NEWSLETTER RGPD/DATA

NUMÉRO 61 ● 2024

SOMMAIRE

ACTUALITE

VU DANS LA PRESSE

ACTUALITES DU CABINET P. 20p

FORMATION A LA PREPARATION A LA CERTIFICATION « DPO ».
DATE SUR DEMANDE

SANCTION SIMPLIFIEE : UNE PROCEDURE UTILISEE PAR LA CNIL POUR CONTROLER LES DPO

Dans une publication du 12 mars 2024, la CNIL est revenue sur quinze sanctions qu'elle a prononcées dans le cadre de la procédure de « sanction simplifiée ». Elle insiste notamment sur l'utilisation de cette procédure pour contrôler les DPO.

Entre janvier et mars 2024, la CNIL a prononcé quinze sanctions en ayant recours à la procédure de « *sanction simplifiée* ».

Ces décisions sanctionnent des responsables du traitement qui, par exemple, ont manqué à leurs obligations :

- de coopérer avec la CNIL ;
- de respecter le droit des personnes ;
- d'informer les personnes concernées ;
- d'assurer la sécurité des données personnelles.

La CNIL explique également avoir utilisé cette procédure pour contrôler la place du DPO dans l'organisme et s'assurer que ce dernier respecte ses missions et dispose de ressources suffisantes.

La CNIL a notamment indiqué avoir sanctionné un responsable du traitement :

- Qui n'a pas associé son DPO aux réunions intéressant la protection des données et la sécurité des systèmes d'information. La CNIL rappelle que le DPO a « *pour mission d'informer et de conseiller le responsable du traitement sur ses obligations légales et d'en contrôler le respect* », ce qui suppose que le DPO soit associé aux échanges qui concernent la protection des données personnelles ;

- Qui n'a pas affecté à son DPO les ressources suffisantes pour accomplir correctement ses missions. La CNIL a effectivement constaté que (i) « les coordonnées et les missions du DPO n'avaient fait l'objet d'aucune communication auprès des employés depuis plusieurs années » et que (ii) le « *DPO n'avait pas accès à la messagerie du site internet de l'organisme permettant aux personnes concernées d'exercer leurs droits* ».

Source : ici

LITIGE EMPLOYEUR / SALARIE : UNE PREUVE OBTENUE DE FAÇON ILLICITE EST-ELLE UTILISABLE ?

La Cour de cassation, dans un arrêt du 14 février 2024, a considéré que les images issues d'un dispositif de vidéosurveillance illicite pouvaient néanmoins être admises en tant que preuves dans le cadre d'une procédure de licenciement.

Une entreprise, ayant constaté des écarts de stocks importants, a placé certains de ses salariés sous une surveillance vidéo permanente pendant près de vingt jours et a utilisé, en tant que preuve, les images issues du dispositif de vidéosurveillance afin de justifier le licenciement d'une salariée fautive. La Cour de cassation a eu à apprécier de la recevabilité de ces images.

Un moyen de preuve obtenu de façon illicite

La salariée licenciée estimait que le système de vidéosurveillance utilisé par l'employeur était illicite, aux motifs suivants :

- l'employeur n'a pas procédé à la consultation des représentants du personnel ;
- l'employeur n'a pas porté ce dispositif de contrôle à la connaissance des salariés ;
- ce systèmes de vidéosurveillance, installé dans un lieux ouvert au public, n'a pas reçu d'autorisation préfectorale ;
- les salariés étaient placés, via ce système, sous une surveillance permanente pendant vingt jours, portant ainsi une atteinte disproportionnée à leur vie personnelle.

Pour la salariée, la cour d'appel aurait dû rechercher si l'employeur ne pouvait pas atteindre un résultat identique en utilisant d'autres moyens plus respectueux de la vie personnelle du salarié . En l'espèce, pour la salariée, son employeur aurait pu utiliser un moyen de preuve moins intrusif, à savoir visionner les images de vidéosurveillance captées antérieures à la constatation de l'écart de stocks, plutôt que placer ses salariés sous une surveillance constante.

Un moyen de preuve obtenu de façon illicite peut néanmoins être recevable, s'il est indispensable à l'exercice du droit à la preuve et proportionné au but recherche

La chambre sociale de la Cour de cassation a rappelé que « *l'illicéité dans l'obtention ou la production d'un moyen de preuve ne conduit pas nécessairement à l'écarter des débat* ».

