NEWSLETTER RGPD/DATA

NUMÉRO 66 ● 2025

ACTUALITÉS DU CABINET P. 23

FORMATION À LA PRÉPARATION À LA CERTIFICATION « DPO ».
DATE SUR DEMANDE

SOMMAIRE

LE VOL D'UNE CLE USB CONSTITUE, DE FACTO, UNE VIOLATION DE DONNEES

AEPD (Espagne), 16 mars 2024

L'autorité de contrôle espagnole a sanctionné un responsable du traitement qui s'était fait voler une clé USB non chiffrée et l'a enjoint à notifier la violation de données personnelles aux personnes concernées.

Le vol, dans les locaux du responsable du traitement, d'une clé USB non chiffrée

Les locaux d'un responsable du traitement ont été cambriolés et une clé USB non chiffrée contenant des données personnelles a été volée. Le responsable du traitement a immédiatement déposé une plainte pénale mais a tardé à notifier la violation à l'autorité de contrôle (notification hors délai), considérant par ailleurs que la notification aux personnes concernées n'était pas nécessaire.

L'autorité de contrôle a d'abord enjoint au responsable du traitement de notifier la violation aux personnes concernées, puis a indiqué ouvrir une enquête.

Pour sa défense, le responsable du traitement indiquait que rien ne prouvait qu'un tiers avait eu accès au contenu de la clé USB et que, par conséquent, rien ne démontrait qu'il y avait eu une violation de données.

Des faits incontestablement constitutifs d'une violation de données

Après avoir rappelé que la clé USB volée *« n'était pas cryptée ou équipée d'une autre mesure visant à empêcher l'accès à ces informations par des tiers non autorisés en cas de perte ou de vol »*, l'autorité de contrôle a considéré que ces faits constituent *« incontestablement »* une violation de données, au sens du RGPD.

Ce faisant, l'autorité a rejeté l'argument du responsable du traitement qui affirmait que le vol d'un dispositif contenant des données à caractère personnel sans aucune protection d'accès ne constitue pas, de facto, une violation de la confidentialité, sauf à démontrer un accès à ces données par un tiers non autorisé.

En effet, selon l'autorité de contrôle, retenir cet argument en défense *« reviendrait à dire que le vol d'un dossier papier ou d'un livre contenant [des données personnelles] ne constitue pas une violation de la confidentialité en raison de l'impossibilité de prouver de manière fiable que la personne qui l'a volé ou un autre tiers ne l'a pas ouvert. »*

Pour l'autorité, *« ce qui est pertinent pour comprendre qu'il y a eu violation de la confidentialité, c'est que l'information est totalement à la disposition de tiers non autorisés ».*

Compte tenu de ce qui précède, l'autorité de contrôle a considéré que le responsable du traitement n'avait pas pris les mesures de sécurité adéquates et a infligé au responsable du traitement une amende de 145 000 €.

Source : ici

L'INTERET SUPERIEUR DE L'ENFANT EST UNE LIMITE AU DROIT D'ACCES

L'autorité de protection des données slovène a considéré qu'une école avait légalement refusé de donner accès à l'intégralité des données sollicitées par un père, qui exerçait le droit d'accès au nom de son enfant.

La demande de droit d'accès exercée par un papa

Un père a demandé, à l'école primaire dans laquelle son fils est scolarisé, l'accès aux données personnelles de ce dernier.

Dans sa demande, le père sollicitait, notamment, la communication de (i) l'identité des personnes autorisées à venir chercher son enfant ainsi que (ii) l'adresse de son enfant.

Constatant, deux mois plus tard, que l'école n'avait toujours pas répondu à sa demande d'accès, le père a déposé une plainte auprès de l'autorité de contrôle.

Le refus de donner accès à l'intégralité des données personnelles

L'école, informée par l'autorité de contrôle de l'ouverture d'une enquête, a finalement transmis au père certaines données personnelles, en prenant le soin d'occulter les données ci-dessus rappelées. Elle justifiait cette occultation par le fait que le père faisait l'objet d'une ordonnance restrictive, par un tribunal, l'interdisant de s'approcher de la mère de son enfant. Elle invoquait donc l'exception au droit d'accès posé à l'article 15.4 du RGPD, selon laquelle le droit d'obtenir une copie des données « *ne devrait pas porter atteinte aux droits ou libertés d'autrui.* »

Accueillant favorablement cet argument, l'autorité de contrôle a précisé qu'un responsable du traitement peut refuser de faire droit à une demande d'accès présentée par l'intermédiaire d'un représentant légal, *« s'il existe des circonstances spécifiques et objectives qui permettent raisonnablement de conclure que les droits ou les intérêts légitimes [du mineur], seraient directement ou indirectement affectés par la divulgation de certaines données à caractère personnel, et lorsque ces droits et intérêts l'emportent sur l'intérêt du représentant légal. »*

En l'espèce, l'autorité de contrôle a considéré que l'intérêt supérieur de l'enfant justifiait le fait que le père ne connaisse pas l'adresse de résidence de l'enfant et l'identité des personnes autorisées à venir le chercher.
En conclusion, l'autorité de contrôle a considéré que le refus de l'école de donner accès à certaines données personnelles était justifié, et n'a prononcé aucune sanction.

Source : ici

REFERENTIELS « SANTE » CNIL : LA MISE A JOUR PROGRESSE

La CNIL travaille actuellement sur un chantier de mise à jour de ses référentiels « santé ». Sont visés les « MR-001 à MR-008, [les] référentiels relatifs aux entrepôts de données de santé, à la gestion des vigilances sanitaires, aux accès précoces et compassionnels ou encore le référentiel d'accès simplifié aux données de l'échantillon du Système national des données de santé (SNDS) ».

A la suite d'une consultation publique ouverte en mai 2024, la CNIL a publié ce mois-ci la « *synthèse des contributions* ».

Il en est notamment ressorti un positionnement sur :

- Les axes de travail prioritaires concernant spécifiquement les MR (tels que « *la possibilité d'apparier les données* », « *l'aménagement des modalités d'information de la personne concernée* ») ;
- Les axes de travail concernant plus généralement tous les référentiels (ex. : les « *besoins non couverts par les référentiels existants* », « *la mise en conformité des registres et des cohortes* », mais également « *le déploiement d'un nouveau formulaire de demande d'autorisation* » ou encore « *la réorganisation de l'onglet « santé » du site internet de la CNIL* (…) » ;
- Les groupe de travail à mettre en place.

Début 2025, les groupe de travail doivent être établis « *afin de construire collectivement les futurs référentiels santé de la CNIL, en lien avec la Plateforme des données de santé et les autres acteurs concernés* ».

A suivre…

Source : ici

LA JURISPRUDENCE EST UNE BASE LEGALE QUI PEUT FONDER UN TRAITEMENT

La notion d'« obligation légale » en tant que base légale d'un traitement de données à caractère personnel a récemment été interprétée de façon extensive par la CJUE. Cette dernière a effectivement considéré que cette notion « couvre la jurisprudence nationale ».

Rappel des principes : l'« obligation légale » comme base légale d'un traitement

Pour mémoire, tout traitement de données à caractère personnel doit reposer sur une des six bases légales prévues par le RGPD, parmi lesquelles figure le respect d'une obligation légale[1]. Cette obligation légale doit être définie « *par le droit de l'Union* » ou « *par le droit de l'Etat membre auquel le responsable de traitement est soumis* »[2]. Dans les deux cas, ce droit doit répondre à « *un objectif d'intérêt public* » et être « *proportionné à l'objectif légitime poursuivi* ».

