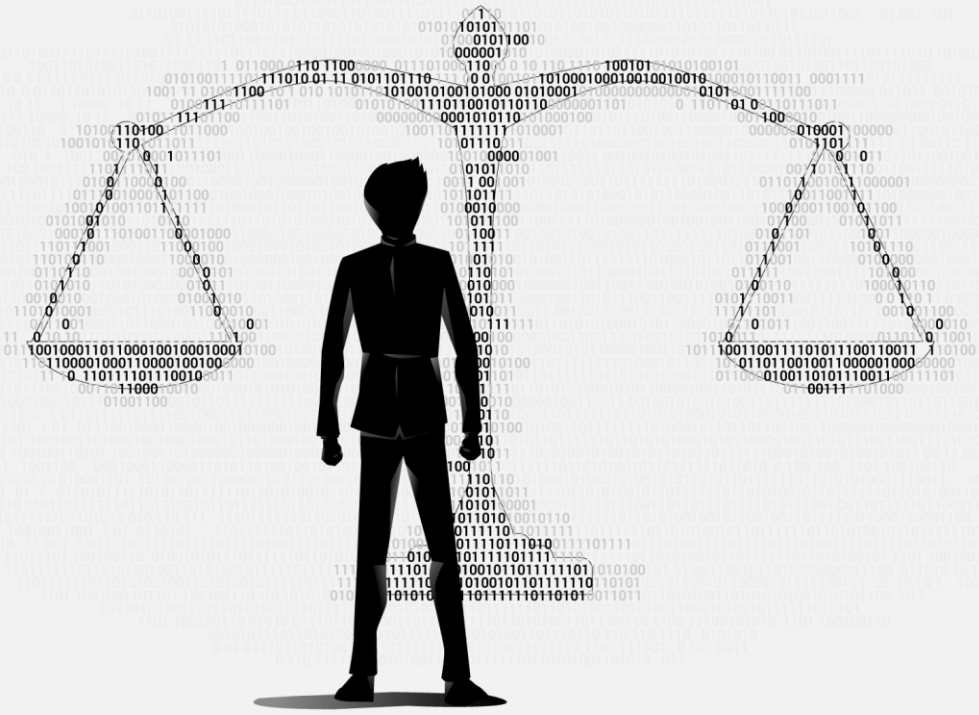
LIVRE BLANC

LE CADRE LÉGAL DE L'OSINT

Réflexion intercommunautaire



1re édition – 2023

1 ÉDITORIAL

Derrière l'acronyme **OSINT** (Open Source Intelligence) ou **ROSO** (Renseignement d'Origine Sources Ouvertes), se cachent **une méthode et un ensemble de techniques visant à identifier, collecter et analyser des informations** relatives à une cible, **extraites de sources librement et légalement accessibles** (sites web, réseaux sociaux, etc.) à tout un chacun à des fins de renseignement. Néanmoins, cette discipline tournée vers l'investigation se heurte à des enjeux définitionnels, éthiques, légaux et peine à être clairement définie.

Quels sont les contours juridiques ou réglementaires qu'il serait possible de tracer pour encadrer cette pratique ? Et quelle serait leur portée (nationale ou européenne) ? Quelles sont les bonnes pratiques et où sont les limites, entre éthique et légitimité des moyens employés ?

Conscient des enjeux liés à cette méthode de renseignement, ce document, qui se veut avant tout pratique, est proposé comme le **premier mini-guide initiatique** à **l'usage de toute personne pratiquant l'OSINT**, dans un cadre privé ou professionnel.

Ce document a donc été pensé comme un **outil d'aide à la recherche**. Il est le fruit d'une réflexion intercommunautaire et à vocation populaire. Nous recommandons au lecteur de commencer par se familiariser avec la table des matières, que nous avons voulu assez détaillée pour permettre de trouver l'information utile rapidement.

Nécessairement non exhaustif, notamment en ce qui concerne les bases de données établies dans d'autres pays hors union européenne. Ce mini-guide se veut vivant et l'ambition des auteurs est d'opérer des mises à jour régulières de ce document. Il pourra à ce titre être utilement complété et actualisé à l'avenir avec de nouvelles ressources. À cet égard, les retours d'informations seront précieux et il est possible de contacter les rédacteurs aux coordonnées indiquées en fin de document.

Enfin, nous tenons à rappeler que la pratique de l'OSINT est avant tout une démarche de **production de connaissance** (nous invitons le néophyte à se documenter via les nombreuses ressources en ligne disponibles sur les sites des différentes communautés et qui sont abordés en fin de document).

La version initiale de ce document a été élaborée en avril 2023 et n'engage que ses auteurs. Publiés sous les termes de la licence :

CC BY-NC-ND (Partage avec Attribution, Pas d'usage commercial, Pas de modification)

TABLE DES MATIERES

2 PRÉAMBULE : CERNER LE SUJET JURIDIQUE

2.1 OSINT : acronyme et définition

Il existe plusieurs définitions communément admises de l'OSINT[1], mais pour en retenir une complète, nous dirons qu'il s'agit d'une technique de **recueil,** de **traitement** et d'**analyse** d'informations disponibles « en sources ouvertes » ou « publique »[2], accessibles **légalement** à tout un chacun à des fins de **renseignement**.

Ces sources d'informations peuvent prendre plusieurs formes (journaux, sites web, conférences, réseaux sociaux…). Il est cependant primordial que l'information soit **accessible à tous,** sans usage de coercition, ruse, stratagème ou hacking.

Ce principe repose également sur deux notions clés : la **traçabilité** de l'information et la **réversibilité** de la méthode (n'importe qui doit pouvoir refaire le processus d'accès à l'information).

Nous cantonnerons ici notre réflexion aux seules données numériques accessibles depuis internet.

2.2 OSINT : Donnée ? Information ?

« Data » ? « Donnée » ? « Information » ? Retenez que les « données numériques » (nous dirons « data ») sont une « représentation » technique d'informations. C'est précisément la définition posée par le règlement UE sur l'*open data* du 30 mai 2022[3] : « *toute représentation numérique d'actes, de faits ou d'informations […] notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels* ». En clair, des data numériques ne constituent que l'aspect technique d'une information (un savoir, un « renseignement ») intelligible, éventuellement à valeur ajoutée, pour un humain.

L'analyse d'informations ne pose que peu de problèmes aux juristes : il s'agit d'exprimer une opinion, une appréciation subjective des informations contenues dans les data collectées. C'est là affaire de liberté d'expression et de ses limites, suffisamment encadrées par le droit commun sur lequel nous ne reviendrons pas.

2.3 OSINT : les points de vigilance juridique

Le problème pour les juristes, c'est d'abord la légalité de l'opération de collecte des data puis celle de leur réutilisation. Puisque nous nous intéressons à des data à copier d'origine « sources ouvertes/publiques », il faut veiller (dans l'ordre) :

(i) à se connecter de manière légitime (loyale) au système d'information pour accéder aux data qui y sont stockées ;

(ii) à disposer du droit de copier les data ;

(iii) à disposer du droit de réutiliser les data.

Évidemment, ces trois conditions successives sont cumulatives. Pour agir dans la légalité, il vous faudra franchir successivement ces 3 niveaux de *compliance*.

---

(1) Open Source INTelligence ou OSINT : littéralement « renseignement en sources ouvertes » ou « ROSO » pour l'acronyme français de « Renseignement d'Origine Source Ouverte »

(2) Wikipedia https://fr.wikipedia.org/wiki/Renseignement_d%27origine_sources_ouvertes

(3) Règlement UE n°2022/868 du 30 mai 2022 portant sur la gouvernance européenne des données https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022R0868

Le dernier niveau sera le plus difficile à réussir car il dépend entièrement de l'usage qui sera fait des data, soit dans un rapport professionnel « confidentiel », soit dans une divulgation publique.

3 NIVEAU 1 : VÉRIFIER LE DROIT D'ACCÈS AU SI CONTENANT LES DONNEES

3.1 La question rituelle…

> *- (question d'un client inquiet) D'où viennent ces informations ?*
>
> *- (réponse embarrassée de l'osinteur) … j'ai piraté un accès serveur et puis…*

Non, cette manière de faire - pour commencer - n'est pas légale.

3.2 La qualification pénale pour accès ou maintien dans un Système de Traitement Automatisé de Données (STAD)

Un accès frauduleux dans un système d'information[4] constitue sans doute possible le délit réprimé par l'article 323-1 du Code pénal. Le caractère « frauduleux » d'un accès et d'un maintien dans un système d'information (SI) est constitué dès que la personne qui rentre dans un SI ne dispose pas d'une autorisation préalable, d'un consentement de la part de l'exploitant de ce SI. Précisons que tout accès à un SI d'une manière non prévue par son exploitant (via une vulnérabilité, par exemple) est - bien sûr - également un accès frauduleux. Depuis le 24 janvier 2023[5], le « tarif » judiciaire de cette infraction pénale est de 3 ans de prison et de 150 000 € d'amende.

Se pose le problème de l'accès à un système d'information (un site web, etc.) qui serait peu ou mal sécurisé. Seul un juge peut décider si un SI est sécurisé « à l'état de l'art ».

Cette appréciation est largement simplifiée lorsque « l'attaqué » reconnaît lui-même à l'audience le défaut de sécurisation. Mais l'hypothèse est suffisamment rare[6] pour ne pas tenter le diable en se reposant sur le seul argument « *c'était pas sécurisé* ».

Comme vous ne faites jamais ça, nous pouvons passer au niveau 2.