Pour la Cour de cassation, la juridiction du second degré a bien « *mis en balance de manière circonstanciée le droit de la salariée au respect de sa vie privée et le droit de son employeur au bon fonctionnement de l'entreprise, en tenant compte du but légitime qui était poursuivi par l'entreprise, à savoir le droit de veiller à la protection de ses biens* ».

La Cour de cassation a, en conséquence, confirmé le raisonnement de la Cour d'appel, qui avait estimé que les images issues du dispositif de vidéosurveillance étaient « *indispensables à l'exercice du droit à la preuve de l'employeur et proportionnée au but poursuivi », de sorte que « les pièces litigieuses étaient recevables* ».

Le rejet du pourvoi s'est donc imposé.

Il doit toutefois être rappelé, à toutes fins utiles, que l'illicéité du dispositif en cause met en lumière un certain nombre de manquements, notamment au RGPD, susceptibles d'engager la responsabilité de l'employeur.

Source : ici

COMMUNICATION ORALE DE DONNEES PERSONNELLES ET RGPD

Une communication orale de données à caractère personnel constitue-t-elle un traitement de données à caractère personnel soumis au RGPD ? La CJUE a récemment répondu par l'affirmative, sous réserve du respect de certaines conditions.

Le litige : une demande de communication orale de données sensibles

L'affaire concernait la société ENDEMOL, laquelle avait demandé oralement à une juridiction des informations sur des éventuelles condamnations pénales en cours ou déjà purgées d'une personne physique. Cette personne était une participante à un concours organisé par ENDEMOL.

La juridiction n'a pas fait droit à cette demande au motif, notamment de l'interdiction de principe de traitement des données relatives aux infractions et condamnations pénales (selon l'article 10 du RGPD).

ENDEMOL a contesté cette position, considérant que la communication orale des informations sollicitées ne constitue pas un traitement de données à caractère personnel au sens du RGPD.

La position de la CJUE : une communication orale de données à caractère personnel relève du RGPD

Pour la CJUE, la notion de « traitement » au sens du RGPD couvre nécessairement la communication orale de données à caractère personnel.

A cet égard, la Cour a précisé que la notion de traitement à une portée large visant notamment la communication par transmission, la diffusion et « *toute autre forme de mise à disposition* », ces opérations pouvant être automatisées ou non automatisées.

Toutefois, pour que le RGPD s'applique à ce traitement, encore faut-il, rappelle la Cour, qu'il relève du champ d'application matériel de la loi, ce qui requiert que les données concernées par le traitement soient contenues ou appelés à figurer dans un fichier.

Selon la CJUE, la notion de « fichier » doit être entendue largement et, notamment, comme visant tout ensemble structuré de données à caractère personnel « *selon des critères déterminés* », sans exigences en termes de modalités ou de forme. Il suffit alors que le fichier « *[permette] que les données relatives à une personne puissent être retrouvées aisément* ».

La CJUE a relevé que cette condition est, a priori, remplie en l'espèce, dans la mesure où il ressort du dossier que les données sont « *contenues dans un fichier de données à caractère personnel tenu par une juridiction* ». La Cour a précisé qu'il appartiendra à la juridiction de renvoi de vérifier ce point « *sans qu'il importe de savoir si lesdites données sont contenues dans des bases de données électroniques ou encore dans des dossiers ou registres physiques* ».

La communication orale d'informations constitue donc bien un traitement de données à caractère personnel relevant du champ d'application matériel du RGPD, dès lors que ces informations sont contenues ou appelées à figurer dans un fichier.

Source : ici

PROSPECTION COMMERCIALE : L'ACHAT DE DONNEES AUPRES D'UN COURTIER ET LA QUESTION DE LA BASE LEGALE

Le 31 janvier 2024, la CNIL a prononcé à l'encontre de la société FORIOU une amende de 310 000 € pour avoir réalisé de la prospection commerciale par téléphone sans base légale valable.

La société FORIOU a pour activité la commercialisation de programmes de fidélité. Afin de promouvoir lesdits programmes, la société a procédé à des campagnes de démarchage par téléphone à partir de fichiers de prospects achetés auprès de partenaires (courtiers en données).

L'étendue du contrôle de la CNIL : la prospection commerciale par appel téléphonique

Conformément à l'article 6 du RGPD, tout traitement de données personnelles doit reposer sur une base légale. Dans le cas d'espèce, plusieurs traitements étaient mis en œuvre :

- la collecte des données, réalisée par le courtier en données ;
- la transmission des données, également réalisée par le courtier en données ;
- la collecte des données (réception des données transmises par le courtier), réalisée par FORIOU ;
- l'utilisation des données, réalisée par FORIOU à des fins de prospection commerciale par appel téléphonique.