La CNIL précise encore que « *ces dispositions légales* » doivent établir « *une obligation impérative de traiter des données personnelles, suffisamment claire et précise* ». Ces dispositions légales doivent également « *au moins* » définir les finalités du traitement en cause[3].

A titre d'exemple, la loi Sapin 2, en imposant à certains organismes la mise en œuvre d'un dispositif de recueil d'alertes pour révéler un manquement à certaines règles, constitue une obligation légale fondant le traitement de données personnelles réalisé dans le cadre de l'utilisation d'un tel dispositif (dans les conditions et limites précisées par la règlementation).

.

L'affaire soumise à la CJUE : le périmètre de l'obligation légale en question

Des sociétés d'investissement, associées d'un fonds d'investissement (faisant appel public à l'épargne), souhaitaient obtenir la communication des noms et adresses des autres associés détenant des participations indirectes (via des sociétés fiduciaires) dans le fonds.

Les sociétés fiduciaires concernées s'opposaient à une telle divulgation de données à caractère personnel, considérant que cette demande ne viserait notamment qu'« *à servir les intérêts économiques propres des* [demanderesses] (…)». Elles soutenaient également que les contrats de participation et fiducie contiennent des clauses interdisant la communication de ces données à d'autres détenteurs de participation. Les demanderesses estimaient, quant à elles, avoir pour seule intention de prendre contact avec les autres associés afin de négocier le rachat de leurs parts.

A cette occasion, la juridiction allemande saisie du litige s'est interrogée sur l'existence d'une obligation légale de divulguer ce type de données personnelles, obligation qui se déduirait de la jurisprudence nationale. En effet, une décision de justice allemande considère comme nulles les clauses garantissant la confidentialité des coordonnées des associés indirects de ce type de société « *de sorte qu'il y aurait lieu de divulguer les données à caractère personnel* [desdits] *associés (…)* ».

A cette occasion, la CJUE s'est prononcée sur le point de savoir si une jurisprudence nationale peut, par principe, constituer une base légale pour fonder un traitement de données à caractère personnel.

La solution : l'« obligation légale » peut inclure la jurisprudence

Selon la CJUE, « *le droit de l'Etat membre auquel le responsable de traitement est soumis* » inclut la jurisprudence nationale[4]. Encore faut-il, précise la CJUE, que cette jurisprudence soit (i) claire et précise et (ii) appliquée de manière prévisible pour les justiciables. Comme toute obligation légale, cette jurisprudence doit, à l'évidence, répondre également à un objectif d'intérêt public et être proportionnée à celui-ci, étant encore rappelé que « *le traitement concerné* [doit être] *opéré dans les limites du strict nécessaire* ». Le respect de ces critères est laissé à l'appréciation du juge national.

Jusqu'à présent, on savait que l'obligation légale devait découler d'un texte (loi, règlement, etc.) prévoyant/autorisant un traitement de données à caractère personnel. A l'appui de cette décision, cette obligation peut donc aussi résulter de la jurisprudence, ce qui ouvre le champ des possibles avec toutefois des incertitudes.

En particulier, comment le juge français appréciera, dans une jurisprudence, le caractère impératif de l'obligation de traiter des données personnelles ou encore la définition des finalités ? Y aura-t-il plus de souplesse que dans l'interprétation d'un texte de loi ? On l'ignore encore…

Dans l'attente de décisions rendues par les juridictions nationales ou une nouvelle jurisprudence de la CJUE, la prudence reste de mise.

A suivre…

Source : ici

[1] Article 6 paragraphe 1 c) du RGPD.
[2] Article 6 paragraphe 3 du RGPD.
[3] Voir également article 6 paragraphe 3 du RGPD.
[4] Pour ce faire, la CJUE s'est fondée sur le considérant 41 du RGPD selon lequel « une base juridique ou (…) une mesure législative, (…) ne signifie pas nécessairement que l'adoption d'un acte législatif par un parlement est exigée ». « Cependant, cette base juridique ou cette mesure législative devrait être claire et précise et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour et de la Cour européenne des droits de l'homme ».

LE CEPD ADOPTE SON PREMIER AVIS SUR L'INTELLIGENCE ARTIFICIELLE

Interrogé par l'autorité irlandaise de contrôle, le CEPD a adopté, le 18 décembre 2024, son premier avis sur l'intelligence artificielle.

L'avis du CEPD porte sur trois points, en réponse aux trois questions qui ont été posées par l'autorité de contrôle irlandaise.

L'application du RGPD aux traitements réalisés au moyen d'outils d'intelligence artificielle

Dès lors que le RGPD ne s'applique pas aux données « anonymes » (considérant 26 du RGPD), l'autorité de contrôle se demande dans quelle mesure les traitements de données réalisés au moyen d'outils d'intelligence artificielle peuvent échapper à l'application du RGPD (dans l'hypothèse où l'outil ne traiterait que des données non personnelles ou des données personnelles anonymisées)

Selon le CEPD, les intelligences artificielles sont entraînées à l'aide de « données d'apprentissage » qui contiennent, généralement, des données à caractère personnel. Ainsi, par principe, il faut considérer les traitements de données réalisés par les outils d'intelligence artificielle comme soumis au RGPD.

Par exception, le CEPD fournit les critères permettant d'évaluer, au cas par cas, si les traitements réalisés au moyen d'outils d'intelligence artificielle échappent à l'application du RGPD (dès lors que l'outil ne traiterait pas de données personnelles ou uniquement des données personnelles anonymisées). Parmi les critères, le CEPD recommande de vérifier (i) que les données d'apprentissage utilisées ne peuvent pas être extraites de l'outil et (ii) que les résultats générés ne font pas ressortir les données à caractère personnelle présentes dans les données d'apprentissage.

La base légale applicable aux traitements réalisés au moyen d'outils d'intelligence artificielle

A l'exception de ceux non soumis au RGPD (*cf*. point précédent), les outils d'intelligence artificielle traitent, en principe, des données à caractère personnel. Or, conformément à l'article 6 du RGPD, tous les traitements de données personnelles doivent reposer sur une base légale. Ainsi, l'autorité de contrôle se demande si l'intérêt légitime est une base légale valable.

Selon le CEPD, les traitements de données personnelles réalisés au moyen d'outils d'intelligence artificielle peuvent être fondés sur l'intérêt légitime. La possibilité d'utiliser cette base légale n'est cependant pas absolue : le responsable du traitement doit préalablement s'assurer que les « conditions » de l'intérêt légitime sont remplies.

Les conséquences du développement illicite d'une intelligence artificielle

Les outils d'intelligence artificielle poursuivent généralement plusieurs phases (l'outil est d'abord développé, puis déployé et enfin utilisé). L'autorité de contrôle se demande si, en cas de non-respect du RGPD pendant la phase de développement, ce manquement peut avoir une conséquence sur l'utilisation de l'outil d'intelligence artificielle.

Selon le CEPD, le développement d'une intelligence artificielle en violation du RGPD rend nécessairement son déploiement et son utilisation illicites.