4 NIVEAU 2 : LE DROIT DE COLLECTER DES DATA

4.1 Les délits à ne pas commettre

Vous pouvez techniquement accéder à des data numériques ?

Vous pouvez donc techniquement les copier dans votre système d'information.

Mais en avez-vous le droit ?

---

(4) Le Code pénal français utilise la notion de « système de traitement automatisé de données » (ou « STAD ») qui - fonctionnellement - rejoint celle de « système d'information » ou « SI ». Nous privilégierons l'emploi de ce dernier terme.

(5) LOPMI (loi d'orientation et de programmation du ministère de l'Intérieur) n°2023-22 du 24 janvier 2023 https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047046768

(6) Ce fut le cas pour Olivier.L alias « Bluetouff », l'ANSES ayant reconnu sa négligence en matière de sécurité, ce qui a conduit la Cour d'appel (5 février 2014) à le relaxer du chef « d'accès frauduleux » https://www.legalis.net/jurisprudences/cour-dappel-de-paris-pole-4-chambre-10-arret-du-5-fevrier-2014

La jurisprudence « Bluetouff »[7] de 2015 de la Cour de cassation nous apporte une réponse très claire : soustraire des données « sans le consentement de leur propriétaire » constitue le délit pénal de vol[8].

Attention, si vous n'êtes pas le « voleur » mais que vous téléchargez le produit d'un vol (hypothèse d'un *leak* disponible depuis un site .onion), vous êtes « receleur » de ce vol. Le receleur est la personne qui « détient une chose […] en sachant que cette chose provient d'un crime ou d'un délit »[9]. Sanction : 5 ans de prison et 375 000 € d'amende.

Le Code pénal va plus loin et prévoit un délit spécifique à l'article 323-3 pour punir la personne qui viendrait à « extraire, détenir [ou] reproduire » les données contenues dans un SI (auquel elle aurait accédé frauduleusement). Le tarif pénal, là encore, est assez lourd : 5 ans d'emprisonnement et 150 000 € d'amende.

Et attention, pour l'application de cet article, la Cour de cassation a précisé en 1999 que le délit était constitué, même si son auteur n'était pas « animé de la volonté de nuire »[10].

Voyons maintenant les conditions légales de copie, hors délit pénal, et plongeons dans les arcanes du droit de l'Union européenne.

4.2 Le droit de l'*open data* : des données en libre copie (et réutilisation)

Si vous souhaitez copier des données, vérifiez qu'elles sont en *open data* !

À compter du 24 septembre 2023, en application du règlement EU *Data Governance Act*[11], véritable loi européenne d'application directe dans les 27 pays de l'UE, certaines données seront officiellement libres de copie et de réutilisation, à titre professionnel ou personnel.

Des données en *open data* peuvent provenir du secteur privé, mais aussi et surtout du secteur public pour être (ré)utilisées par « des personnes physiques ou morales, à des fins commerciales ou non commerciales »[12].

Les données seront accessibles gratuitement ou à des frais raisonnables pour le « réutilisateur », sans exclusivité. Elles devront en outre avoir été traitées au préalable pour ne plus contenir de « données à caractère personnel » (obligation d'anonymisation) ni porter atteinte à un « secret d'affaires » ou à un droit d'auteur.

---

(7) Cour de cassation chambre criminelle 20 mai 2015 n°14-81.336 https://www.legifrance.gouv.fr/juri/id/JURITEXT000030635061

(8) Article 311-1 du Code pénal « Le vol est la soustraction frauduleuse de la chose d'autrui » https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418127/2023-02-17 Sanction pénale : 3 ans de prison et 45 000 € d'amende (article 311-3 du Code pénal https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418131).

(9) Article 321-1 du Code pénal https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418234

(10) Cour de cassation chambre criminelle 8 décembre 1999 n° 98-84.752 https://www.legifrance.gouv.fr/juri/id/JURITEXT000007069418

(11) Règlement (UE) « DGA » n°2022/868 du 30 mai 2022 portant sur la gouvernance européenne des données https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32022R0868&from=EN

(12) L'UE précise : des « données détenues par des organismes du secteur public à des fins (…) autres que l'objectif initial de la mission de service public pour lequel les données ont été produites » (article 2.2 du règlement (UE) n°2022/868)

4.3 Le droit d'extraction légitime depuis une base de données « privée »

Si vous consultez légitimement une base de données (hors *open data*), vous regardez ce que contient une « base de données » au sens de la directive européenne de 1996[13]. Cette législation est unique au monde.

Le concept se résume simplement. Si une entreprise dépense du temps et de l'argent à « remplir » une base de données, cette entreprise est « producteur » de son contenu. La qualité de producteur permet d'interdire, au sens pénal du terme, toute copie d'une quantité « substantielle » du contenu d'une base de données.

La loi permet en contrepartie à toute personne qui accède de manière légitime au contenu d'une base de données d'en faire un usage libre, pour autant que le contenu copié soit « non substantiel ».

Pour le dire autrement, si vous accédez à la base de données des entreprises légalement constituées en France, vous pourrez copier l'intégralité (ou une quantité modeste) des data concernant une entreprise, mais pas celles concernant toutes les entreprises. Cela s'applique aux données collectées depuis Facebook, LinkedIn, TikTok, etc.

Le niveau 2 étant réussi, passons au niveau 3: que peut-on légalement faire avec des data d'origine OSINT légalement copiées ?

[13] Directive 96/9/CE du 11 mars 1996 concernant la protection juridique des bases de données https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:31996L0009

5 NIVEAU 3 : LE DROIT DE RÉUTILISATION DES DATA

5.1 La qualification pénale de « réutilisation de données sans consentement »

Disons-le sans préambule : réutiliser des data volées, c'est-à-dire copiées « sans le consentement de leur propriétaire », constitue également le délit pénal de vol. C'est encore l'arrêt de la Cour de cassation de 2015[14] dans l'affaire « Bluetouff » qui l'affirme.

L'article 323-3 du Code pénal complète cette jurisprudence : « reproduire, transmettre… » des data *volées* (par exemple téléchargées dans un *leak*) « est puni de 5 ans d'emprisonnement et de 150 000 € d'amende ».

5.2 Le risque d'atteinte aux droits du producteur du contenu d'une base de données « privée »

Enfin, si vous doutiez du sérieux du délit commis par l'osinteur inconscient à qui prendrait l'idée folle de copier la totalité d'une base de données, l'article L.343-4 du Code de la propriété intellectuelle[15] punit de 7 ans de prison et de 750 000 € d'amende toute personne qui viendrait à « porter atteinte aux droits du producteur » d'une base de données. Pour le dire autrement, copier une partie « substantielle » du contenu d'une base de données, ou réutiliser plus qu'une partie non substantielle du contenu de cette même base de données constitue un délit pénal particulièrement grave lorsqu'il est commis « en bande organisée ».

5.3 La problématique centrale du droit d'usage des data d'origine OSINT

Heureusement, vous avez choisi d'accéder à une base de données en *open data* : qu'avez-vous le droit de faire avec les data que vous téléchargez ? Si vous respectez bien toutes les conditions (un peu longues à énumérer ici) de la loi, vous pourrez réutiliser ces data « à des fins commerciales ou non commerciales »[16] et de manière « confidentielle » ou publique.

De la même manière, sur le fondement du droit des bases de données auxquelles vous auriez accédé de manière légitime, vous pourrez réutiliser, « à quelque fin que ce soit […] des parties non substantielles de son contenu »[17]. Attention, « réutiliser » se comprend, selon la jurisprudence de la Cour d'appel de Paris de 2021[18], comme télécharger des contenus ou les « indexer » par lien http actif sans téléchargement.

---

[14] Cité en note [7]

[15] Article L.343-4 du Code de la propriété intellectuelle https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032655054/2023-02-17

[16] Article 2.2 du règlement UE n°2022/868 du 30 mai 2022 https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32022R0868&from=EN

[17] Article 8.1 de la directive 96/9/CE du 11 mars 1996 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:31996L0009

[18] Jurisprudence « Le Bon Coin c. Entre Particuliers » CA Paris 2 février 2021 https://www.legalis.net/jurisprudences/cour-dappel-de-paris-pole-5-ch-1-arret-du-2-fevrier-2021 et Cour de cassation 5 octobre 2022 https://www.courdecassation.fr/decision/633d28b9a3bbc43e2e4d4b68

5.4 Réutiliser des data dans un rapport « confidentiel »

Mais oublions le juridique un instant et regardons la réalité : vous effectuez des recherches en OSINT pour rendre, à titre professionnel, un rapport à votre client. Votre rapport concerne par exemple un investisseur personne physique, une entreprise étrangère, ou un groupe d'attaquants cyber. Que vous fassiez de l'intelligence économique ou de la CTI[19], vous prendrez évidemment soin d'indiquer clairement « confidentiel » en tête de votre rapport.

Si votre rapport a été transmis au client de manière suffisamment sécurisée, qui saura ce qu'il contient (à part ses destinataires) ? Et qui pourrait se plaindre de l'éventuelle illégalité des data qui y seraient contenues ? La réponse pratique à ce problème est une variante du célèbre dicton « pas vu, pas pris »… d'autant que, devant un juge pénal, une preuve obtenue de manière illicite peut parfaitement être prise en compte (voir section 6.2 « La preuve en droit pénal »).

