

OSINT

Quels enjeux juridiques ?

L'OSINT en quelques mots



L'OSINT en quelques mots

L'objectif principal de l'OSINT est de **compiler des données disparates pour en tirer des conclusions utiles**, que ce soit, par exemples, pour la sécurité nationale, la cybersécurité, les enquêtes journalistiques ou les recherches privées.

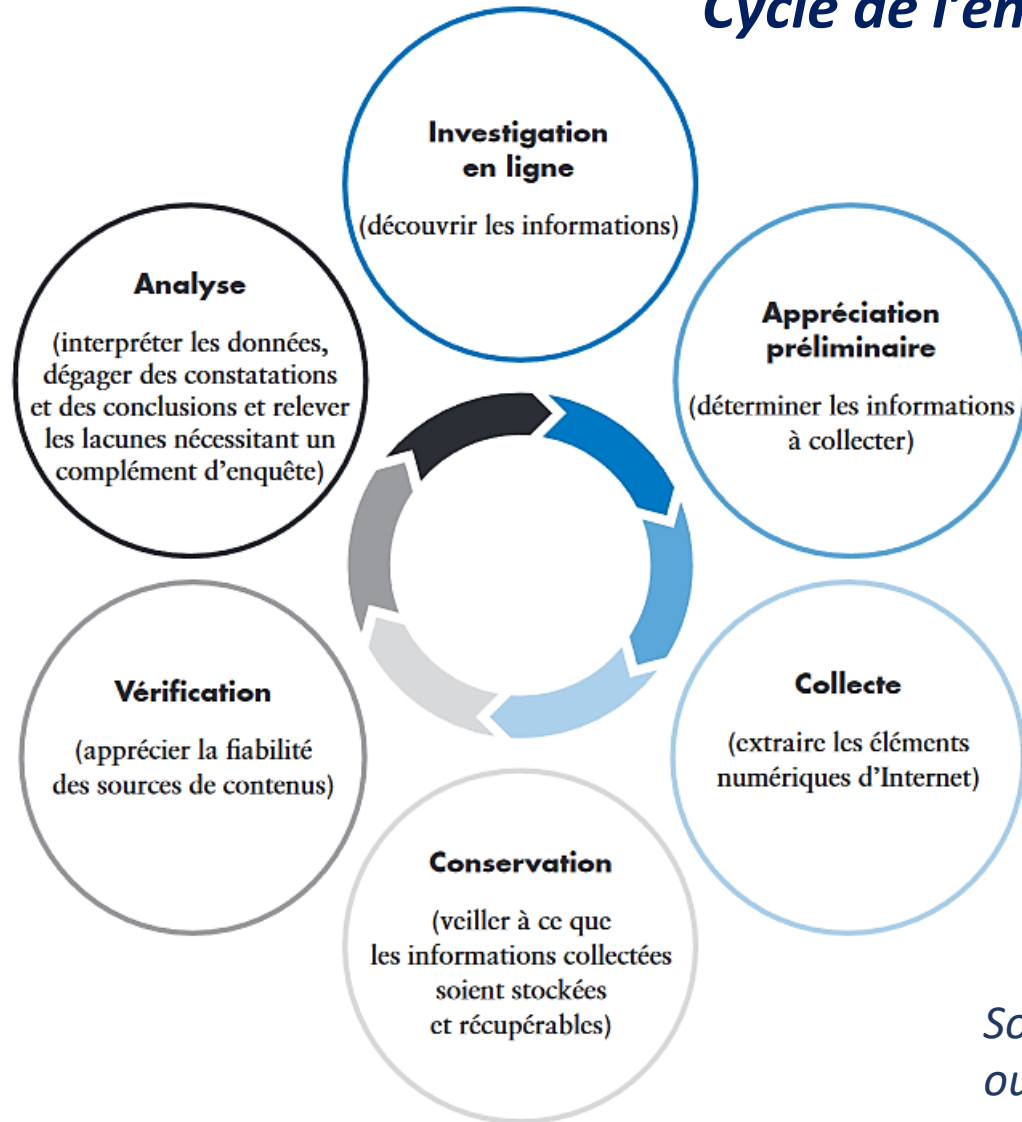
Les techniques d'OSINT permettent notamment de **détecter des failles de sécurité** ou de **rassembler des preuves** dans le cadre de litiges.