Source : Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models

PUBLICITE INSEREE DANS DES BOITES MAILS : ORANGE SANCTIONNEE POUR DEFAUT DE CONSENTEMENT

Le 14 novembre 2024, la CNIL a prononcé à l'égard d'Orange une amende de 50 millions d'euros, pour avoir affiché, sans consentement, des publicités dans les boites mails des utilisateurs de son service de messagerie électronique.

Des publicités insérées dans la boite de réception

Dans le cadre de la mise à disposition de son service de messagerie électronique « Mail Orange », Orange affichait, entre les courriels des utilisateurs du service, des annonces publicitaires, qui revêtaient le même format que les courriels reçus, avec certaines adaptations (le terme « annonce » figurait par exemple à l'emplacement où il y a habituellement l'heure de réception du courriel).

L'affichage de ces annonces était réalisé sans que les données personnelles de l'utilisateur ne soient traitées, sans qu'un courriel ne soit envoyé, et sans que le consentement ne soit recueilli.

Un consentement nécessaire, quand bien même aucun courriel n'est adressé

La CNIL, suite à un contrôle, a estimé que ce type de publicité est régi par l'article L34-5 du Code des postes et communications électroniques (« CPCE ») et nécessite, à ce titre, de recueillir le consentement de la personne concernée.

L'argumentaire de la CNIL s'appuie sur un arrêt du 25 novembre 2021, par lequel la CJUE a estimé que, lorsque le message publicitaire prend une forme qui s'apparente à un véritable courriel et est placé au même emplacement qu'un courriel, il doit être régi par l'article 13 de la directive e-privacy :

> « *l'affichage dans la boîte de réception de l'utilisateur d'un service de messagerie électronique de messages publicitaires sous une forme qui s'apparente à celle d'un véritable courrier électronique et au même emplacement que ce dernier* » constitue une « *utilisation [...] de courrier électronique à des fins de prospection directe* », *au sens de [l'article 13 de la directive 2002/58 dite e-privacy]* ».

Orange a, pour sa part, estimé que l'arrêt de la CJUE a été rendu sur le fondement de l'article 13 de la directive e-privacy, dont la formulation diffère de celle de l'article L34-5 du CPCE, qui est le texte directement applicable à Orange : si le premier interdit « *l'utilisation de courrier électronique à des fins de prospection directe* », le second prohibe « *la prospection directe au moyen de système automatisé de communications électroniques* », or le message de prospection n'a, en l'espèce, pas véritablement été adressé au moyen d'un système automatisé de communications électroniques.

L'imprécision et l'imprévisibilité du cadre juridique aurait dû, selon Orange, conduire la CNIL à s'abstenir de prononcer une sanction, sauf à violer le principe de légalité.

La CNIL a répondu à Orange que l'article L34-5 du CPCE doit être lu « *à la lumière* » de la directive e-privacy, de sorte que la jurisprudence de la CJUE était bien applicable au cas d'espèce : « *il ressort de l'arrêt de la CJUE que, peu importe que les annonces en cause ne constituent pas, d'un point de vue technique, de véritables courriels – c'est-à-dire des messages envoyés par un utilisateur à un autre utilisateur en utilisant son adresse électronique –, leur seul affichage dans un espace normalement spécifiquement réservé aux courriels privés suffit à considérer que ces messages sont communiqués au moyen de la boîte aux lettres électronique des personnes concernées, et donc de leur courrier électronique* ».

Il n'est pas nécessaire d'être annonceur pour être sanctionné

Orange a fait valoir qu'elle n'est pas annonceur mais fournisseur de messagerie électronique or, jusque-là, la CNIL a toujours fait peser la charge du recueil du consentement sur les annonceurs, qui sont les plus à même de savoir s'il faut recueillir le consentement, compte tenu de l'existence potentielle d'une relation préalable avec la personne concernée.

Sur ce point, pour la CNIL, « *ORANGE a la maîtrise de l'affichage de ces publicités, dans la mesure où elle met à disposition des annonceurs susvisés des emplacements dédiés, qu'elle a préalablement déterminés, au sein de la boîte de messagerie des utilisateurs de son propre service " Mail Orange ".* » Orange peut donc bien être sanctionnée, quand bien même elle ne serait pas un annonceur.

Compte tenu de ces manquements, ainsi que d'opérations de lectures de cookies sans le consentement de l'utilisateur, la CNIL a prononcé à l'égard d'Orange une amende administrative d'un montant de 50 millions d'euros.

Source : ici

LES RESTRICTIONS DE VISIBILITE LINKEDIN NE DOIVENT PAS ETRE CONTOURNEES

Le 5 décembre 2024, la CNIL a prononcé à l'égard de la société KASPR une amende de 240.000 euros, pour avoir collecté sur LinkedIn des données personnelles d'utilisateurs qui avaient précisément choisi d'en limiter la visibilité.

Une collecte de données personnelles contournant les restrictions de visibilité paramétrées sur LinkedIn

Suite à plusieurs saisines, la CNIL a procédé à un contrôle sur audition des représentants de KASPR, ce qui a mis en lumière le fonctionnement de l'extension de navigateur internet proposée par cette société.

Cette extension permet d'avoir accès aux coordonnées professionnelles d'une « *personne cible* », lorsque son profil LinkedIn est visité, y compris lorsque cette personne a restreint la visibilité de son profil.

Les coordonnées des personnes cibles ainsi affichées sont notamment collectées par KASPR auprès des utilisateurs de l'extension eux-mêmes. En effet, les comptes LinkedIn des utilisateurs sont synchronisés avec l'extension, de telle sorte que KASPR collecte les données de profils de leurs contacts LinkedIn.

Un contournement des restrictions de visibilité outrepassant les attentes raisonnables des personnes cibles

La CNIL s'est intéressée aux opérations de collecte de données des personnes cibles ayant restreint la visibilité de leur profil LinkedIn, opérations fondées, selon KASPR, sur l'intérêt légitime.

Pour la CNIL, KASPR ne peut pas collecter les données des personnes cibles ayant choisi de restreindre la visibilité de leurs coordonnées, sans que cela n'aille à l'encontre de leurs « *attentes raisonnables* ».

En effet, les personnes cibles, en autorisant certains de leurs contacts à prendre connaissance de leurs coordonnées, n'ont pas, « *par cette action, entendu autoriser la société KASPR à collecter de telles données* ». Aucune « *relation pertinente et appropriées* » ne lie les personnes cibles à KASPR.

En conséquence, la CNIL a considéré que « *les intérêts ou les libertés et droits fondamentaux des personnes concernées, notamment leur droit au respect de la vie privée, prévalaient sur l'intérêt légitime du responsable de traitement à traiter leurs données pour pouvoir assurer le fonctionnement de son extension, de sorte que le fondement juridique de l'intérêt légitime de la société ne peut être retenu* ».

En l'absence d'intérêt légitime, la CNIL a conclu que le traitement était dépourvu de base légale. Compte tenu notamment de ce manquement, la CNIL a prononcé à l'égard de KASPR une amende de 240.000 €.

Un défaut de base légale limité à certains cas de collecte

Il est à noter que le défaut de base légale relevé par la CNIL est cantonné au seul cas de collecte de données des personnes cibles ayant restreint l'affichage de leurs coordonnées sur LinkedIn.