Mais si le rapport « fuite » et devient public, que peut-il se passer ? Si la « fuite » vient du système d'information de l'osinteur, le *leak* révèlera le nom de celui ou celle qui a collecté et stocké les data et il appartiendra alors à l'osinteur *victime* de (tenter de) prouver la légalité de ses opérations de collecte, de stockage et de réutilisation…

Si la « fuite » provient d'un piratage du SI du client auquel le rapport a été remis, c'est le « piraté » (le client) qui risque juridiquement d'avoir officiellement des problèmes… avant de se retourner en responsabilité contre l'osinteur.

5.5 Le risque de divulguer publiquement des data (pourtant) librement accessibles ?

Que des data soient librement accessibles est une chose, que la loi vous permette de les réutiliser librement et publiquement en est une autre… Un exemple simple ? Le contenu de la quasi-totalité des sites web ! En naviguant sur un site web vitrine, de e-commerce, etc., vous disposez du droit de visualiser les contenus qui vous sont proposés en ligne mais pas du droit de les copier. Et ce pour des tas de raisons juridiques non encore évoquées jusqu'à présent. Vous retiendrez sans problème les deux raisons principales.

Imaginons que vous naviguiez sur un site web sur lequel sont librement consultables des présentations illustrées en bandes dessinées : avez-vous le droit de télécharger ces présentations pour les réutiliser à titre professionnel ? Le Code de la propriété intellectuelle en France vous répond que non. Si vous le faites, vous êtes contrefacteur et vous risquez 3 ans de prison et 300 000 € d'amende[20].

Imaginons que vous soyez assez inconscient pour publier le fruit de recherches concernant des personnes physiques identifiées (par leur nom/prénom/adresse/numéro de portable,…). Vous commettriez le délit pénal de traitement « frauduleux, déloyal ou illicite » de données à caractère personnel et vous risqueriez, votre publication étant un aveu en soi (*une preuve facilement collectable en OSINT*), 5 ans d'emprisonnement et 300 000 € d'amende[21].

---

[19] CTI pour Cyber Threat Intelligence ou « renseignement sur la menace cyber »

[20] Article L.335-2 du Code de la propriété intellectuelle https://www.legifrance.gouv.fr/codes/id/LEGISCTA000006161658

[21] Article 226-18 du Code pénal https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006417968/2023-02-17

Dernier point, si vous divulguez publiquement des informations protégées dans l'Union européenne par la législation « secret d'affaires »[22], que risquez-vous juridiquement ?

Bonne nouvelle (?), aucune sanction pénale n'est attachée en France à une atteinte publique à un secret d'affaires (par essence privé). Néanmoins, le droit - comme la nature - ayant horreur du vide[23], la France a transposé la directive « secret d'affaires » en prévoyant trois types d'action judiciaire[24] : la première permet de prévenir (par anticipation) la réutilisation ou la divulgation publique, par une personne non autorisée, de secrets d'affaires. La deuxième action tend à permettre sa cessation. La troisième est une mise en œuvre d'une demande d'indemnisation tout à fait dérogatoire des règles du droit commun (« éliminer tout avantage commercial ou économique que l'auteur de l'atteinte au secret des affaires aurait pu tirer de l'obtention, de l'utilisation ou de la divulgation illicite du secret des affaires » prévoit l'article L152-3 du Code de commerce).

5.6 Le problème spécifique du téléchargement de « leaks »

Les *leaks*, très utiles pour savoir « qui » a subi une fuite de données, donnent également de précieux renseignements sur les vulnérabilités exploitées par celles et ceux qu'il faut bien qualifier de « voleurs »[25] d'information et posent un véritable problème juridique.

Aucun professionnel sérieux ne peut prétendre accéder à un *leak* ni le copier, sans se douter de son origine illicite. L'analyste de CTI qui viendrait à copier/télécharger un *leak* se rendrait probablement coupable de recel[26] de vol d'informations numériques[27]. On pourrait alors tenter de plaider *je détiens ce leak de manière « légitime à des fins de recherche ou de sécurité informatique »* (article 323-3-1 du Code pénal). À l'égard du ministère public, pourquoi pas (cela nous paraît risqué). À l'égard d'une personne privée, morale ou physique, cela nous paraît très risqué.

Le problème d'un *leak* est qu'il faut regarder ce qu'il contient pour savoir combien de délits, au sens pénal, sont caractérisés : Des données à caractère personnel (problème avec le RGPD) ? Des données protégées par le droit d'auteur ? Des secrets d'affaires ? Des données dont le caractère secret (confidentiel) est protégé par la loi ?

Une purge immédiate (ou une anonymisation stricte, par exemple par réalisation d'empreintes cryptographiques) sera nécessaire pour pouvoir conserver légalement ces données d'origine : difficile.

---

[22] Directive n°2016/943 du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016L0943

[23] « La nature est un grand vide qu'il convient de bien combler » disait Bonaparte

[24] Articles L.152-1 à L.152-8 Code de commerce https://legifrance.gouv.fr/codes/section_lc/LEGITEXT000005634379/LEGISCTA000037266547/#LEGISCTA000037266547

[25] « Le vol est la soustraction frauduleuse de la chose d'autrui » article 311-1 du Code pénal https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418127. « Le vol est puni de trois ans d'emprisonnement et de 45 000 euros d'amende » article 311-3 du Code pénal https://legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418131

[26] Article 321-1 du Code pénal « 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. 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 5 ans d'emprisonnement et de 375 000 euros d'amende » https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418234

[27] Cour de cassation chambre criminelle 20 mai 2015 n°14-81.336

6 OSINT ET DROIT DE LA PREUVE

6.1 Des informations ? Oui, mais pour quoi faire ?

L'OSINT regroupe l'ensemble des techniques de recherche et d'analyse d'informations disponibles en sources ouvertes. Oui, mais pour quoi faire : pour servir de preuve ?

L'entreprise qui cherche des informations publiques sur une personne (futur collaborateur ?) ou une entreprise (investisseur potentiel ? Cible pour rachat ? Concurrent anormalement agressif ?) n'a pas besoin de preuve au sens juridique du terme. Cette entreprise souhaite sans doute simplement « savoir », de manière à permettre à un décideur de… décider, en connaissance de cause : oui je recrute la personne (ou pas), oui, je cède des parts à l'investisseur (ou pas), oui, je lance le processus de rachat de l'entreprise cible (ou pas).

Le décideur, via des informations d'origine OSINT, cherche-t-il la vérité (notion éminemment subjective) ou cherche-t-il à prendre une décision « éclairée », en limitant son risque d'erreur (« prendre la bonne décision ») ?

Et d'ailleurs, une « preuve », en droit, qu'est-ce que c'est ? C'est « la démonstration de l'existence d'un fait (…un dommage) ou d'un acte (… un contrat) dans les formes admises ou requises par la loi »[28].

6.2 La preuve en droit pénal

Dans le cadre d'une procédure judiciaire pénale, LA PREUVE EST ABSOLUMENT LIBRE : « Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction. » (article 427 du Code de procédure pénale).

6.3 Idée reçue : « la loyauté de la preuve »

Contrairement à une idée largement répandue, le Code de procédure pénale n'impose nulle part le principe de « loyauté de la preuve ».

Au contraire, la jurisprudence rappelle sans ambiguïté que les « juges répressifs » n'ont pas le pouvoir « d'écarter les moyens de preuve […] obtenus de façon illicite ou déloyale ». La Cour de cassation rappelle ainsi que, quelle que soit l'origine de la preuve, le juge doit seulement « en apprécier la valeur probante »[29].

L'hypothèse la plus courante d'une preuve « illicite ou déloyale » est celle d'une conversation enregistrée sans le consentement de la partie enregistrée. Ce défaut de consentement constitue le délit pénal d'atteinte à la vie privée réprimé par l'article 226-1 du Code pénal.

Mais si cette « preuve » résultant du produit d'un délit pénal peut emporter l'intime conviction du juge, pourquoi des données d'origine OSINT ne le pourraient-elles pas ? Pourquoi un juge réserverait-il un sort différent à des informations « confidentielles » collectées en *open source* ? Pourquoi un juge refuserait-il de prendre en compte les données d'un « *leak* », par définition d'origine *délictueuse* ?

[28] G. Cornu « Vocabulaire juridique » de l'Association Henri Capitant, PUF, 8e édition 2007

[29] Cour de cassation chambre criminelle 15 juin 1993 n°92-82.509

Citons enfin la jurisprudence qui précise que « les impératifs de loyauté et de légalité de la preuve ne s'appliquent pas aux journalistes »[30] puisqu'ils bénéficient de la protection du secret des sources offerte par l'article 109 du Code de procédure pénale.

Il appartient là encore au juge de s'interroger sur la « valeur probante » de preuves fournies par un journaliste, que ces informations soient d'origine *open source* ou non.

Il n'en va pas de même en droit civil où les problématiques de preuve sont apparemment (mais est-ce bien le cas au final ?) plus strictement encadrées par le Code civil.

6.4 La preuve en droit civil

Comme en droit pénal, le principe en droit civil est celui de la liberté de la preuve[31], qu'il s'agisse de prouver un « fait juridique »[32] ou un « acte juridique »[33], pour reprendre la distinction du Code civil.

C'est encore plus vrai en droit commercial, qui énonce que toute forme de preuve est admissible à l'égard d'un « commerçant »[34]. À titre d'exemple, un email suivi du paiement d'une facture peut suffire à prouver l'existence d'un contrat commercial (un acte juridique) que les parties n'auraient pas pris la peine d'écrire ni de signer. D'ailleurs, aujourd'hui encore, de nombreuses professions se dispensent de contrat écrit (commerce de viande en gros, marché de l'art, etc.).