Les techniques faisant appel à de l'OSINT sont utilisées dans de nombreux domaines :

- Dans le cadre d'enquête sur la manipulation de l'opinion publique et la lutte contre les opérations de désinformation
- Pour identifier des **menaces, des vulnérabilités** voire des **auteurs d'une cyberattaque** (par la collecte d'adresses IP utilisées et en recoupant des informations)

L'OSINT en quelques mots

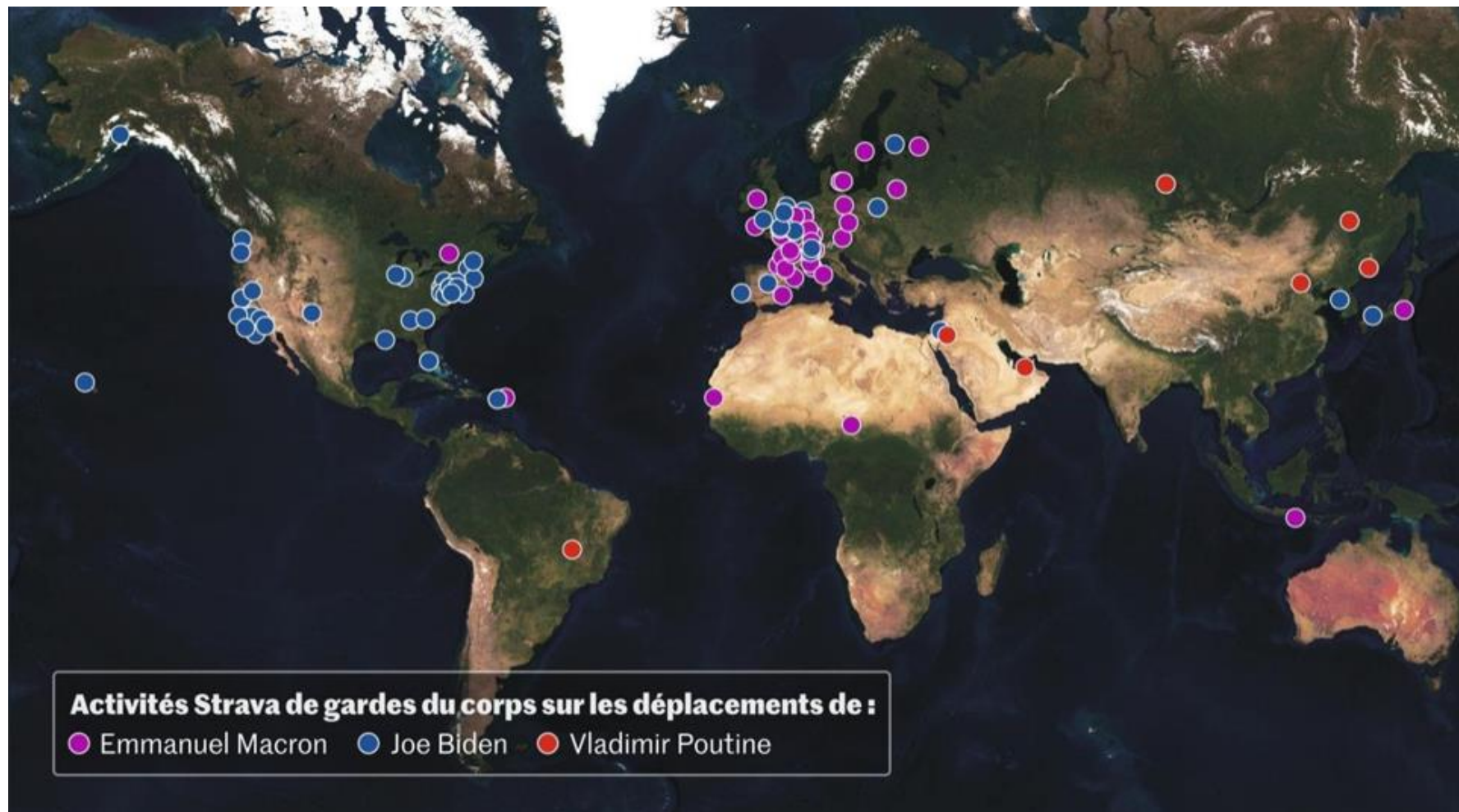
Cycle de l'enquête en sources ouvertes



« Les enquêtes en sources ouvertes se fondent entièrement ou partiellement sur des informations accessibles au public pour mener des recherches en ligne à caractère formel et systématique sur des agissements présumés »

