# Newsletter DPO : mars 2025

J&A

**EN BREF :**

- **SANCTIONS** – Bilan 2024 des sanctions et mesures correctrices prononcées par la CNIL et sanction d'une société pour la surveillance excessive de ses salariés.
- **INTELLIGENCE ARTIFICIELLE** – Clarification de la définition des systèmes d'IA par la Commission européenne et nouvelles recommandations de la CNIL pour accompagner une IA responsable.
- **ANONYMISATION/PSEUDONYMISATION** – Un moteur de recherche rappelé à l'ordre par la CNIL et publication de lignes directrices par le Comité européen de la protection des données.
- **DROIT D'ACCES** – L'action coordonnée européenne identifie les lacunes de la mise en œuvre du droit d'accès.
- **TRANSFERT HORS UNION EUROPEENNE** – Publication du guide de la CNIL sur les analyses d'impact des transferts des données.

## I. LES SANCTIONS A RETENIR

### a. Bilan 2024 des sanctions de la CNIL

En 2024, la Commission Nationale de l'Informatique et des Libertés (« **CNIL** ») (France) a prononcé **87 sanctions, dont 69 dans le cadre de la procédure simplifiée** (ici). Cette hausse significative par rapport à 2023 (42 sanctions) et 2022 (21 sanctions), s'explique par l'utilisation de plus en plus fréquente de la procédure simplifiée (près de trois fois plus qu'en 2023).

Dans le cadre de sa procédure ordinaire, la CNIL a notamment sanctionné les sociétés au sujet de :

- **La prospection commerciale** : notamment pour l'absence de collecte de consentement préalable des personnes avant l'envoi de communications commerciales.
- **Les traitements de données de santé** : notamment concernant l'anonymisation (ex. clarification de la qualification des données traitées dans des entrepôts de données de santé).

Dans le cadre de sa procédure simplifiée, la CNIL a notamment sanctionné (i) le défaut de **coopération** avec la CNIL, (ii) le non-respect de **l'exercice des droits**, (iii) le manquement à la **minimisation** des données, (iv) le manquement relatif à la **sécurité** des données personnelles, et (v) le manquement à la réglementation relative aux **cookies**.

### b. Surveillance excessive des salariés : amende de 40 000 euros pour une entreprise du secteur immobilier

La CNIL, par une délibération SAN-2024-021 du 19 décembre 2024 (ici), a infligé une amende de **40 000 euros** à une société du secteur immobilier pour avoir mis en place une surveillance excessive de ses salariés, au moyen d'un logiciel de suivi du temps de travail et de la performance des salariés et d'un système de vidéosurveillance en continu mis en place dans les espaces de travail et de pause des salariés. La CNIL a relevé plusieurs manquements, notamment :

| Manquements | Détails |
|---|---|
| **Surveillance excessive** | (i) La captation en continue d'images et de sons des salariés est contraire au principe de minimisation des données (article 5 du RGPD) ; et<br>(ii) La mise en œuvre d'un logiciel de surveillance des postes de travail ne repose sur aucune base légale (article 6 du RGPD). |

| | |
|---|---|
| **Absence d'information** | **L'information orale sur la mise en œuvre du logiciel de surveillance ne remplit pas les conditions d'accessibilité dans le temps et, en l'absence de trace écrite de celle-ci, son caractère complet n'est pas établi (articles 12 et 13 du RGPD).** |
| **Défaut de mesures de sécurité** | La CNIL rappelle l'exigence renforcée d'individualisation des accès aux comptes administrateur, qui disposent de droits très étendus sur les données personnelles – ici, plusieurs collaborateurs partageaient le même accès aux données issues du logiciel de surveillance (article 32 du RGPD). |
| **Absence d'analyse d'impact (AIPD)** | La surveillance systématique des salariés à leur poste de travail nécessitait la formalisation d'une AIPD (article 35 du RGPD). |

## II. VERS UNE IA RESPONSABLE

### a. Pratiques interdites en matière d'intelligence artificielle : les nouvelles lignes directrices de la Commission Européenne