Nous n'insisterons pas sur la preuve d'un acte juridique (d'un contrat) que les techniques d'OSINT n'apporteront en pratique pas souvent. En revanche, les techniques d'OSINT peuvent se révéler extrêmement utiles pour prouver l'existence d'un « fait juridique », d'un « agissement » ou d'un « événement ».

Tout professionnel de la procédure judiciaire civile vous le dira : la meilleure preuve est celle qui provient d'un écrit. Cela s'appelle le « commencement de preuve par écrit »[35], essentiel dans les procédures civiles qui sont elles-mêmes, le plus souvent, écrites. Mais cet impératif ne vaut que pour les « actes juridiques », il est donc de peu d'intérêt pratique pour des recherches en OSINT.

Par réflexe pavlovien, les procéduriers ont tendance à « investir » dans le recours au *sacro-saint* PV d'huissier qui, de par le serment attaché à la profession, devrait apporter un poids supplémentaire dans la constatation de « faits juridiques ». Pourtant, tel n'était pas le cas jusqu'en 2016, lorsque l'ordonnance du 2 novembre 1945 relative au statut des huissiers précisait qu'en matière pénale, les « constatations purement matérielles » d'un huissier n'ont valeur que de « simple renseignement »[36].

---

[30] Cour de cassation chambre criminelle 1er décembre 2020 n°20-82.078

[31] Article 1358 du Code civil « Hors les cas où la loi en dispose autrement, la preuve peut être apportée par tout moyen »

[32] Article 1100-2 du Code civil « Les faits juridiques sont des agissements ou des événements auxquels la loi *[NDLR : ou un contrat]* attache des effets de droit… »

[33] Article 1100-1 du Code civil « Les actes juridiques sont des manifestations de volonté destinées à produire des effets de droit. Ils peuvent être conventionnels ou unilatéraux. Ils obéissent, en tant que de raison, pour leur validité et leurs effets, aux règles qui gouvernent les contrats »

[34] Article L.110-3 du Code de commerce « À l'égard des commerçants, les actes de commerce peuvent se prouver par tous moyens à moins qu'il n'en soit autrement disposé par la loi »

[35] Article 1362 du Code civil « Constitue un commencement de preuve par écrit tout écrit qui, émanant de celui qui conteste un acte (…) rend vraisemblable ce qui est allégué… »

[36] Article 1er Ordonnance n°45-2592 du 2 novembre 1945 relative au statut des huissiers https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000699573

Le magistrat qui instruit (ou qui poursuit) est donc libre d'apprécier la force probante des faits relevés dans un PV d'huissier.

Et il en va de même en matière civile puisque les « constatations purement matérielles d'un huissier font foi jusqu'à preuve du contraire ». Cette preuve contraire peut donc être apportée par tout moyen (pas seulement par PV d'huissier), comme par exemple par des informations d'origine OSINT.

Comme en matière pénale, il appartient au juge civil, confronté à des éléments de preuve qui sembleraient contradictoires (au sens de « *dire le contraire les uns des autres* ») de déterminer celle des preuves qui serait « le plus vraisemblable »[37]. Cette appréciation subjective, qui est du devoir du juge, rejoint la notion de l'intime conviction qu'il appartient au juge pénal (ou au jury d'assises) de se forger.

7 PREMIÈRE CONCLUSION

L'OSINT n'est pas une jungle pour les juristes : comme en toute matière, il existe des règles que tout professionnel doit respecter. Et il est tout à fait possible de faire de l'OSINT de manière légale.

Rappelons le célèbre « nul n'est censé ignorer la loi ». Cet adage n'impose pas à chaque citoyen de connaître l'intégralité des lois existantes (cela n'est pas possible, même pour les juristes). Il signifie, c'est une jurisprudence de la chambre criminelle de la Cour de cassation qui le dit, que « l'ignorance de la loi ne saurait être une cause de justification »[38] permettant d'échapper à une condamnation pénale si vous vous faites « attraper ».

Rappelons enfin que l'entreprise employeur est, sauf cas rarissimes, responsable pénalement et civilement des délits commis par ses salariés dans l'exercice de leur contrat de travail[39].

[37] Article 1368 du Code civil « À défaut de dispositions ou de conventions contraires, le juge règle les conflits de preuve par écrit en déterminant par tout moyen le titre le plus vraisemblable »

[38] Cour de cassation chambre criminelle 4 mars 1986 n°85-93.398 https://www.legifrance.gouv.fr/juri/id/JURITEXT000007065367

[39] Article 121-2 du Code pénal https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006417204

8 FOCUS SUR QUELQUES PROFESSIONS UTILISANT L'OSINT

8.1 OSINT et intelligence économique (IE)

Si le renseignement d'origine sources ouvertes a toujours existé, aux prémices de l'intelligence économique, l'OSINT avait une faible importance et l'information provenait essentiellement d'approches et de sources humaines (ROHUM / HUMINT). Sa démocratisation, liée à la surabondance des données accessibles à travers le web, les bases de données, les réseaux sociaux et les services spécialisés, a donné une nouvelle dimension au secteur de l'intelligence économique. À titre d'illustration, l'accès gratuit aux données du Registre National du Commerce et des Sociétés (RNCS) permis par la loi Macron de 2015, couplé à des outils de cartographie sur la base des informations présente dans le registre, comme en propose Pappers.fr, a très fortement simplifié et amélioré la collecte de renseignement à partir des données légales.

Bien que l'information, qui représente le cœur de métier du renseignement d'affaires, soit techniquement *trouvable* en ligne, la trouver demeure une affaire de spécialistes confrontés à trois défis : la surabondance des sources (qui oblige à chercher une aiguille dans une botte de foin), la potentielle volonté d'une partie de dissimuler une information la concernant (ou d'en véhiculer de fausses) et enfin, la nécessaire maîtrise d'outils permettant d'enrichir des résultats.

Aussi, l'OSINT, ou plutôt la quantité exponentielle d'informations qu'il est désormais possible de trouver publiquement à partir d'un ordinateur, possède une valeur forte qui a considérablement fait évoluer les cabinets d'IE. Historiquement, leur valeur ajoutée a toujours été le renseignement humain, permettant l'accès à une information impossible à obtenir autrement. Dans de nombreux cas, l'OSINT permet désormais de remplacer un travail de renseignement humain, et peut, à tout le moins, l'appuyer.

Cet apport se retrouve dans l'ensemble des activités d'IE qui se découpent en trois grands types de missions :

(i) le renseignement : analyse d'environnement/de risques (état du marché, cartographie d'acteurs) ; appui aux appels d'offres ; couverture des obligations légales, en réalisant des *due diligence*/enquête d'intégrité dans une logique de conformité (compliance) pour répondre au RGPD ou à la loi Sapin II[40] ;

(ii) l'investigation : lutte contre la contrefaçon et la fraude ; recouvrement d'actifs ; appui aux contentieux ; détection et analyse des menaces ;

(iii) la protection de l'information : audits de sécurité et évaluation de l'empreinte numérique sur des personnes morales ou physiques en vue de réduire leur vulnérabilité et exposition en ligne.

Enfin, il n'apparaît pas inutile de rappeler que l'intelligence économique est une activité strictement bornée par le cadre légal, dans laquelle l'espionnage, le piratage et l'usurpation n'ont pas leur place. Le Syndicat Français de l'Intelligence Économique[(41)] (SYNFIE) insiste d'ailleurs sur la dimension éthique de la profession.

(40) https://gouvernement.fr/action/la-loi-pour-la-transparence-l-action-contre-la-corruption-et-la-modernisation-de-la-vie

(41) https://synfie.fr/communique-ieethique

8.2 OSINT et agent de recherches privées (ARP)

La recherche d'information à titre privé est parfaitement légale en France. Mais qu'en est-il lorsqu'on est « enquêteur privé » ? L'OSINT est-il permis aux « détectives privés » ?

En France, la profession d'agent de recherches privées (ou « détective privé ») est réglementée depuis 2012 par le Code de la sécurité intérieure qui en donne la définition suivante[42] : « profession libérale qui consiste, pour une personne, à recueillir, même sans faire état de sa qualité ni révéler l'objet de sa mission, des informations ou renseignements destinés à des tiers, en vue de la défense de leurs intérêts ».

Il est donc tout à fait possible pour un agent de recherches privées de chercher des informations en OSINT, même sous pseudonymat. L'usurpation d'identité, dans le cadre de sa mission, lui est évidemment interdite en application du droit commun[43].

À noter que ne peuvent exercer cette profession que les personnes physiques, sans casier judiciaire, qui bénéficient d'un agrément individuel préalable et d'une carte professionnelle délivrés par le Conseil National des Activités Privées de Sécurité (CNAPS) sous tutelle du ministère de l'Intérieur, doté de mission de surveillance de la profession (suspension/retrait des agréments, etc.).

Il est fait obligation aux agents de recherches privées de disposer d'une assurance de responsabilité professionnelle[44] et tout renouvellement de la carte professionnelle est subordonné « au suivi d'une formation continue ». Depuis 2014, les agents de recherches privées doivent respecter un code de déontologie[45].

Le non-respect des conditions légales d'exercice de la profession est réprimé par de nombreuses dispositions pénales[46].