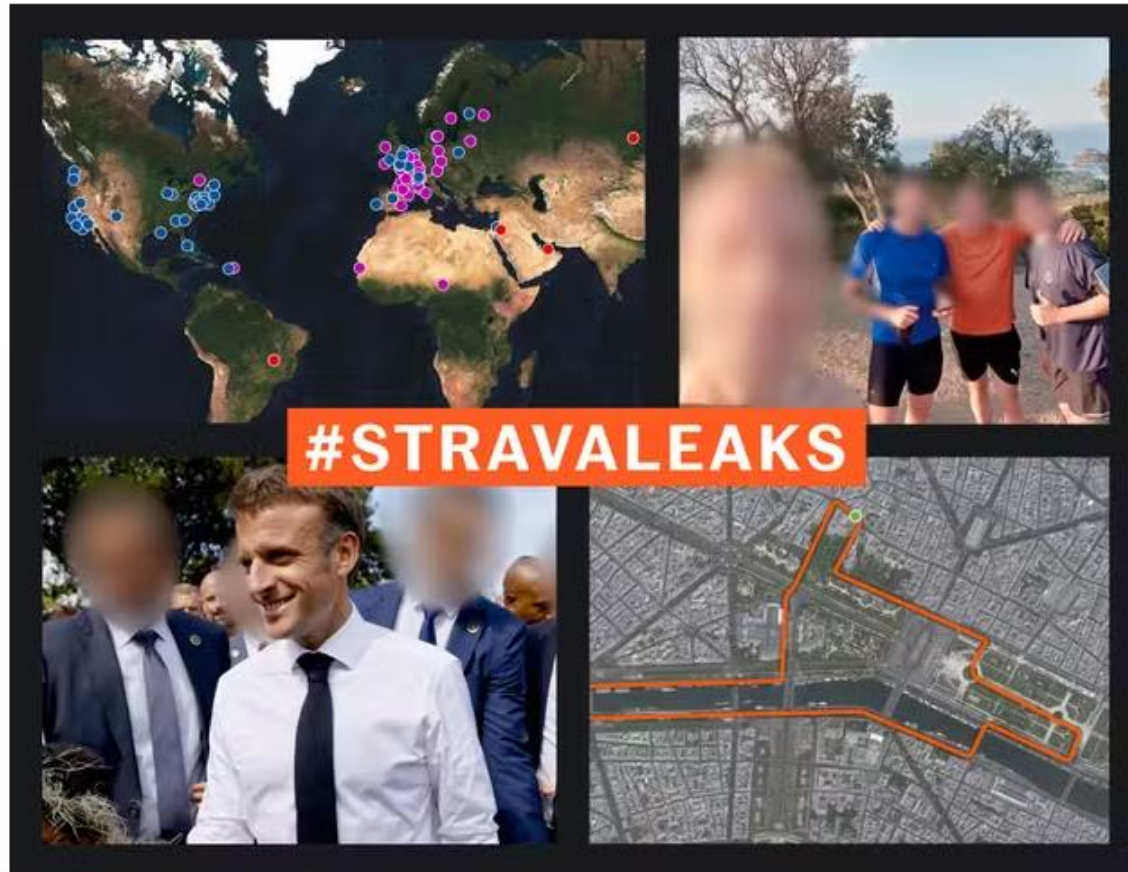
Source : Protocole de Berkeley sur l'utilisation de sources ouvertes numériques dans les enquêtes, 2024

Illustration : « StravaLeaks »



Source : *Le Monde*, « StravaLeaks », épisode 3, 29 octobre 2024

Illustration : « StravaLeaks » en France



Source : *Le Monde*, « StravaLeaks », épisode 1
27 octobre 2024

Déduire des **informations confidentielles** à partir d'une information rendue publique

- Informations confidentielles :
 - Le lieu où réside Emmanuel Macron lorsqu'il est en déplacement
 - L'identité des agents du GSPR (Groupe de sécurité de la Présidence de la République)
 - L'adresse du domicile des membres du GSPR

- Données publiques :
 - Les courses publiées sur l'application STRAVA par certains membres du GSPR

Illustration : « StravaLeaks » aux Etats-Unis



Source : *Le Monde*, « StravaLeaks », épisode 2
28 octobre 2024

Déduire des **informations confidentielles** à partir d'une information rendue publique

➤ Informations confidentielles :

- Identité des membres de la garde rapprochée de la Présidence américaine
- Adresse du domicile des membres de la garde rapprochée de la Présidence américaine
- Localisation exacte d'évènements dont l'adresse est gardée secrète avant le Jour-J