La Commission européenne a adopté, le 6 février 2025, des lignes directrices sur la définition des systèmes d'intelligence artificielle (« **IA** ») afin d'aider les parties concernées à identifier si un système logiciel relève de l'IA (ici, disponibles uniquement en anglais). Il est à noter que ces lignes directrices ne portent pas sur les modèles d'IA à usage général. La Commission a identifié et précisé les 7 éléments qui composent la définition de « système d'IA », introduite à l'article 3(1) du règlement (UE) 2024/1689 sur l'IA :

| Définition du règlement | Précisions de la Commission |
|---|---|
| **Un système automatisé** | Les systèmes d'IA doivent être basés sur le calcul et les opérations de **machines**. |
| **conçu pour fonctionner à différents niveaux d'autonomie** | La capacité de déduction des systèmes est clé pour assurer leur autonomie : un système d'IA doit fonctionner avec un certain degré raisonnable d'**indépendance d'action** (ce qui exclut les systèmes nécessitant une implication et une intervention humaine manuelle totale). |
| **et pouvant faire preuve d'une capacité d'adaptation après son déploiement** | La condition de capacité d'auto-apprentissage du système est **facultative** et non-décisive. |
| **Et qui, pour des objectifs explicites ou implicites** | Les objectifs explicites (encodés) ou implicites (déduits de comportement ou d'hypothèses) sont internes et se réfèrent aux buts et résultats des tâches à accomplir. Ils font partie d'une notion plus large de « destination » du système d'IA, qui correspond au contexte dans lequel il a été conçu et à la manière dont il doit être exploité. |
| **Déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties** | Cette notion se réfère à la **phase de construction** du système, et est donc plus large que la seule phase d'utilisation du système. La Commission, par des exemples, distingue les systèmes d'IA de ceux qui n'ont qu'une capacité limitée à analyser des modèles et à ajuster leurs sorties de manière autonome. |
| **Telles que des prédictions, du contenu, des recommandations ou des décisions** | Les systèmes d'IA se distinguent par leur capacité à générer des résultats nuancés, en exploitant des modèles complexes ou des règles définies par des experts. La Commission détaille chacun des termes de la définition. |
| **Qui peuvent influencer les environnements physiques ou virtuels** | Les systèmes d'IA ne sont pas passifs mais ont un impact actif sur les environnements dans lesquels ils sont déployés. |

## b. Les nouvelles recommandations de la CNIL pour une IA responsable

Le 7 février 2025, la CNIL a publié ses nouvelles recommandations pour accompagner le développement d'une IA responsable, en conformité avec le RGPD (ici). Celles-ci portent à la fois sur l'information des personnes, et sur l'exercice de leurs droits :

- **Information** : **le responsable de traitement doit informer les personnes lorsque leurs données personnelles servent à l'entraînement d'un modèle d'IA**. Cette information peut être adaptée en fonction des risques pour les personnes et des contraintes opérationnelles et peut donc parfois se limiter à une **information générale** (lorsque les personnes ne peuvent être contactées individuellement) **et / ou globale** (lorsque de nombreuses sources sont utilisées, en indiquant par exemple seulement des catégories de sources).
- **Droits des personnes** : la CNIL invite les acteurs à prendre en compte la protection de la vie privée dès le stade de conception du modèle (ex. stratégie d'anonymisation, non-divulgation de données confidentielles). La mise en œuvre des droits dans le cadre de modèle d'IA peut être difficile et **un refus d'exercice des droits peut parfois être justifié**. Lorsque ces droits doivent être garantis, **la CNIL prendra en compte les solutions raisonnables disponibles et pourra aménager les conditions de délai**.

# III. L'ANONYMISATION ET LA PSEUDONYMISATION EN DEBAT

## a. La CNIL adresse à Qwant un rappel à ses obligations légales

La CNIL a adressé au moteur de recherche Qwant un **rappel à ses obligations légales** (ici). Dans le cadre de l'affichage de publicité contextuelle, Qwant estimait transmettre à la société Microsoft des données essentiellement techniques et anonymisées (ex. adresse IP tronquée ou hachée). A la suite de deux contrôles et d'échanges avec ses homologues européens, la CNIL a considéré que les données transférées sont pseudonymisées et non anonymisées.

Elle a choisi de prononcer à l'encontre de la société un rappel aux obligations légales plutôt qu'une sanction en raison : (i) du niveau d'**intrusivité faible** du moteur de recherche, (ii) des nombreuses **mesures techniques** déployées pour réduire le risque de réidentification, (iii) du **caractère non-intentionnel** du manquement, entrainé par une erreur d'analyse initiale, (iv) de la **modification rapide** de sa politique de confidentialité, et (v) de sa **bonne foi et coopération** tout au long de la procédure.

## b. Les nouvelles lignes directrices du CEPD sur la pseudonymisation

Le 16 janvier 2025, le Comité européen de la protection des données (CEPD) a adopté de nouvelles lignes directrices 01/2025 sur la pseudonymisation, soumises à consultation publique jusqu'au 14 mars 2025 (ici, disponibles uniquement en anglais).