8.3 OSINT et journalisme

Les journalistes utilisent l'OSINT dans le cadre de leurs investigations, dans la détection, la vérification et l'évaluation d'information (*fact-checking*). Unique moyen d'informer le public (hors communication officielle du pouvoir en place) à une époque où cette information passait principalement par des écrits « papier », la profession de journaliste est encadrée en France depuis 1935 et aujourd'hui par l'article L.7111-3 du Code du travail : « Est journaliste professionnel toute personne qui a pour activité principale, régulière et rétribuée, l'exercice de sa profession dans une ou plusieurs entreprises de presse, publications quotidiennes et périodiques ou agences de presse et qui en tire le principal de ses ressources. »

Ce statut légal permet au journaliste de protéger ses sources d'information (qu'elles soient d'origine OSINT ou pas). Depuis la loi du 4 janvier 2010[47], « le secret des sources des journalistes est protégé dans l'exercice de leur mission d'information du

---

[42] Article L.621-1 du CSI https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000025506411

[43] Article 226-4-1 du Code pénal https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042193593

[44] Article L.622-5 du CSI https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000025506427/2023-02-22

[45] Articles R.631-1 à R.631-3 du CSI
https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000029656358/#LEGISCTA000029658078

[46] Articles L.624-1 à L.624-14 du CSI
https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000025506498/#LEGISCTA000025507396

[47] Loi n°2010-1 du 4 janvier 2010 relative à la protection du secret des sources des journalistes
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000021601325

public », ce qui ne saurait profiter à tout osinteur qui ne disposerait pas d'une carte de presse ou du statut de journaliste.

Cette protection du secret des sources du journaliste professionnel est étendue en matière de procédure pénale qui prévoit, de manière tout à fait dérogatoire, que « …tout journaliste, entendu comme témoin sur des informations recueillies dans l'exercice de son activité, est libre de ne pas en révéler l'origine. »[48]

8.4 ROSO et services de renseignement d'État

Le ROSO pour Renseignement d'Origine Sources Ouvertes (équivalent français du terme anglo-saxon OSINT) est employé historiquement dans les divers services institutionnels de renseignement à travers les époques, en complément de renseignements d'origine humaine, d'origine électromagnétique (ROEM) et de sources fermées (base de données alimentées et gérées par l'État, données bancaires, données d'opérateurs téléphoniques ou de fournisseur d'accès internet, etc.).

L'OSINT s'intègre tout à fait dans cet écosystème car sa pratique suit parfaitement la définition du cycle du renseignement : orientation, recherche, analyse et diffusion. On observe une professionnalisation de la pratique ainsi que des enjeux en matière de souveraineté sur les outils employés par les « services » pour collecter et/ou analyser du signal utile dans un bruit assourdissant de données[49].

D'un point de vue légal, si l'on s'en tient à la définition *stricto sensu* de l'OSINT, sa pratique par des « services de renseignements » ne subit pas d'encadrement spécifique en dehors des lois régissant leurs activités codifiées en majorité dans le Code de la sécurité intérieure. Depuis la loi sur le renseignement du 24 juillet 2015[50], le Conseil d'État et la Commission nationale de contrôle des techniques de renseignement (CNTCR) sont venus combler des espaces vides sur le contrôle et le cadre juridique de l'activité des services de renseignement[51]. Mais cela concerne principalement l'emploi de techniques de renseignement particulières (traduisez par : portant atteinte à la vie privée et à d'autres droits fondamentaux[52]).

Si la pratique de l'OSINT ne semble pas concernée, il n'en demeure pas moins que la collecte et la conservation de données personnelles ainsi que l'accès à des bases de données tombent sous le coup des lois françaises et européennes évoquées précédemment.

Cependant, on observe une réelle volonté de légiférer sur la zone grise du cyberespace et de pratiquer une politique de transparence sur des services pouvant provoquer l'inquiétude de la société civile concernant la surveillance de masse et l'atteinte à la vie privée.

Bien qu'il ne s'agisse pas d'un service de renseignement du premier ni du second cercle, le service de vigilance et de protection contre les ingérences numériques

---

[48] Article 109 du Code de procédure pénale https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006575522

[49] Revue Hérodote N°186 : *Renseigner autrement ? Trajectoires de l'OSINT dans les services de renseignement. Clément Renault, Paul Charon, Fabien Laurençon.*

[50] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement
https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030931899/2021-01-03

[51] Guilhem Marois « Le contrôle des services de renseignement en France » Université de Bordeaux 2019

[52] Articles L.801-1 à L.898-1 du Code de la sécurité intérieure
https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000030934655

étrangères (VIGINUM), créé en 2021[53] et placé sous l'autorité du Premier ministre, fait office d'élève modèle en matière de législation.

Opérant exclusivement sur internet via notamment l'OSINT et participant à la défense de l'intérêt national comme les autres services de renseignement, les textes de loi encadrant la création et l'activité de cette entité sont d'une rare transparence[54].

Le décret encadre et s'aventure même sur un territoire de l'OSINT assez rare et original pour mériter d'être souligné : la création de comptes dédiés sur les réseaux sociaux (de faux comptes de travail, en somme), toujours dans une logique de préciser légalement le champ d'action et le contrôle des activités de VIGINUM, un second décret définit les modalités de collecte automatisée de données et le rôle d'un comité éthique et scientifique[55].

9 OSINT : RÉFLEXIONS AUTOUR DE QUELQUES CAS D'USAGE

9.1 OSINT dans le cadre du *pentest*, du *redteam* et du *phishing* « pédagogique »

Dans le cadre du *pentest* (« test de pénétration » ou « audit de sécurité » d'un système d'information), la recherche d'information en OSINT sur la « cible » est une étape préalable essentielle qui conditionne le bon accomplissement du process dans son ensemble.

À la différence des phases de *découverte active* d'un système d'information (une intrusion au sens des articles 323-1 à 323-3 du Code pénal), la recherche d'information en OSINT sur la « cible » est une phase qui doit rester passive (sans la moindre interaction avec la « cible »). Elle consistera à interroger des sources de données ouvertes comme Censys[56] ou Shodan[57], mais également les réseaux sociaux, par exemple pour identifier des personnes ou des technologies utilisées par l'environnement de la cible. L'objectif avoué de la collecte de ces informations est l'optimisation de la phase d'intrusion par identification préalable de vulnérabilités ou de surfaces d'attaque.

Dans le cas d'un *pentest* correctement encadré par un contrat signé entre le prestataire et le client « cible », l'utilisation des *Google Dorks*[58] est autorisée car l'entreprise a expressément donné son accord pour la recherche, la récupération et l'exploitation des données indexées par Google, alors qu'elles seraient pourtant clairement identifiées comme « confidentielles ». L'auditeur/pentesteur devra bien entendu mettre en œuvre toutes les précautions de stockage de ces informations afin

[53] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043788361

[54] Décret n° 2021-922 du 13 juillet 2021 portant création auprès du SGDSN du service VIGINUM https://www.legifrance.gouv.fr/loda/id/JORFTEXT000043788361

[55] Décret n° 2021-1587 du 7 décembre 2021 portant autorisation d'un traitement automatisé de données à caractère personnel dans le but d'identifier les ingérences numériques étrangères https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044454057

[56] https://censys.io

[57] https://www.shodan.io

[58] Un *Google Dork* est une astuce de recherche permettant d'accéder à des ressources qui ne sont pas censées être indexées par le moteur de recherche. Voir https://www.exploit-db.com/google-hacking-database

de préserver la confidentialité des données (*qui sont pourtant techniquement librement accessibles…*).

Dans le cadre d'une prestation de *phishing*[59] ou de *social engineering*[60] à des fins pédagogiques[61], l'utilisation de l'OSINT est nécessaire afin de pouvoir contextualiser les supports utilisés (par exemple en faisant référence à l'actualité sociale d'une entreprise pour créer un email de phishing efficace) et paraître ainsi le plus crédible possible pour la « cible ». En revanche, au-delà du Code pénal, ce sont bien les bonnes pratiques du métier qui vont définir certaines lignes à ne pas dépasser. Pour pouvoir mener ce type de tests, les salariés doivent être prévenus du déroulement d'un test de type *phishing* ou *redteam*.

Les données personnelles collectées en OSINT lors de prestations de *pentest* ou de *redteam* doivent respecter le RGPD et :

- soit être collectées sous forme d'échantillon représentatif (solution idéale mais juridiquement dangereuse sans information préalable des personnes concernées) ;
- soit faire l'objet d'une stricte et immédiate anonymisation[62].

Les données OSINT collectées doivent être mentionnées au rapport de *pentest* et réversibles : le processus d'obtention (outils et sources) doit être décrit en détail. Si les sources se doivent d'être librement accessibles (*par nature dans le cas d'une recherche en OSINT*), les outils logiciels utilisés peuvent reposer sur une licence « *open source* » ou commerciale (pour les logiciels dits propriétaires).

On considère cependant aujourd'hui que, dans les bonnes pratiques, toute donnée concernant une entreprise et collectée à sa demande (que la source soit ouverte ou non) bénéficie à cette dernière dans le cadre d'un audit de sécurité.

Il est donc admissible de requêter et utiliser des sources non ouvertes à partir du moment où l'intérêt de l'entreprise signataire est l'objectif de traitement, et que les données ne contreviennent pas au droit pénal ni au droit du travail.

9.2 OSINT comme aide à la recherche de personnes disparues

La pratique de l'OSINT peut concourir à la recherche de personnes disparues, sans remplacer la procédure judiciaire légale de signalement de « disparition inquiétante ».

Les personnes intéressées peuvent se rapprocher de l'association Assistance et Recherche de Personnes Disparues (ARPD)[63]. Cette association aide les familles à retrouver des proches disparus et mobilise ses bénévoles pour effectuer des recherches. Son actuel président est un ancien commissaire de police.