La CNIL n'a donc pas relevé de défaut de base légale s'agissant des opérations de collecte de données issues de profils LinkedIn « publics », également réalisées par KASPR. Pourtant, les Conditions d'utilisation de LinkedIn prohibent dans une très large mesure la collecte automatisée d'informations sur ce réseau social, ce qui aurait pu conduire la CNIL à caractériser l'absence d'« *attentes raisonnables* » des personnes concernées, y compris s'agissant des données collectées auprès de profils publics.

Source : ici

DOCTRINE

RGPD

Divulgation de données personnelles d'un tiers à un média : quel régime applicable ?

Comme chaque mois, Alexandre Fievée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en s'appuyant sur les décisions rendues par les différentes autorités de contrôle nationales au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur la question de savoir s'il est possible, dans les médias, de communiquer, en toute légalité, les données personnelles d'un tiers. La solution est-elle différente si les données communiquées ont déjà été rendues publiques par ce tiers ?

En application de l'article 5-1 du RGPD, non seulement les données à caractère personnel doivent être traitées « *de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence)* », mais elles doivent aussi être collectées « *pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités* ». L'article 6 ajoute que le traitement ainsi réalisé doit reposer sur une base légale, à savoir : le consentement, l'intérêt légitime, l'exécution du contrat, l'obligation légale, la mission d'intérêt public ou encore la sauvegarde des intérêts vitaux.

En application de ces principes, on peut légitimement se poser la question de savoir si un organisme, une administration ou encore une personne physique est légitime à communiquer, dans le cadre d'un entretien avec un journaliste, les données personnelles concernant une autre personne. À ce propos, est-ce que la réponse serait différente s'agissant de données qui auraient été déjà rendues publiques par la personne visée ?

L'affaire[1]

Une députée, à la recherche d'informations concernant des amendes pour excès de vitesse qui lui avaient été infligées, a contacté le maire de la commune de Torri del Benaco, afin qu'il l'accompagne dans les bureaux de la police locale. L'un des agents sollicités lui a fourni oralement, en présence du maire, toutes les informations souhaitées : le nombre d'amendes, leur montant, le nombre de points retirés, etc. S'interrogeant sur la régularité des contrôles mis en œuvre par la ville de Torri del Benaco, la députée déposa une question parlementaire. Puis, dans le cadre de plusieurs déclarations publiques, la députée confirma avoir fait l'objet d'un certain nombre d'amendes. Quelques semaines plus tard, dans le cadre d'une interview pour un journal, le maire de la commune, interrogé sur cette affaire, confirmait, dans l'optique de défendre les choix opérés par l'administration concernant les contrôles mis en place, que des amendes pour excès de vitesse avaient effectivement été infligées à la députée. Cette dernière, qui considérait que la divulgation ainsi réalisée de ses données personnelles par le maire avait été effectuée en violation du RGPD, déposa une plainte auprès de l'autorité italienne de protection des données.

L'autorité, qui a d'abord rappelé que le maire s'est borné à répondre à des questions posées par un journaliste concernant une affaire qui avait déjà été traitée par la presse, a ensuite relevé que le maire, agissant en tant que représentant de la commune, n'avait pas seulement communiqué des informations partiellement rendues publiques par la plaignante elle-même, mais aussi des « *informations supplémentaires* ». Dans ce contexte, l'autorité de protection des données a estimé que le traitement avait été effectué sans base légale et en violation des principes de « *licéité, loyauté et transparence* » et a ajouté que « *les circonstances dans lesquelles l'affaire et certaines informations étaient déjà connues de la population locale et rapportées par certains organes de presse locaux ne peuvent être considérées comme suffisantes pour justifier la divulgation des données à caractère personnel du plaignant* ».

Quelles recommandations ?

Il n'est pas rare de voir dans les médias des personnalités publiques divulguer des anecdotes ou raconter des histoires dans lesquelles des tiers sont protagonistes. Dans ces récits, bien souvent, des données personnelles concernant ces tiers sont publiées, diffusées. Cette décision montre qu'il faut se montrer extrêmement prudent dans ce genre de situation car le RGPD pourrait s'appliquer, et une telle divulgation pourrait heurter les principes de licité (absence de base légale) mais également les principes de loyauté et de transparence. La circonstance selon laquelle les données litigieuses auraient déjà été rendues publiques par ces tiers serait indifférente. Alors, prudence !

Alexandre FIEVEE
Avocat Associé
DERRIENNIC ASSOCIES

Notes

(1) =Autorité italienne de protection des données, 20 juin 2024.

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

DOCTRINE

DONNÉES PERSONNELLES

Quels faisceaux d'indices pour un entrepôt de données de santé ?

Dans une récente affaire, la Cnil a appliqué un faisceau d'indices pour qualifier une base de données d'entrepôt de données de santé. Ce type de décision (publiée) est suffisamment rare pour être souligné.

La création d'entrepôts de données de santé ne fait que croître, aussi bien dans le secteur privé que dans le secteur public. Les entrepôts de données de santé, eu égard à la nature des données qu'ils traitent (données sensibles) et à leur volume, sont soumis à un cadre juridique strict. Pour autant, la notion d'entrepôt de données de santé ne fait pas l'objet d'une définition légale. La qualification d'une base de données en entrepôt de données de santé n'est pas, en conséquence, toujours aisée.

Les entrepôts de données de santé soumis à un cadre juridique strict…

Pour mémoire, la Cnil a publié un référentiel relatif « *aux traitements de données à caractère personnel mis en œuvre à des fins de création d'entrepôts de données de santé dans le domaine de la santé* »[1] (le « *référentiel* »). Ce référentiel concerne uniquement les entrepôts de données de santé « *nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement* ».

Ainsi, un organisme, responsable de traitement, souhaitant mettre en œuvre un entrepôt de données de santé dans le cadre de l'exercice d'une mission d'intérêt public, doit, par principe, s'assurer de la conformité de son projet au référentiel. Dans le cas où l'organisme considère que son projet est en stricte conformité avec le référentiel, il peut alors se contenter d'une déclaration de conformité auprès de la Cnil.

Dans l'hypothèse, en revanche, où il existe des écarts avec les exigences prévues au référentiel, il appartient à l'organisme de saisir la Cnil d'une demande d'autorisation spécifique préalable[2]. Tel est le cas notamment pour un organisme privé qui réalise un entrepôt de données de santé dans le cadre de son intérêt légitime.

L'absence de définition légale

Si les entrepôts de données de santé ne font pas l'objet d'une définition légale, plusieurs autorités administratives/publiques indépendantes et groupement d'intérêt public ont eu l'occasion d'apporter des éclairages sur cette notion.

La Cnil a publié plusieurs documents dans lesquels elle explique ce qu'il faut entendre par « *entrepôt de données de santé* ». Ainsi, par exemple, dans une publication « *Traitements de données de santé : comment faire la distinction entre un entrepôt et une recherche et quelles conséquences* » du 2 mars 2023, l'autorité de protection des données a indiqué que : « *Lorsque le responsable de traitement envisage la constitution d'une importante base de données et la réutilisation des données contenues (« entrepôt »)* dans plusieurs projets de recherche, un raisonnement en deux temps doit être opéré car chaque traitement fait l'objet d'un régime juridique distinct : - la création de l'entrepôt de données en tant que tel (c'est-à-dire la collecte et la conservation des données dans une base unique pendant une plus longue durée) ; - les projets de recherches, d'études ou d'évaluations réalisés à partir des données conservées dans l'entrepôt par le même responsable de traitement ou d'autres organismes ». Par ailleurs, la Cnil a expliqué, dans les termes suivants, comment opérer la distinction entre un « *entrepôt de données de santé* » et

une « *recherche* » : « *Les entrepôts de données sont créés principalement pour collecter et disposer des données massives (données relatives à la prise en charge médicale du patient, données socio-démographiques, données issues de précédentes recherches, registre de pathologies, etc.). Ces données sont ensuite réutilisées, la plupart du temps partiellement, à des fins d'études, de recherches et d'évaluations dans le domaine de la santé. Ces bases de données sont constituées pour une longue durée (au moins 10 ans en général) et l'objectif est d'obtenir un volume de données important. Elles peuvent être alimentées par de multiples sources (professionnels de santé, patients, pharmacies, établissements de santé, etc.* ».