La pseudonymisation permet de ne plus attribuer les données personnelles à une personne concernée sans information supplémentaire (article 4(5) du RGPD). **Les données pseudonymisées sont des données personnelles car il existe un risque de réidentification des personnes concernées.**

Le CEPD indique que la pseudonymisation peut (i) **faciliter l'utilisation de la base juridique de l'intérêt légitime**, pour autant que toutes les autres exigences du RGPD soit respectées, (ii) garantir la **compatibilité avec la finalité initiale** dans le cadre d'un traitement ultérieur, et (iii) aider les organisations à respecter les obligations relatives aux principes du RGPD, à la protection dès la conception et par défaut, et à la sécurité.

Le CEPD analyse également un ensemble de mesures techniques robustes pour empêcher toute réidentification non autorisée. Parmi les techniques recommandées figurent **le hachage avec clé secrète ou sel, la séparation des informations permettant l'attribution, et le contrôle strict des accès**.

Il sera soulevé que ces lignes directrices sont à lire à la lumière de l'affaire C-413/23 pendante devant la Cour de justice de l'Union européenne opposant le contrôleur européen de la protection des données au conseil de résolution unique (CRU). Dans cette affaire, des données pseudonymisées ont été transférées par le CRU à Deloitte pour les besoins d'une mission d'analyse. Dans ses conclusions en date du 6 février 2025, l'avocat général invite la Cour à se prononcer sur le fait de savoir si le destinataire de données pseudonymisées qui ne dispose pas de moyens raisonnables pour réidentifier les personnes concernées, pourrait être considéré comme ne traitant pas de données à caractère personnel dans la mesure où le risque d'identification est « inexistant ou insignifiant ».

## IV. LUMIERE SUR LE DROIT D'ACCES

La CNIL et le Contrôleur européen de la protection des données ont participé à une action coordonnée du Comité européen de la protection des données afin d'évaluer la mise en œuvre du droit d'accès aux données personnelles.

Au cours de l'année 2024, la CNIL a contrôlé des organismes publics et privés, choisis sur la base de plaintes reçues, et a prononcé plusieurs rappels aux obligations légales. Elle remarque que les mesures organisationnelles mises en œuvre par ces organismes pour traiter les demandes de droit d'accès sont parfois insuffisantes / insatisfaisantes. Les organismes devraient à la fois (i) **fournir des informations sur le traitement,** (ii) **inclure une copie des données traitées**, et (iii) ne devraient pas exclure systématiquement de leurs réponses certains traitements ou catégories de données personnelles.

Le CEPD a quant à lui contrôlé le traitement des demandes de droit d'accès par les institutions, organes et organismes de l'UE et a mis en évidence dans son rapport du 16 janvier 2025 : (i) le faible volume de demandes, (ii) la décentralisation de la gestion des demandes, (iii) le fait qu'il est difficile de distinguer les demandes d'accès des autres types de demandes, (iv) le traitement excessif de données engendré par la vérification de l'identité des demandeurs, (v) la difficile conciliation entre la protection des droits et libertés et le respect du droit d'accès des personnes. Les responsables de traitement et sous-traitants sont invités par le CEPD à se référer aux lignes directrices 01/2022 sur le droit d'accès des personnes concernées.

## V. ANALYSE D'IMPACT DES TRANSFERTS DE DONNEES

Le 31 janvier 2025, la CNIL a publié la version finale de son guide sur l'Analyse d'Impact des Transferts de Données (AITD) (ici) afin d'aider les exportateurs de données à évaluer le niveau de protection dans les pays de destination situés hors de l'Espace Economique Européen et la nécessité de mettre en place des garanties supplémentaires. Cette analyse est nécessaire lorsque le transfert repose sur un outil de l'article 46 du RGPD (clauses contractuelles types, règles d'entreprise contraignantes, etc.) : le pays de destination ne bénéficie alors pas d'une décision d'adéquation et le transfert n'est pas effectué sur la base d'une dérogation de l'article 49 du RGPD.

Le guide propose une méthodologie en six étapes :

1) Identifier les données concernées et les acteurs impliqués ;
2) Choisir l'outil de transfert approprié ;
3) Analyser les risques liés aux lois et pratiques du pays tiers ;
4) Déterminer et appliquer les mesures supplémentaires (ex. chiffrement ou anonymisation) ;
5) Mettre en œuvre ces mesures supplémentaires ;
6) Réévaluer à intervalles appropriées la conformité du transfert.

Cette publication fait suite à une consultation publique qui a permis à la CNIL d'adapter son guide aux réalités pratiques des entreprises, et de le modifier afin de prendre en compte les derniers avis du Comité Européen de la Protection des Données.

***Notre équipe IT/Data se tient à votre disposition pour toutes questions***

**Emilie de VAUCRESSON**
Avocate associée
edevaucresson@joffeassocies.com

**Amanda DUBARRY**
Avocate
adubarry@joffeassocies.com

**Hanna – Marie BORTEN-GUARY**
Avocate
hmbortenguary@joffeassocies.com