---

(59) Le *phishing* est une technique d'attaque consistant à envoyer un faux courrier électronique à une ou plusieurs personnes dans un but d'incitation à cliquer sur un lien malveillant redirigeant généralement sur une imitation d'un site légitime. L'objectif étant de tromper la cible dans le but de collecter des informations sensibles

(60) Le *social engineering* consiste à obtenir des informations sensibles par tromperie via des canaux comme le téléphone ou l'email

(61) Par exemple pour répondre aux obligations légales de sensibilisation aux risques numériques prévues dans la directive UE n°2022/2555 "NISv2" du 14 décembre 2022 sur la sécurité des réseaux et des systèmes d'information https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=fr ou dans le règlement UE "DORA" n°2022/2554 sur la résilience opérationnelle du secteur financier (encore) du 14 décembre 2022 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022R2554

(62) Référentiel CNIL « L'anonymisation de données personnelles » 19 mai 2020 https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles

(63) https://www.arpd.fr

L'association est bien consciente des limites. Elle organise d'ailleurs des formations à destination de ses bénévoles.

Toutefois, rappelons qu'en France, une personne majeure a le droit de « disparaître » de son environnement professionnel ou familial.

9.3 OSINT en milieu criminel

Le caractère clandestin de l'activité criminelle fait de l'enquête en sources ouvertes de ce milieu une pratique d'une part intrinsèquement liée au décodage de l'obfuscation de cette activité, et d'autre part à l'obtention d'accès à des cercles fermés ou semi-fermés sur les différents réseaux sociaux, forums, et groupes de conversations en ligne. Tout ceci avec l'objectif, pour l'enquêteur, d'avoir accès à du « contenu illicite ».

L'accès à ces espaces est souvent conditionné à une interaction avec un acteur du milieu. Il va de soi que si la condition d'accès à un groupe de discussion est de s'incriminer, par exemple en commandant un produit, l'enquêteur ne disposant pas des habilitations nécessaires se voit passible de poursuites pénales. Quant aux groupes ouverts ou partiellement ouverts, il n'est pas rare que la condition d'accès ne se cantonne qu'à une discussion avec un de ses membres. Pourtant, le simple fait de discuter avec un membre dans l'objectif d'entrer dans un groupe de discussion criminel est passible de poursuites. En effet, la notion d'association de malfaiteurs définie par l'article 450-1 du Code pénal est une infraction « obstacle » : l'objectif de cet article est de pouvoir entamer des poursuites avant qu'une infraction se produise. Le simple fait de tenter de pénétrer un groupe criminel est[64] donc un élément qui permet de caractériser une entente entre plusieurs individus en vue de commettre un crime ou un délit.

Concernant les contenus eux-mêmes, bien que l'OSINT, en soi, ne soit pas une activité pénalement répréhensible, la consultation en ligne de « contenus » illicites reste un délit (ex : article 227-23 du Code pénal pour la « représentation d'un mineur à caractère pornographique »). Le législateur admet néanmoins un principe de « sérendipité »[65] : consulter un contenu illicite de manière fortuite et involontaire n'est généralement pas qualifié de délit, puisque l'élément moral (l'intentionnalité) est nécessaire au déclenchement de l'action publique (article 121-3 du Code pénal). Cela dit, le principe de sérendipité ne saurait s'appliquer à une activité répétée dans le temps. Il est donc possible de considérer que toutes les activités d'OSINT en milieu criminel, en vertu du caractère intentionnel et habituel d'une enquête classique de police judiciaire en sources ouvertes[66], sont considérées comme des délits.

Nonobstant ce principe, le début de l'action publique ou son extinction restent à l'usage du ministère public : le parquet se réserve le droit de qualifier ou de requalifier une infraction. En effet, dans certains cas précis, l'autorité publique peut considérer que la consultation de contenu illicite n'entre pas dans un cadre délictuel sous réserve de certaines conditions.

---

[64] Au sens de l'article 450-1 du Code pénal : « Constitue une association de malfaiteurs tout groupement formé ou entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'un ou plusieurs crimes ou d'un ou plusieurs délits punis d'au moins cinq ans d'emprisonnement. Lorsque les infractions préparées constituent des crimes ou des délits punis de dix ans d'emprisonnement, la participation à une association de malfaiteurs est punie de dix ans d'emprisonnement et de 150 000 euros d'amende. Lorsque les infractions préparées sont des délits punis d'au moins cinq ans d'emprisonnement, la participation à une association de malfaiteurs est punie de cinq ans d'emprisonnement et de 75 000 euros d'amende"

[65] https://fr.wikipedia.org/wiki/Sérendipité « La sérendipité est le fait de faire par hasard une découverte inattendue qui s'avère ensuite fructueuse »

[66] Hors habilitations particulières. (Voir définition page 27)

C'est ainsi que des journalistes ou des chercheurs et chercheuses en criminologie ont pu approcher le monde criminel et consulter du « contenu » illicite sans sanctions pénales. Bien que cela reste à l'appréciation du parquet, il est possible de supposer que ces dispositions particulières sont bien liées au statut de scientifique ou de journaliste de l'enquêteur et ne sauraient s'appliquer au seul principe que le mis en cause réalisait une enquête en sources ouvertes.

Outre les dangers propres aux activités clandestines du monde criminel, l'enquêteur en sources ouvertes ne dispose pas des autorisations nécessaires et se retrouve alors également en péril d'un point de vue pénal. Non seulement la nature même des contenus consultés lors de l'enquête est illicite, mais la pratique du SOCMINT actif en milieu criminel est également caractérisable comme un délit en soi.

9.4 OSINT au service du recrutement

Vous êtes recruteur et vous souhaitez vérifier, compléter, les informations fournies habituellement par un candidat, telles que CV, lettre de motivation, lettre de recommandation… Cette collecte d'information, autrefois essentiellement effectuée par téléphone, est dorénavant, avec l'avènement d'internet, enrichie par de nombreuses autres possibilités. La facilité d'accès à ces informations peut faire oublier qu'il existe des règles. La collecte par un recruteur d'informations publiées par un candidat sur internet constitue un traitement de données à caractère personnel même si elles sont « *open source* ».

Le législateur a encadré cette pratique par diverses itérations. Le point de départ est dans le Code civil avec l'article 9 relatif au respect de la vie privée[(67)], en vigueur depuis le 19 juillet 1970. Il est suivi par la Convention européenne des droits de l'homme et son article 8[(68)]. Il faudra attendre 2008 pour que le Code du travail s'empare du sujet avec l'article L1221-6[(69)]. Enfin, le règlement général sur la protection des données [(70)] – RGPD entre en action en 2018 et vient compléter ce dispositif réglementaire.

Grand principe : la protection de la vie privée, qui est due à tout citoyen. Les limites deviennent assez rapidement floues, une information peut être publiée à la vue de tous sur internet (Facebook) et relever de la vie privée.

Un élément aussi « privé » que l'accord salarial entre un employé et un employeur peut devenir un élément de preuve, porté à la connaissance de tiers. Arrêt n° 231 FS-B de la Cour de cassation, chambre sociale, du 8 mars 2023 : « La cour d'appel a relevé que […] la salariée était bien fondée à obtenir la communication des bulletins de salaires de huit autres salariés occupant des postes de niveau comparable au sien […] ». Il convient donc de choisir ses sources de recherches avec soin, conformément à la finalité de l'enquête.

Encadrement plus spécifique, le droit du travail : « Les méthodes et techniques d'aide au recrutement ou d'évaluation des candidats à un emploi doivent être pertinentes au regard de la finalité poursuivie. » .
Tout va se jouer dans la définition de cette finalité et l'évaluation de la pertinence.

---

(67) Article 9 du code civil (droit au respect de la vie privée), légifrance.fr

(68) Articles 8 de la Convention européenne des droits de l'homme et des libertés fondamentales (droit au respect de la vie privée et familiale), echr.coe.int

(69) Articles L.1221-6 et suivants du code du travail (finalités, pertinence des données, et information préalable des candidats dans le cadre de recrutement), légifrance.fr

(70) Articles 4.2, 12, 13 et 14 du RGPD, cnil.fr

L'OSINT peut entrer dans cette définition mais on indiquera son utilisation et les limites imposées et respectées.

Nous avons vu que ces collectes sont réalisées à des fins de traitement de données à caractère personnel. Il faudra donc, même si elles sont issues d'une méthodologie OSINT, leur appliquer avec rigueur toutes les recommandations de la CNIL sur les durées et conditions de conservation et de sécurisation.

Enfin, il ne faut pas oublier l'obligation d'information et de recueil du consentement préalable des candidats de la consultation de ses informations personnelles diffusées en ligne. Ceci afin qu'ils puissent exercer leur droit d'accès, de rectification, d'opposition et de suppression des informations collectées.

En conclusion, l'utilisation de la technique de l'Open Source Intelligence (OSINT) pour vérifier les antécédents des candidats est une méthode précieuse et efficace pour les entreprises. En exploitant les outils OSINT, les organisations peuvent acquérir une compréhension globale des antécédents, des compétences et de l'adéquation d'un candidat pour un poste donné.

Cependant, cette pratique doit être strictement encadrée. Afin d'aider les recruteurs à protéger la vie privée des candidats et à se conformer aux lois et règlements en vigueur, la CNIL a publié le 30 janvier 2023 un guide intitulé « Recrutement - Les fondamentaux en matière de protection des données personnelles »[(71)].