Dans un communiqué du 26 octobre 2021 annonçant la publication du référentiel, la Cnil a défini les entrepôts de données de santé comme des « *bases de données destinées à être utilisées notamment à des fins de recherche, d'études ou d'évaluation dans le domaine de la santé* ». Le référentiel, quant à lui, ne contient aucune définition de l'entrepôt de données de santé. Il précise toutefois qu'il s'applique aux responsables du traitement qui souhaitent « *réunir des données en vue de leur réutilisation, pour les finalités mentionnées au point 3.1 [telles que la production d'indicateurs et le pilotage stratégique de l'activité, l'amélioration de la qualité de l'information médicale, l'optimisation du codage dans le cadre du programme de médicalisation des systèmes d'information, le fonctionnement d'outils d'aide au diagnostic médical ou à la prise en charge, la réalisation d'études de faisabilité, ou plus généralement, la recherche ou l'étude dans le domaine de la santé]* ». À noter que plusieurs CHU ont eu l'occasion de solliciter et d'obtenir de la Cnil une autorisation dans le cadre de la constitution d'un entrepôt de données de santé regroupant des données produites lors de la prise en charge des patients du CHU et ce, à des fins de recherches[3]. Ces délibérations – tout comme celles qui ont été rendues dans d'autres cas de figure – n'apportent toutefois aucun éclairage supplémentaire sur la notion d'entrepôt de données de santé. En l'occurrence, il s'agissait, dans chacun de ces cas, d'un organisme qui décide – seul ou conjointement avec un partenaire – de regrouper des données de santé à des fins de recherches.

Selon le Health Data Hub, les entrepôts de données de santé visent à collecter et mettre à disposition des données « *qui peuvent être massives et issues de sources diverses (établissements de santé et notamment les hôpitaux, professionnels de santé, patients…)* », pour être ensuite « *réutilisées à des fins de recherche ou encore d'évaluation dans le domaine de la santé.* ». Le Health Data Hub précise que les établissements de santé, qui ont déployé des entrepôts de données de santé, visent principalement à « *industrialiser le recueil et le rassemblement de données* ». Une telle initiative leur permet (i) « *à moyen terme l'interconnexion des multiples sources de données de [l'établissement] ; (ii) « davantage de visibilité aux potentiels utilisateurs sur l'existant en matière de données (…) utilisables pour la recherche, l'innovation ou le pilotage* » et (iii) des opportunités de collaboration externe, y compris avec d'autres secteurs et à l'étranger[4].

Pour la Haute Autorité de Santé (HAS), les entrepôts de données de santé doivent être définis comme « *la mise en commun des données d'un ou plusieurs systèmes d'information médicaux, sous un format homogène pour des réutilisations à des fins de pilotage, de recherche ou dans le cadre des soins.* ». Ces réutilisations sont qualifiées de « *réutilisations secondaires* ». La HAS considère que la création d'entrepôts de données de santé repose sur plusieurs étapes. Il y a d'abord la collecte des données « *depuis les différentes sources constituant le SIH* » afin de « *centraliser ces données initialement cloisonnées dans chacun des SI* » dans un entrepôt de données de santé. Ensuite, vient l'étape de la transformation et de l'agrégation des données « *rarement homogènes* » et ce, « *afin d'aboutir à un entrepôt exploitable* ». La HAS précise par ailleurs que la notion d'entrepôt de données de santé intègre aussi « *la plateforme technologique utilisée pour transformer ces données* ». La troisième étape réside dans « *la mise à disposition « des jeux de données spécifiques (parfois nommés datamarts) à chaque usage secondaire de la donnée* ».5.

Pour le Comité consultatif national éthique, un entrepôt de données de santé est « *une infrastructure informatique qui rassemble en un lieu physique des données, pouvant être exprimées dans des formats variés, provenant de plusieurs sources souvent hétérogènes, et parfois de natures très différentes* ». On retrouve également la notion d'organisation / transformation des données (i) « *selon un modèle unifié de manière à faciliter pour l'utilisateur leur exploitation* » ou (ii) sans un tel modèle, « *dès lors que le lien entre les différentes données des bases de données rassemblées dans l'entrepôt peut être établi* ». Par ailleurs, le Comité indique qu'il y a de plus en plus d'appariements entre des entrepôts de données de santé et d'autres plateforme de données « *pour pouvoir permettre in situ des traitements sur leurs données.* »[6].

Au regard de tous ces éléments, la qualification d'entrepôt de données de santé pourrait ainsi notamment être retenue en présence des critères suivants : (i) collecte et stockage, sous forme homogène, de données de santé massives issues de sources diverses ; (ii) réutilisation de ces données à des fins de recherches (usage secondaire) dans le secteur de la santé.

La Cnil et le faisceau d'indices

À l'occasion d'une affaire contentieuse, la formation restreinte de la Cnil a récemment qualifié une base de données d'entrepôt de données de santé[7]. L'affaire concernait un éditeur équipant des cabinets médicaux et des centres de santé d'un logiciel de gestion d'agenda, de dossiers patients et de prescriptions. Dans ce cadre, l'éditeur proposait à certains de ses utilisateurs d'adhérer

à un observatoire pour collecter des données de dossiers patients traités par le logiciel pour qu'elles soient ensuite transmises et utilisées par d'autres clients de l'éditeur (dont des sociétés appartenant au groupe de l'éditeur), notamment pour réaliser des études en santé. À la suite d'un contrôle sur place, le rapporteur a considéré que, du fait de ces traitements, l'éditeur s'était constitué un entrepôt de données et aurait dû, pour ce faire, solliciter une autorisation de la Cnil, ce qu'il n'avait pas fait.

Dans son analyse, la formation restreinte a souligné que la notion d'entrepôt de données de santé n'est pas définie par la loi (en l'occurrence la loi Informatique et libertés), et qu'il s'agit d'« *une construction doctrinale de la Cnil (...)* ». L'autorité de protection des données, qui estime que la qualification d'un entrepôt de données de santé s'apprécie « *à l'aide d'un faisceau d'indices* », a listé les trois éléments qui lui semblent être « *déterminants* » pour une telle qualification : (i) « *la réutilisation des données dans des traitements ultérieurs* », (ii) « *l'alimentation au fil de l'eau de la base* », (iii) « *ainsi que [les] finalités du traitement* ». Elle a également précisé que ce faisceau d'indices doit tenir compte « *notamment, mais pas uniquement* » de la durée de conservation des données de santé à caractère personnel.

