals.openedition.org/cdst/6859