[(71)] https://www.cnil.fr/sites/default/files/atoms/files/guide_-_recrutement.pdf

10 POINTS DE REPÈRE

10.1 Checklist & questions à se poser AVANT une enquête OSINT

Voici les principales questions à se poser AVANT de pratiquer une enquête OSINT :

- ☐ Ai-je un **accès légitime** aux données ? *(accès dans un STAD, lettre de mission…)*
- ☐ Les données sont-elles de **provenance légitime** ? *(leak, fuites de données…)*
- ☐ Ai-je le droit de **copier et d'utiliser** cette information ? *(CGU, propriété intellectuelle…)*
- ☐ L'information ne comporte-t-elle pas d'indication manifeste qu'elle est **confidentielle** ?
- ☐ Si je révèle cette information publiquement, je m'assure de ne pas risquer de **nuire** à quelqu'un ? *(doxing)*
- ☐ Suis-je en mesure de **sourcer** chaque élément ?
- ☐ Est-ce possible que quelqu'un d'autre puisse **refaire** le processus/cheminement jusqu'à l'information trouvée ? *(réversibilité de la méthode, des pivots)*
- ☐ Est-ce que l'ensemble des cases de cette checklist sont bien cochées ? Si oui, je peux démarrer mon investigation en toute **sérénité** !

Il est donc important de comprendre la nature de l'information recueillie, mais également le contexte dans lequel vous allez la restituer. Si vous constatez des crimes ou délits durant votre investigation, signalez-le aux autorités compétentes (cf paragraphe suivant).

Pour conclure, n'oubliez pas qu'il y a une différence entre ce qui est juste et ce qui est légal ! On ne gagne jamais à vouloir se faire justice soi-même. Privilégions une pratique légale et éthique de l'OSINT.

10.2 Vous êtes témoin d'une activité illégale

Si lors de vos recherches, vous êtes témoin ou constatez une activité illégale, vous pouvez communiquer au procureur de la République les éléments dont vous disposez. Si vous constatez un **danger grave et imminent** sur une personne, vous avez l'obligation de prévenir l'autorité judiciaire, sous peine de risquer une accusation pour non-assistance à une personne en péril[72] ou de commettre le délit de non-dénonciation de crime[73].

Vous pouvez, par exemple, signaler les activités illégales que vous constatez, via internet sur la plateforme Ma Sécurité[74]. Les tentatives d'arnaques cyber peuvent aussi être dénoncées sur la plateforme PHAROS[75] ou sur la plateforme cybermalveillance[76].

---

[72] Délit pénal de non-assistance à personne en péril article 223-6 du Code pénal
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037289588

[73] Délit pénal de non dénonciation de crime article 434-1 du Code pénal
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032207673

[74] https://www.masecurite.interieur.gouv.fr

[75] « Signaler un contenu suspect ou illicite avec PHAROS » https://www.internet-signalement.gouv.fr/PharosS1

[76] https://www.cybermalveillance.gouv.fr

11 GLOSSAIRE

.Onion : « .onion » est un suffixe de domaine de premier niveau réservé aux sites web hébergés sur le réseau Tor, qui est un réseau informatique décentralisé conçu pour permettre aux utilisateurs de naviguer sur Internet de manière anonyme et sécurisée.

ANSSI : Créée en 2009, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) est l'autorité française responsable de la sécurité informatique et de la cybersécurité. Elle est chargée de la protection des systèmes d'information de l'État et des entreprises vitales, ainsi que de la lutte contre les cybermenaces.

Audits de sécurité : Les audits de sécurité sont des examens systématiques et méthodiques des systèmes informatiques et des réseaux pour identifier les vulnérabilités, les menaces et les risques de sécurité. L'objectif de ces audits est de détecter les failles de sécurité afin de les corriger et de renforcer la sécurité globale du système.

Base de données : Une base de données est un ensemble de données organisées et structurées qui peuvent être stockées, consultées et mises à jour de manière efficace. Les bases de données sont utilisées pour stocker une grande quantité d'informations, telles que des noms, des adresses, des numéros de téléphone, etc.

CNIL : Créée en 1978, la CNIL (Commission nationale de l'informatique et des libertés) est une autorité administrative indépendante française chargée de veiller à la protection des données personnelles. Elle est responsable de la réglementation de la collecte, du traitement et de la conservation des données à caractère personnel en France.

Compliance : La conformité (compliance en anglais) désigne le respect des lois et des règles en vigueur dans un domaine spécifique, tel que la conformité fiscale, la conformité réglementaire ou la conformité à la sécurité des données.

Crime : Un crime est une violation grave de la loi qui est punie par la justice. Les crimes peuvent inclure des actes tels que le meurtre, le viol, le vol, etc.

Criminologie : La criminologie est l'étude scientifique des crimes, des délinquances, de la justice pénale et de la prévention du crime.

Cyber : Le terme cyber fait référence à tout ce qui concerne l'informatique, les réseaux, Internet et les technologies numériques en général. Le préfixe cyber est souvent utilisé pour qualifier des termes tels que cybercriminalité, cybersécurité, cyberattaques, etc.

Cyberespace : Le cyberespace est l'environnement numérique où les communications électroniques ont lieu. Il englobe tous les réseaux, les systèmes informatiques, les serveurs et les dispositifs connectés qui permettent aux utilisateurs de communiquer et de partager des informations.

Data : Le terme data (données en français) fait référence à des informations numériques, telles que des fichiers, des documents, des images, des vidéos, etc. Les données sont souvent stockées et traitées dans des bases de données ou sur des serveurs informatiques.

Délit : Le délit est une infraction pénale qui est considérée comme moins grave qu'un crime. Les délits sont généralement punis par des amendes ou des peines de prison moins sévères que celles appliquées aux crimes.

Données à caractère personnel : Les données à caractère personnel (DCP) sont des informations qui permettent d'identifier directement ou indirectement une personne physique. Les exemples courants de DCP incluent les noms, les adresses, les numéros de téléphone, les adresses e-mail, les numéros d'identification fiscale, etc. Les DCP sont soumises à des règles strictes de protection de la vie privée dans de nombreuses juridictions.

Doxing : Le doxing est une pratique consistant à rechercher et à publier des informations personnelles sur une personne, généralement dans le but de nuire à sa réputation ou de la harceler. Le doxing peut inclure la publication de données sensibles telles que l'adresse, le numéro de téléphone, les informations bancaires, les antécédents criminels ou toute autre information pouvant être utilisée pour causer du tort à la personne.

Due diligence : La due diligence est un processus d'examen et d'analyse approfondi d'une entreprise, d'une organisation ou d'un individu avant de conclure un accord ou une transaction. Ce processus peut inclure des vérifications de crédit, des enquêtes de sécurité, des audits financiers, des évaluations de risques et des examens juridiques pour s'assurer que toutes les informations pertinentes ont été examinées avant de prendre une décision.

Empreinte cryptographique : Une empreinte cryptographique, également appelée « hash », est une série de caractères aléatoires générée par un algorithme de hachage. Elle représente une version numérique unique et condensée d'un fichier ou d'un document, qui peut être utilisée pour vérifier l'intégrité des données et s'assurer qu'elles n'ont pas été altérées.

Empreinte numérique : L'empreinte numérique, également appelée « empreinte digitale », est une trace numérique laissée par une personne ou une entreprise sur Internet, qui peut inclure des informations telles que les adresses IP, les historiques de navigation, les commentaires en ligne, les profils de réseaux sociaux, etc.

Fact-checking : Le fact-checking est un processus de vérification des faits et des informations, généralement en lien avec les actualités, les médias et la politique. Il s'agit d'un processus de recherche et de vérification des informations pour s'assurer de leur véracité avant de les publier ou de les partager.

Fuite : une fuite se produit lorsqu'une information ou des données confidentielles sont divulguées de manière non autorisée. Les fuites peuvent provenir de sources internes ou externes, et peuvent être causées par des erreurs humaines, des cyberattaques ou des violations de sécurité.

Google dorks : Google dorks ou dorking est un terme qui désigne des requêtes de recherche avancée utilisées pour trouver des informations sensibles qui ne sont pas censées être accessibles via une recherche basique sur un moteur de recherche.

Groupe de conversation en ligne : un groupe de conversation en ligne est une plateforme qui permet à plusieurs personnes de communiquer entre elles en temps réel via Internet. Les groupes de conversation peuvent prendre la forme de chats, de forums de discussion ou de réseaux sociaux, et sont utilisés pour des activités telles que la collaboration professionnelle, la planification d'événements ou simplement pour socialiser.

Hash : en informatique, un hash (ou hachage) est une fonction mathématique qui convertit une chaîne de données en une valeur numérique unique. Les hash sont souvent utilisés pour stocker des mots de passe de manière sécurisée, car il est difficile (voire impossible) de reconstruire la chaîne de données à partir du hash. Les hash sont également utilisés dans des algorithmes de vérification d'intégrité de données pour garantir que les données n'ont pas été altérées pendant la transmission ou le stockage.

HTTP : HTTP (Hypertext Transfer Protocol) est un protocole de communication utilisé pour le transfert de données sur le Web. Il permet aux navigateurs Web et aux serveurs Web de communiquer entre eux pour récupérer des ressources telles que des pages Web, des images et des vidéos.

HUMINT : HUMINT (Human Intelligence) est un terme utilisé pour décrire la collecte de renseignements en utilisant des sources humaines. Il s'agit d'une méthode d'espionnage qui implique l'utilisation d'agents, d'informateurs et d'autres sources humaines pour recueillir des informations sur des sujets spécifiques.

Intelligence Économique (IE) : L'intelligence économique est une discipline qui vise à collecter, analyser et exploiter des informations stratégiques pour aider les entreprises à prendre des décisions éclairées en matière de stratégie et de développement économique. L'IE peut inclure la collecte d'informations sur les marchés, les concurrents, les partenaires commerciaux et les tendances économiques.