➤ Données publiques :

- Les courses publiées sur l'application STRAVA par les membres de la garde rapprochée de la Présidence américaine

Illustration : « StravaLeaks » en Russie

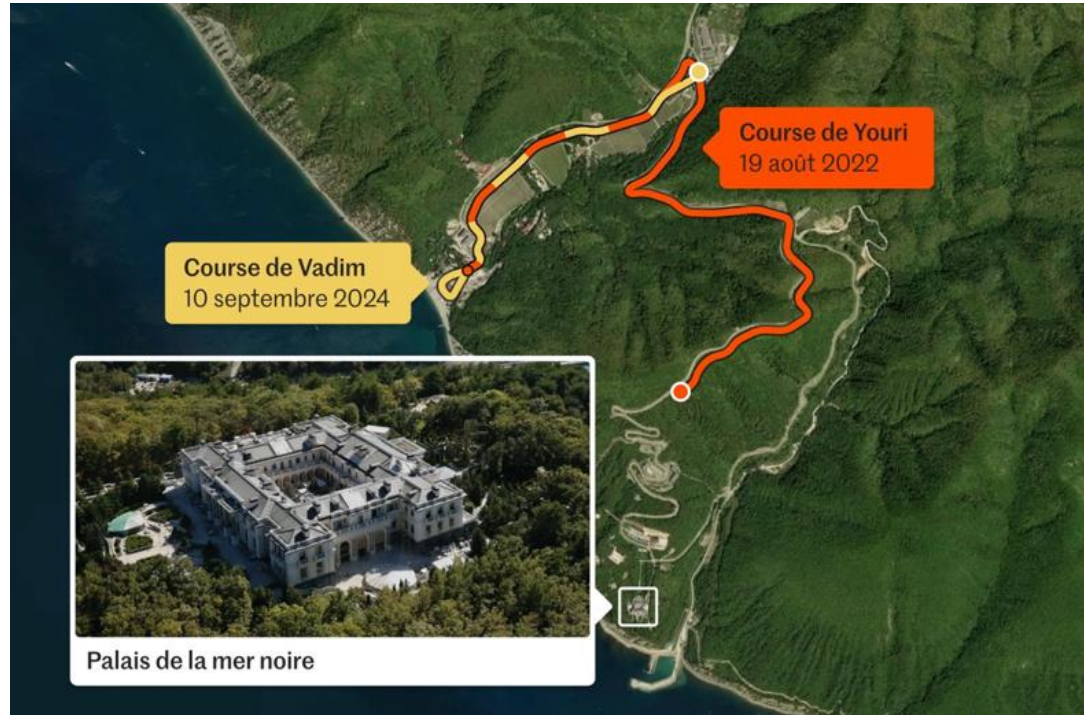


Source : *Le Monde*, « StravaLeaks », épisode 3,
29 octobre 2024

Déduire des **informations confidentielles** à partir d'une information rendue publique

- Informations confidentielles :
 - Le lieu où réside Vladimir Poutine lorsqu'il est en déplacement
 - Localisation exacte d'évènements dont l'adresse est gardée secrète avant le Jour-J
- Données publiques :
 - Les courses publiées sur l'application STRAVA par les membres du Service fédéral de protection (FSO)

Illustration : « StravaLeaks » en Russie



Source : *Le Monde*, « StravaLeaks », épisode 3,
29 octobre 2024

Informations stratégiques dans le cadre d'enquêtes diverses :

- Les gardes du corps de Vladimir Poutine multiplient les courses aux abords de luxueuses propriétés que le chef d'Etat dément posséder.
- En juillet 2023, un officier de l'armée est assassiné dans un parc de la ville de Krasnodar.
 - Le militaire était un utilisateur régulier de l'application et fréquentait souvent ce parc.
 - Dans son enquête, *Le Monde* précise que parmi les utilisateurs ayant « liké » l'une des dernières activités de cet officier sur STRAVA, l'un porte le nom de Kyrilo Boudanov (directeur du renseignement militaire ukrainien).