Dans le cas d'espèce, la Cnil a d'abord retenu que l'éditeur avait collecté « *massivement des données de santé de patients et de médecins* », et ce sur une période de plusieurs mois. Si la collecte de données massives ne fait pas partie des « *éléments déterminants* » retenus par la Cnil, ce critère a toutefois été utilisé par la Cnil. Ensuite, l'autorité a relevé que l'éditeur avait alimenté sa base « *au fil de l'eau, afin d'obtenir un volume important de données (remontée journalière des données depuis les postes médecins)* ». Enfin, la Cnil a constaté que l'éditeur mettait les données à disposition de ses clients à des fins « *d'études et des statistiques dans le domaine de la santé* ». La Cnil en a donc tiré la conclusion que l'éditeur s'était bien constitué un entrepôt de données de santé.

Cette décision nous livre un éclairage pratique bienvenu quant à la qualification d'une base de données en entrepôt de données de santé. Nous ne sommes toutefois pas à l'heure d'une pleine clarification. Certes, dans cette décision, la Cnil a souligné des éléments à prendre en compte dans le travail de qualification d'un entrepôt de données de santé, pour autant, ces éléments ne sont pas limitatifs. La prudence reste donc de mise...

Alexandre FIEVEE
Avocat associé

Alice ROBERT
Avocate of Counsel

DERRIENNIC ASSOCIES

Notes

(1) https://www.cnil.fr/sites/cnil/files/atoms/files/referentiel_entrepot.pdf

(2) À noter que l'organisme pourrait aussi se dispenser de formalité Cnil dans l'hypothèse théorique d'un recueil du consentement explicite des personnes concernées par les traitements de l'entrepôt de données de santé (collecte, enregistrement, conservation, etc.), sous réserve de pouvoir démontrer que les traitements mis en œuvre sont conformes au RGPD.

(3) Délibération 2020-028 du 27 février 2020 (eHop Rennes – CHU Rennes) ; Délibération n°2019-124 du 10 octobre 2019 (CHUGA-EDS – CHU Grenoble ; Délibération n°2019-103 (Include – CHU Lille).

(4) Health Data Hub, « Kit de creation d'un entrepôt de données de santé », janvier 2024.

(5) HAS, rapport « Entrepôts de données de santé hospitaliers en France. Quel potentiel pour la Haute Autorité de santé ? », 20 octobre 2022.

(6) Avis commun « Plateforme de données de santé : enjeux d'éthique », février 2023.

(7) Délibération SAN-2024-013 du 5 septembre 2024.

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info

DOCTRINE

RGPD

Comment piloter (de manière licite) la gouvernance des données ?

Comme chaque mois, Alexandre Fievée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en s'appuyant sur les décisions rendues par les différentes autorités nationales de contrôle au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur le rôle et les missions du DPO dans le cadre du pilotage, conformément au RGPD, de la gouvernance des données personnelles.

Le délégué à la protection des données (« *DPD* » ou « *DPO* ») est au cœur de la conformité au règlement européen sur la protection des données personnelles (« *RGPD* »).

Ainsi, en application de l'article 39-1 du RGPD, le DPO doit notamment informer et conseiller le responsable du traitement (ou le sous-traitant) ainsi que les employés sur leurs obligations en vertu du droit applicable en matière de protection des données personnelles. Pour ce faire, l'article 38-1 du RGPD précise que le DPO doit être « *associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.* » Le CEPD explique que « *l'information et la consultation du DPD dès le début [doivent permettre] de faciliter le respect du RGPD et d'encourager une approche fondée sur la protection des données dès la conception ; il devrait donc s'agir d'une procédure habituelle au sein de la gouvernance de l'organisme* »[1].

Le CEPD ajoute qu'il est fondamental que le DPD soit considéré comme un « *interlocuteur* » au sein de l'organisme et qu'il soit « *membre des groupes de travail* » consacrés aux activités de traitement de données personnelles.

Afin de permettre au DPO d'exercer effectivement ses missions, l'article 38-2 du RGPD souligne que l'organisme doit l'aider « *en fournissant les ressources nécessaires* », ce qui passe, selon le CEPD, par l'octroi de « *temps suffisant* » pour qu'il puisse accomplir ses tâches, mais aussi par un « *soutien adéquat du point de vue des ressources financières, des infrastructures (locaux, installations, équipements) et du personnel, le cas échéant* »[2].

L'affaire[3]

Une société avait mis au point, dès 2018, une gouvernance des données en nommant un DPD au niveau du groupe et des points de contacts locaux, au niveau de chaque société. À la suite de deux contrôles (l'un sur pièces, l'autre sur place) portant sur la fonction et le rôle du DPD, l'autorité luxembourgeoise de protection des données (la « *CNPD* ») a infligé à cette société une amende administrative en raison des manquements constatés aux dispositions des articles 38 et 39 du RGPD, ainsi qu'une injonction de se conformer à ces articles 38 et 39. Cette dernière a fait appel, sans succès, de cette décision devant le Tribunal administratif du Grand-Duché de Luxembourg.

La juridiction a d'abord estimé qu'il ne ressort pas des éléments du dossier que l'intervention du DPD du groupe se faisait conformément aux exigences règlementaires, dès lors qu'il ne réalisait qu'un contrôle a posteriori des décisions d'ores-et-déjà prises par les points de contacts locaux. En d'autres termes, le DPD du groupe n'était pas associé en temps utile aux questions relatives à la protection des données personnelles. Deux éléments ont retenu l'attention de la juridiction : d'une part, le fait

qu'il n'était pas démontré la mise en place, au niveau du groupe, d'une « *politique commune* » pour les différents points de contacts locaux quant à la décision à adopter au niveau des différents traitements de données personnelles ; d'autre part, la société n'a pas été en mesure d'établir qu'il existait une « *communication régulière* » entre le DPD du groupe et ses points de contacts locaux, « *par le biais d'appels téléphoniques, de visioconférences et de courriers électroniques* », visant à échanger sur la position à adopter sur les problématiques rencontrées par ces derniers au niveau local.

La juridiction a ensuite reproché à la société de ne pas avoir quantifié ni formalisé le temps de travail que le DPD et son équipe devaient allouer à leurs missions, ni les ressources dont ils avaient effectivement besoin. En tout état de cause et sur la base des éléments en sa possession, le tribunal administratif a estimé, conformément à la décision de la CNPD, que le DPD du groupe et ses points de contact ne disposaient pas des ressources suffisantes pour exercer leurs missions : « *Force est de constater que l'activité de la demanderesse a une envergure certaine au Luxembourg pour englober (...) 70 sites, entre 1 600 et 2 100 salariés et quotidiennement 25 000 consommateurs, de sorte que, d'une part, l'exigence de la CNPD que la demanderesse aurait dû, au moins, charger une personne travaillant à plein temps sur les questions relatives à la protection des données à caractère personnel ne peut être mis en cause, et, d'autre part, que le temps de travail consacré initialement par le point de contact à ladite tâche (...), durée que la demanderesse a quantifiée comme correspondant à un travail à mi-temps, a, à juste titre, été retenue par la CNPD comme étant insuffisant.* »

Quelles recommandations ?