Intrusion : une intrusion est une tentative non autorisée d'accéder à un système informatique ou à des données sensibles. Les intrusions peuvent être causées par des hackers, des virus informatiques, des employés malveillants ou d'autres acteurs malveillants qui cherchent à compromettre la sécurité d'un système informatique.

Leak : un leak est une fuite d'informations ou de données sensibles qui sont divulguées de manière non autorisée. Les leaks peuvent être causés par des erreurs humaines, des cyberattaques ou des violations de sécurité et peuvent avoir des conséquences graves pour les individus ou les organisations touchées.

Obfuscation : l'obfuscation est une technique utilisée pour rendre le code informatique plus difficile à comprendre pour les humains, tout en conservant sa fonctionnalité. Cette technique est souvent utilisée pour protéger la propriété intellectuelle, empêcher l'ingénierie inverse et renforcer la sécurité en rendant plus difficile la compréhension du code par les pirates informatiques.

Open data : Open data (ou données ouvertes) désigne des données accessibles au public et réutilisables, souvent publiées par des organisations gouvernementales, des entreprises ou des organisations à but non lucratif. Ces données sont souvent disponibles gratuitement, et peuvent être utilisées pour créer des applications, des analyses de données et des visualisations pour le bénéfice du public.

Osinteur : (néologisme) un Osinteur est une personne qui se spécialise dans l'utilisation de l'OSINT (Open Source Intelligence), c'est-à-dire la collecte et l'analyse de renseignements à partir de sources publiques, telles que les réseaux sociaux, les sites Web, les forums de discussion et les publications en ligne.

Pentest : un Pentest (ou test d'intrusion) est une méthode de test de sécurité informatique utilisée pour évaluer la vulnérabilité d'un système informatique en simulant une attaque de hacker. Les tests d'intrusion sont généralement réalisés par des professionnels de la sécurité informatique et peuvent aider les organisations à identifier les failles de sécurité et à mettre en place des mesures de protection.

Phishing pédagogique : le phishing pédagogique est une technique de formation utilisée pour sensibiliser les utilisateurs à la sécurité informatique en simulant une attaque de phishing. Cette technique implique l'envoi d'e-mails de phishing simulés à des employés pour leur apprendre à reconnaître et à éviter les tentatives de phishing réelles.

Pivot : lors de l'analyse, une information « pivot » ou « rebond » peut apparaître. Il s'agit d'une donnée qui permet d'accéder à une nouvelle information afin de réaliser plus de recherche sur certains points d'intérêts.

Premier cercle : Les services spécialisés de renseignement, dits du « premier cercle », sont :

- la direction générale de la sécurité extérieure (DGSE) ;
- la direction du renseignement et de la sécurité de la défense (DRSD) ;
- la direction du renseignement militaire (DRM) ;

- la direction générale de la sécurité intérieure (DGSI) ;
- le service à compétence nationale dénommé « direction nationale du renseignement et des enquêtes douanières » (DNRED) ;
- le service à compétence nationale dénommé « traitement du renseignement et action contre les circuits financiers clandestins » (Tracfin).

À l'exception de la DRM et de Tracfin, les services du premier cercle ont la faculté de recourir à l'ensemble des techniques de renseignement.

Pseudonymat : Le pseudonymat est l'utilisation d'un pseudonyme ou d'un nom d'emprunt pour protéger l'identité d'une personne. Le pseudonymat permet à une personne de rester anonyme tout en communiquant avec d'autres personnes sur Internet ou dans d'autres domaines où l'identité réelle n'est pas nécessaire.

Recel : Le recel est le fait de cacher, de détenir ou de revendre des biens volés ou acquis de manière illégale en sachant qu'ils ont été volés ou acquis de manière illégale. Le recel est considéré comme un crime dans la plupart des pays.

Redteam : Le redteam est une approche globale des risques sur l'entreprise, incluant le risque informatique (pentesting), le risque humain (phishing, social engineering), le risque physique (intrusions) et le risque wireless (Wifi) - Voir https://www.linkedin.com/pulse/quest-ce-que-le-red-team-julien-m%25C3%25A9tayer/

RGPD : Le RGPD (Règlement Général sur la Protection des Données) est une loi européenne qui a été adoptée en mai 2018 pour renforcer la protection des données personnelles des citoyens de l'Union européenne. Le RGPD établit des règles pour la collecte, le traitement et le stockage des données personnelles, et oblige les entreprises à obtenir le consentement des utilisateurs pour utiliser leurs données.

ROEM : Le renseignement d'origine électromagnétique ou ROEM (en anglais : signals intelligence ou SIGINT).

ROHUM : Renseignement d'Origine HUMaine : traduction française d'HUMINT.

ROSO : Renseignement d'Origine Source Ouverte : traduction française d'OSINT.

Second cercle : Les services, dits du « second cercle », sont désignés par décret en Conseil d'État pris après avis de la CNCTR. Ils relèvent aujourd'hui des ministres de la défense, de l'intérieur et de la justice, et peuvent se voir confier des missions de renseignement. Ils ne peuvent avoir recours qu'à certaines techniques pour certaines finalités seulement.

Les services du second cercle sont :

- l'unité de coordination de la lutte antiterroriste, certains services de la direction centrale de la police judiciaire, certains services de la direction centrale de la police aux frontières, certains services de la direction centrale de la sécurité publique,
- certains services de la direction des opérations et de l'emploi ainsi que les sections de recherche,
- à la préfecture de police de Paris : certains services de direction du renseignement, certains services de la direction régionale de la police judiciaire, certains services de la direction de la sécurité de proximité de l'agglomération de Paris ;
- les sections de recherches de la gendarmerie maritime, de la gendarmerie de l'air et de la gendarmerie de l'armement ;
- certains services de la direction de l'administration pénitentiaire.

Sérendipité : La sérendipité est un concept qui se réfère à la capacité de découvrir des choses inattendues ou des opportunités fortuites grâce à un concours de circonstances imprévues, souvent par hasard ou par accident. Cela peut se produire lors de recherches ou d'expériences scientifiques, dans les domaines de la créativité, de l'innovation ou même de la vie quotidienne.

Social engineering : Le social engineering est une technique de manipulation psychologique utilisée pour obtenir des informations confidentielles ou un accès non autorisé à des systèmes informatiques, en exploitant la confiance, la naïveté ou la vulnérabilité des individus. Cette technique peut impliquer l'utilisation de l'ingénierie sociale pour obtenir des informations à partir de sources humaines, telles que des employés ou des utilisateurs d'un système, ou des tactiques de phishing et de spamming.

SOCMINT : SOCMINT (Social Media Intelligence) est une forme de collecte et d'analyse de renseignements qui se concentre sur les données publiques disponibles sur les réseaux sociaux, les forums en ligne et les blogs. Les analystes de SOCMINT utilisent des outils de surveillance pour collecter des informations sur les tendances, les opinions et les comportements des utilisateurs de ces plateformes, dans le but de comprendre les comportements sociaux et de prédire les évolutions futures.

Source ouverte : les sources d'informations légalement accessibles à tout un chacun. Il est important de noter que l'accès à ces sources peut être parfois payant.

Système d'information (SI) : Un système d'information (SI) est un ensemble organisé de ressources (personnes, matériel, logiciels, données et procédures) qui permettent de collecter, stocker, traiter et diffuser des informations au sein d'une organisation. Les systèmes d'information sont souvent utilisés pour automatiser les processus opérationnels, améliorer la prise de décision et faciliter la communication entre les différents acteurs d'une organisation.

TTP : TTP est l'acronyme de Tactics, Techniques and Procedures, soit tactiques, techniques et procédures en français. Les TTP sont des méthodes et des stratégies utilisées par les cybercriminels, les hackers ou les groupes d'espionnage pour mener à bien leurs attaques. Les TTP incluent des techniques d'ingénierie sociale, des vulnérabilités d'exploitation, des outils malveillants et des tactiques d'évasion.

Vulnérabilité : Une vulnérabilité est une faiblesse ou une lacune dans un système informatique qui peut être exploitée par des attaquants pour compromettre la sécurité du système. Les vulnérabilités peuvent être liées à des erreurs de conception, des bogues de logiciel ou des configurations inadéquates. Il est important de repérer et de corriger les vulnérabilités pour réduire le risque d'attaques informatiques.

12 CONTRIBUTEURS

Ont œuvré à la rédaction de ce livre blanc (dans l'ordre alphabétique) :

- Yoan Blanc, freelance OSINT
- Steven Deffous, formateur et analyste dans un cabinet d'intelligence économique
- Pascale Duc, rédactrice web SEO et correctrice
- Christian Harbulot, directeur de l'École de Guerre Économique (EGE) et du Centre de Recherche 451
- Artus Huot de Saint-Albin, formateur et responsable OSINT dans un cabinet d'intelligence économique
- Vincent Le Bouar, agent de recherches privées
- Marc-Antoine Ledieu, avocat à la cour et RSSI
- Marshall, étudiant en criminologie
- Alexis Martins, étudiant en cybersécurité
- Amandine Metayer, responsable communication
- Julien Metayer, hacker éthique, pentester
- Yann Pilpré, consultant en cybersécurité et gestion des risques
- Émilie Musso-Pouffier-Thompson, docteure en droit

… et tous les « John Doe » ayant souhaité rester anonymes pour leur apports et relecture.

Pour toutes questions ou suggestions d'amélioration :

question@technique-et-droit-du-numerique.fr

osint-veille-bureau@aege.fr

info@ozint.eu