Les enjeux juridiques de l'OSINT au regard



- ✓ du droit pénal
- ✓ de la propriété intellectuelle
- ✓ de la protection des données à caractère personnel
- ✓ du droit de la preuve

Respect du principe de légalité de l'accès aux données

- Différencier la **recherche légitime** de l'atteinte à un **Système de Traitement Automatisé de Données (STAD)**
- **Article 323-1 du Code Pénal** : un accès est qualifié de « frauduleux » s'il est réalisé sans autorisation.
 - *Par exemple, accéder à des pages en libre accès qui ne devraient pas être référencées, telles que des documents marqués « confidentiels », peut soulever un risque juridique.*

> Article 323-1

Version en vigueur depuis le 26 janvier 2023

Modifié par LOI n°2023-22 du 24 janvier 2023 - art. 6

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

Scraping (ou moissonnage)

- **L'article L342-1 du Code de la propriété intellectuelle**, dispose qu'il est interdit d'extraire « (...) *une partie qualitativement ou quantitativement substantielle du contenu d'une base de données* (...) ».
- *Scraper* l'intégralité d'un site web peut constituer une **infraction**, punie de trois ans d'emprisonnement et de 300 000 euros d'amende, conformément à **l'article L343-4 du même code**.
- **Respect du droit d'auteur** : publier un contenu protégé par le droit d'auteur sans autorisation constitue un **délit de contrefaçon**, tel que défini à **l'article L335-3 du Code de la propriété intellectuelle**.

Fouilles de données (« data mining »)

➤ Article L122-5-3 du Code de la Propriété Intellectuelle :

- La fouille de données se définit comme la « mise en œuvre d'une technique d'analyse automatisée de textes et données sous forme numérique afin d'en dégager des informations, notamment des constantes, des tendances et des corrélations ».
- Des « copies ou reproductions numériques d'œuvres auxquelles il a été accédé de manière licite peuvent être réalisées **sans autorisation des auteurs** en vue de fouilles de textes et de données menées à bien aux seules fins de la recherche scientifique » par des organismes de recherche et institutions du patrimoine culturel (musées, bibliothèques ...)
- « à leur demande par d'autres personnes, y compris dans le cadre d'un partenariat sans but lucratif avec des acteurs privés » ;
- « des copies ou reproductions numériques d'œuvres auxquelles il a été accédé de manière licite peuvent être réalisées en vue de fouilles de textes et de données menées à bien par toute personne **sauf si l'auteur s'y est opposé de manière appropriée** ».

Fouilles de données (« data mining »)

- **Nécessité à mettre en place une gouvernance pour garantir**
 - la **licéité de l'accès** aux œuvres ;
 - l'absence d'un mécanisme d' « **opt out** » de la part du titulaire des droits ;
 - un niveau de **sécurité** approprié concernant le stockage des copies et reproduction de données (**l'article L122-5-3-III**) ;
 - la **destruction** des copies et reproduction de données à l'issue de la fouille (**l'article L122-5-3-III**).

OSINT et Protection des données à caractère personnel

Que dit la CNIL ?



« La réutilisation d'information disponible publiquement n'est pas interdite par principe.

Cependant, elle doit notamment respecter les principes de protection des données contenus dans le règlement général sur la protection des données (RGPD) et la loi Informatique et Libertés (loyauté de la collecte, base légale du traitement, information des personnes, finalité, etc.) »

Recoupement d'informations en ligne : ce que vous publiez peut dévoiler votre vie privée,
6 février 2024

OSINT et Protection des données à caractère personnel

Recommandations de la CNIL pour encadrer la Recherche sur Internet de Fuites d'Informations (RIFI)

- 1 **Démontrer un intérêt légitime** et prouver que la RIFI est nécessaire pour atteindre l'objectif visé
- 2 Trouver un équilibre entre **l'intérêt de l'organisme** et les **droits des personnes concernées**
- 3 **Limiter et déterminer la durée de conservation** des données en fonction de l'objectif de la recherche et **supprimer** les données non pertinentes après l'analyse
- 4 Respecter les **droits des personnes** incluant le **droit d'accès**, de **rectification**, d'**effacement**, de **limitation** du traitement ou encore **d'opposition**

OSINT comme outil opérationnel et puissant pour les acteurs judiciaires

- **En droit civil**, un mode de preuve déloyale n'est plus nécessairement écarté des débats : le juge doit se livrer à un contrôle de proportionnalité en mettant en balance les droits en cause. *(Cf. revirement de jurisprudence le 22 décembre 2023)*
- **En droit pénal**, le principe de la liberté de la preuve permet d'utiliser divers moyens de preuve, y compris ceux issus de l'OSINT, conformément à l'article 427 du Code de procédure pénale.