Dans son rapport de 2024 faisant suite aux contrôles menés par les différentes autorités nationales de protection des données dans le cadre de son action coordonnée 2023[4], le CEPD avait mis en exergue les insuffisances décrites dans l'affaire commentée. Plusieurs recommandations avaient été émises visant à encourager les organismes à se mettre dans le droit chemin... Cette décision montre qu'une organisation - qui pourtant repose sur, d'une part, un DPO groupe et, d'autre part, des points de contact locaux - reste critiquable, dès lors que le DPO ne participe pas aux prises de décisions, en laissant ses équipes – à temps partiel – participer aux réunions et ce, sans échange préalable sur la position à adopter. Il est donc fondamental, dans ce type d'organisation, que le DPO soit, grâce notamment à des ressources adaptées, davantage impliqué en amont et qu'il délivre à ses équipes des lignes directrices sur les positions à adopter selon les cas d'usage.

Alexandre FIEVEE
Avocat associé
Derriennic Associes

Notes

(1) CEPD, Lignes directrices concernant le délégué à la protection des données, 5 avril 2017.

(2) CEPD, Lignes directrices concernant le délégué à la protection des données, 5 avril 2017.

(3) Tribunal administratif du Grand-Duché de Luxembourg, 4e chambre, 14 mai 2024.

(4) CEPD, rapport « Mesures d'application coordonnées - Désignation et poste des délégués à la protection des données », 16 janvier 2024.

VU DANS LA PRESSE

« DSIH », NOVEMBRE 2024

RECHERCHE CLINIQUE : LES CRO ONT DESORMAIS LEUR PROPRE CODE DE CONDUITE

La CNIL vient d'adopter le Code de conduite pour les prestataires de service en recherche clinique (CRO) [1]. Ce nouveau code, porté par la fédération EUCROF (European Clinical Research Organisations Federation), vise à répondre aux enjeux identifiés par le secteur en matière de protection des données personnelles.

Un code de conduite, c'est quoi ?

Il s'agit d'un outil juridique prévu par le RGPD, qui a pour objet de répondre aux besoins opérationnels de professionnels. Il permet notamment, selon la CNIL, « *de construire un socle commun de bonnes pratiques, de contribuer à démontrer sa conformité au RGPD et d'envoyer un signal positif aux clients et aux professionnels du secteur d'activité concerné* » [2].

Un code conduite a une force contraignante pour l'organisme qui y adhère. Il oblige ainsi les adhérents à se conformer aux règles écrites dans le code et à accepter qu'un organisme tiers contrôle sa bonne application.

Pourquoi un code dédié aux activités des CRO ?

La CNIL indique que ce nouveau code a pour objectif « *de décrire de manière opérationnelle les engagements pris par les sociétés privées qui fournissent, sur une base contractuelle, des services dans le domaine de la recherche en santé, notamment pour l'industrie pharmaceutique, en tant que sous-traitants (au sens de l'article 28 du RGPD) dans le cadre de l'exécution du contrat qui les lie au promoteur*. [3] »

Selon la Présidente de la CNIL, cet outil juridique est essentiel en ce qu'il permettra une « *diffusion harmonisée de bonnes pratiques* » auprès de nombreux acteurs, avec « *des réponses pragmatiques et concrètes, adaptées aux enjeux des professionnels du secteur* ».

Que contient ce code dédié aux CRO ?

Son champ d'application est relativement large puisqu'il couvre une grande partie des services proposés par les CRO, à savoir notamment la conception du protocole ou du cahier d'observations, la sélection et la contractualisation avec les centres investigateurs, la collecte et l'hébergement des données, leur analyse et la production de rapports, ou encore des services d'archivage ou de support technique.

Ce code rappelle le cadre général pour la protection des données applicable aux CRO, mais aussi décrit les grands principes (licéité, loyauté, transparence, etc.) qu'ils doivent respecter, leurs obligations en tant que sous-traitant (au sens du RGPD), ainsi que les conditions et modalités du contrôle par le comité de surveillance (COSUP) de l'application du code par les adhérents.

Quoi d'autre encore ?

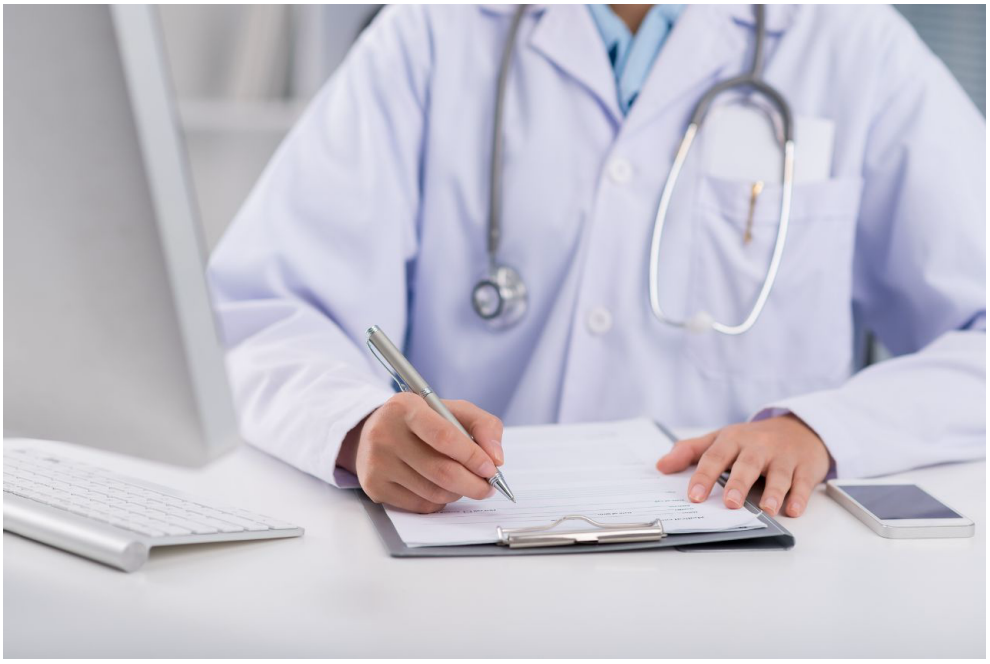
L'EUCROF a publié un certain nombre de documents complémentaires. Ces documents ne font pas partie du code et n'ont pas été approuvés par les Autorités Européennes de contrôle de la protection des données. Ils constituent une « boîte à outils » avec des modèles de documents et des guides destinés à faciliter la mise en œuvre du code par les candidats adhérents.

L'utilisation de ces outils n'est ni normative ni obligatoire. Cela signifie que les CROs peuvent utiliser toute ou une partie des outils selon leur propre choix.

[1] Délibération n° 2024-064 du 12 septembre 2024 portant approbation du code de conduite européen porté par la fédération EUCROF (European Contract Research Organisation Federation) (Demande d'approbation n° 21000034).

[2] https://www.cnil.fr/fr/recherche-clinique-la-cnil-approuve-le-code-de-conduite-europeen-de-la-federation-eucrof

[3] Promoteur : « *personne physique ou morale qui est responsable d'une recherche clinique, en assure la gestion, vérifie que son financement est prévu et qui détermine les finalités et les moyens des traitements nécessaires à celle-ci* ».



VU DANS LA PRESSE

« BFM BUSINESS », DECEMBRE 2024

ECONOMIE

COURTISER OU CONDUIRE, IL FAUT CHOISIR

Par Alexandre Fievée, avocat associé du cabinet Derriennic Associés Le 10/12/2024 à 15:14

Image d'illustration - Un homme en train de conduire, au volant d'un véhicule - Pexels

[AVIS D'EXPERT] Un conducteur commet-il une faute en utilisant le numéro de téléphone de la mère d'une usagère pour lui adresser un sms, dans lequel il lui déclare sa flamme? C'est à cette question que la Cour d'appel de Bordeaux a dû répondre, dans un arrêt du 14 août 2024.