OSINT et Droit de la preuve

*« Le fait que les données à caractère personnel collectées par [un enquêteur privé] aient été pour partie en accès libre sur internet ne retire rien au **caractère déloyal de cette collecte**, dès lors qu'une telle collecte, de surcroît réalisée à des fins dévoyées de profilage des personnes concernées et d'investigation dans leur vie privée, à l'insu de celles-ci, ne pouvait s'effectuer sans qu'elles en soient informées ».*

Cour de cassation, criminelle, Chambre criminelle, 30 avril 2024, 23-80.962, Publié au bulletin

*« Un motif tiré de la vie personnelle du salarié ne peut, en principe, justifier un licenciement disciplinaire, sauf s'il constitue un manquement de l'intéressé à une obligation découlant de son contrat de travail. Dès lors, une **conversation privée** qui n'était pas destinée à être rendue publique ne pouvant constituer un manquement du salarié aux obligations découlant du contrat de travail, le licenciement, prononcé pour motif disciplinaire, est insusceptible d'être justifié, de sorte que l'employeur n'est pas fondé à invoquer la méconnaissance de son droit à la preuve.*

*Doit en conséquence être approuvé, l'arrêt qui, après avoir constaté que le salarié a été licencié pour faute grave en raison de **propos échangés lors d'une conversation privée** avec une collègue au moyen de la messagerie intégrée au compte Facebook personnel du salarié installé sur son ordinateur professionnel, en déduit que **ces faits de la vie personnelle ne pouvaient justifier un licenciement disciplinaire** »*

Cour de cassation, Assemblée plénière, 22 décembre 2023, 20-20.648, Publié au bulletin

Enquête interne : Quelques recommandations...

Avant

- Réviser les termes du contrat de travail des personnes chargées de la mission d'investigation afin d'y ajouter une clause de confidentialité renforcée
- Élaborer un code de déontologie tenant compte des cas d'usages
- Etablir une description technique détaillée de la méthode de recherche

Pendant

- Documenter la démarche de recherche (durée de conservation, base légale, etc.)
- Classifier rigoureusement l'ensemble des données
- Assurer la sécurité et la confidentialité des données
- Veiller à l'exactitude des données

Après

- Produire un rapport de fin de mission
- Etablir un retour d'expérience documenté
- Réaliser des audits réguliers afin d'assurer la conformité des pratiques et définir les évolutions nécessaires

Former et sensibiliser les collaborateurs

Notre expertise à votre service

Une newsletter offerte



VOUS AVEZ PEUT-ÊTRE MANQUÉ...

IA et charte informatique : un impératif juridique et opérationnel

L'émergence des IA génératives, comme ChatGPT, et leur adoption croissante dans les activités professionnelles, justifient la nécessité d'encadrer spécifiquement leurs usages.

Les risques associés à l'utilisation de ces technologies, comme la divulgation de données confidentielles, les atteintes aux droits de propriété intellectuelle, les biais cognitifs, ou encore la diffusion d'informations inexacts, exigent une régulation adaptée.



EN SAVOIR

Usage devant le juge civil de la preuve obtenue de façon déloyale

Ces deux pourvois en cassation portaient sur l'admissibilité des preuves recueillies par l'employeur afin de justifier le licenciement d'un salarié.

Que nous enseignent ces deux arrêts, rendus le 22 décembre 2023, par la Cour de cassation, réunie en Assemblée plénière ?

Quelles sont les conditions de



EN SAVOIR

L'actualité décryptée pour vous



Dommages causés par des produits ou services utilisant l'IA : quel régime de responsabilité ?

19 Sep, 2024 | Conformité, Droit du numérique, Intelligence artificielle

Au regard du développement exponentiel des systèmes utilisant l'intelligence artificielle (IA), pour des usages de plus en plus nombreux et variés, la Commission européenne a proposé de créer un cadre réglementaire adapté à l'évolution de ces...
[lire plus](#)



Digital Services Act : mise en oeuvre et actualités

24 Oct, 2024 | Conformité, Droit du numérique
Le Règlement relatif à un marché unique des services numériques, dit Digital Services Act (DSA), a été adopté le 19 octobre 2022. Il vise notamment à lutter contre la diffusion de contenus illicites et à instaurer plus de transparence entre les...
[lire plus](#)

Le BLOG : www.avocats-mathias.com



Mathias | Avocats



[Catalogue des formations](#)



19 rue Vernier 75017 PARIS
+33 (0)1 43 80 02 01
contact@avocats-mathias.com



@MathiasAvocats



www.avocats-mathias.com