Un salarié avait été engagé en qualité notamment de conducteur accompagnateur de personnes présentant un handicap ou à mobilité réduite par une entité dont l'activité principale est le transport adapté.

Un sms inapproprié?

La situation de ce salarié a basculé lorsque son employeur a reçu de l'un de ses clients – le Conseil départemental de la Charente – un courriel l'alertant de son comportement inapproprié. Il était en effet reproché au conducteur d'avoir adressé un sms à la mère de l'une des enfants pris en charge, dans lequel il lui déclarait sa flamme. Cette

dernière s'en est plainte au Conseil départemental et a demandé que ce que le conducteur soit remplacé, n'osant plus accompagner sa fille jusqu'au véhicule.

L'employeur, qui a pris l'affaire au sérieux, a convoqué le salarié à un entretien préalable, puis lui a notifié une rupture anticipée de son contrat à durée déterminée pour faute grave, "en raison de son comportement inadapté envers un usager et l'utilisation de données professionnelles confidentielles dans un intérêt personnel". Selon l'employeur, le comportement du conducteur avait enfreint plusieurs règles, souligne cet arrêt du 14 août 2024 du CA Bordeaux, chambre sociale, section A, n° 21/04476 :

- le book conducteur, qui impose un comportement professionnel en toute circonstance
- la charte de bonne conduite qui interdit "les propos à caractère sexuel provenant d'un conducteur accompagnateur"
- et le règlement intérieur qui prévoit que les salariés sont tenus à "une attitude correcte" dans le cadre des rapports avec la clientèle.

C'est dans ce contexte que le salarié a saisi le conseil de prud'hommes d'Angoulême en vue notamment de contester la légitimité de la rupture de son contrat de travail.

Selon lui, il n'avait enfreint aucune des prescriptions de la charte de bonne conduite applicable dans l'entreprise et du règlement intérieur, puisque ses messages non seulement ne contenaient aucun propos déplacé, mais aussi avaient été envoyés en dehors de ses heures de service et avec son téléphone personnel. Par ailleurs, il soutenait qu'il s'était contenté d'utiliser un numéro de téléphone qui avait été mis à sa disposition par l'entreprise. Le salarié, débouté de toutes ses demandes en première instance, a donc interjeté appel.

Attention à l'usage qui est fait des données

Le conducteur n'a pas eu plus de succès devant la juridiction du second degré, qui a considéré comme établie la réalité des faits reprochés dans la lettre de rupture: "L'employeur souligne que les faits en cause, caractérisant un manquement de M. [V] à ses obligations contractuelles, rendaient, par leur nature, le maintien du salarié dans l'entreprise impossible. Ce moyen doit être considéré comme pertinent, au regard des faits en cause, du contexte de leur commission, le salarié s'étant permis de joindre Mme [W] pour lui déclarer sa flamme alors que son numéro de téléphone ne lui avait été communiqué qu'à des fins professionnelles mais également en raison de leur retentissement sur un public vulnérable et du potentiel impact sur la relation commerciale avec le conseil départemental de la Charente, exigeant une conduite irréprochable du transporteur".

La Cour d'appel de Bordeaux a donc considéré que le comportement du conducteur n'était pas adapté au regard du contexte et qu'en tout état de cause il n'aurait pas dû utiliser à des fins personnelles le numéro de téléphone de la mère de l'une des

usagères, sachant que ce numéro lui avait été remis dans un cadre strictement professionnel.

Des décisions similaires en Allemagne

Si cette décision est assez originale en France, il n'est pas rare de trouver, dans d'autres pays, des affaires similaires, étant précisé qu'elles sont, le plus souvent, abordées non pas sous l'angle du droit du travail – comme en l'espèce – mais sous l'angle de la protection des données personnelles.

En Allemagne, une cliente, qui s'était rendue dans un restaurant, avait, en application de la règlementation en vigueur dans le pays au moment des faits (période du COVID), renseigné ses coordonnées - dont son numéro de téléphone mobile personnel - sur une fiche dédiée. Le lendemain, cette personne avait eu la surprise d'être contactée sur Messenger par l'un des serveurs. Elle avait déposé une plainte devant l'autorité allemande de protection des données et le serveur a été sanctionné pour avoir détourné les données de leur finalité initiale, comme le rappelle le rapport annuel 2022 du Commissaire à la protection des données de la ville de Brême (Allemagne).

Des exemples de ce type sont nombreux. On pense notamment à cet agent de sécurité qui avait recontacté une personne accusée de vol à l'étalage grâce aux coordonnées recueillies au moment du contrôle en magasin, précise alors le Rapport annuel 2023 de l'Office bavarois de la protection des données (BayLDA) (Allemagne) ou encore à cette patiente d'un laboratoire de biologie médicale qui avait été sollicitée sur Instagram, le lendemain de son test, par un membre du personnel de cet établissement, note le Rapport annuel 2022 du Commissaire à la protection des données de la ville de Brême (Allemagne).

Les données que nous collectons dans un cadre professionnel répondent à une finalité. Les détourner de cette finalité, notamment dans le cadre d'un usage personnel, s'analyse comme une faute qui peut donner lieu à des sanction. Prudence.

Par Alexandre Fievée, avocat associé du cabinet Derriennic Associés

ACTUALITÉS DU CABINET

DERRIENNIC ASSOCIÉS PROPOSE UN PROGRAMME DE FORMATION DE 35 HEURES POUR LA PRÉPARATION À LA CERTIFICATION DPO

OBJECTIFS

1/ Acquérir les compétences, les connaissances et le savoir-faire attendus par la CNIL et permettre au collaborateur de se présenter à l'examen de certification en maximisant ses chances de succès.

2/ Indépendamment de la certification, la formation permet à l'apprenant de se familiariser avec la matière et d'acquérir les compétences, les connaissances et le savoir-faire pour :

- analyser une situation impliquant un traitement de données personnelles ;
- définir et appréhender les problématiques, les enjeux et les risques qui en découlent ;
- prendre les décisions qui s'imposent en concertation avec l'équipe « DPO ».

CONTENU DE LA FORMATION

Partie 1 - Réglementation générale en matière de protection des données et mesures prises pour la mise en conformité

Partie 2 - Responsabilité (Application du principe d'« Accountability »)

Partie 3 – Mesures techniques et organisationnelles pour la sécurité des données au regard des risques

COÛT

4.000 € HT/personne

INTERVENANT

Alexandre FIEVEE
Avocat Associé
01.47.03.14.94
afievee@derriennic.com

CLASSEMENTS

Alexandre Fievee figure dans le classement BestLawyers dans la catégorie « *Information Technology Law* » (2024).

Il a également fait en 2020 son entrée dans le classement Legal 500 dans la catégorie *« Next Generation Partners* ».

RENSEIGNEMENTS PRATIQUES

Prochaine session en 2024/2025 :
Sur demande.

Lieu de la formation :
Au cabinet Derriennic Associés (5 avenue de l'opéra - 75001 Paris) ou en visio-conférence.

Inscription et informations :
afievee@derriennic.com