Dans le cadre de son contrôle, la CNIL s'est uniquement interrogée sur l'existence d'une base légale valable pour le 4ème traitement.

La recherche d'une base légale valable pour la prospection commerciale

FORIOU n'étant pas en mesure d'indiquer sur quelle base légale son activité de prospection commerciale était fondée, la CNIL a rappelé que de tels traitements peuvent uniquement être fondés sur l'intérêt légitime de la société ou sur le consentement. Elle a donc recherché si ces bases légales étaient invocables en l'espèce.

La CNIL a considéré que :

Dans un premier temps, FORIOU ne pouvait pas fonder ses opérations de prospection commerciale sur son intérêt légitime. En effet, après avoir analysé les supports de collecte des courtiers en données, la CNIL a constaté que FORIOU n'était pas listée parmi les partenaires susceptibles de démarcher les personnes concernées et qu'ainsi ces dernières ne pouvaient légitimement s'attendre à recevoir des offres commerciales de la société ;

Dans un second temps, FORIOU ne pouvait pas fonder ses opérations de prospection commerciale sur le consentement des personnes concernées. Effectivement, après avoir analysé les supports de collecte des courtiers en données, la CNIL a considéré que le consentement recueilli par le courtier n'était pas « univoque, spécifique, libre et éclairé ».
Compte tenu de ce qui précède, la CNIL a prononcé une amende de 310 000 euros à l'encontre de la société FORIOU, précisant que « *l'écosystème de la revente des données de partenaires en partenaires exige des garanties particulièrement fortes quant à la qualité et à la validité du consentement obtenu par le primo-collectant des données et dont les partenaires se prévalent à des fins de prospection commerciale* » et que « *l'organisme qui se prévaut d'un tel consentement pour mener des opérations de prospection commerciale endosse une responsabilité essentielle lui imposant […] de s'assurer que les conditions lui permettant de réaliser lesdites opérations sont réunies, indépendamment de la responsabilité éventuelle des fournisseurs de données, primo-collectants* ».

Source : ici

ATTENTION A L'ARRIERE-PLAN DE VOS PHOTOGRAPHIES : L'EXCEPTION DOMESTIQUE NE S'APPLIQUE PAS TOUJOURS

L'autorité de contrôle maltaise a sanctionné un couple qui avait transmis en justice une photographie dans laquelle apparaissait, en arrière-plan, une personne et son enfant.

Dans le cadre d'un contentieux les opposant au service de l'urbanisme d'une commune, un couple a saisi le tribunal de l'environnement et a joint, comme preuve à l'appui de ses prétentions, deux photographies.

Sur ces photographies figuraient, en premier plan, la fille du couple, floutée, et, en arrière-plan, une femme et son enfant mineur, non floutés. La femme, étant partie au procès devant le tribunal de l'environnement, a eu connaissance de l'existence et de la transmission de ces photographies et a déposé une plainte auprès de l'autorité de contrôle maltaise.

Appelé à présenter ses observations pour sa défense, le couple a indiqué :

- Qu'il s'agit de photos pixelisées sur lesquelles le plaignant et son enfant ne sont pas identifiables ;
- Que le RGPD ne s'applique pas car le traitement est réalisé dans le cadre d'une activité strictement personnelle ou domestique » et donc qu'il entre dans l'exception posée à l'article 2 dudit texte puisque les photographies litigieuses sont des photographies de famille prises au domicile familial dans un cadre privé ;
- Que le traitement des photographies est licite, car « *nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice* » ;
- Que les photographies n'ont été transmises que dans le cadre d'un recours en justice, seul le tribunal et la partie adverse y avaient accès.

L'autorité de contrôle a :

- Dans un premier temps, examiné les photographies et a conclu qu'il y a bien un traitement de données personnelles car « les personnes apparaissant sur les photographies peuvent être reconnues et effectivement identifiées » ;
- Dans un deuxième temps, rappelé le principe de « l'exception domestique » posée à l'article 2 du RGPD, et indiqué que cette exception devait être écartée en l'espèce. Se fondant sur la jurisprudence européenne, elle a considéré que cette exception « ne couvre que les activités qui se déroulent dans le cadre de la vie privée ou familiale des personnes » et qu'ainsi « une activité ne peut être considérée comme exclusivement personnelle ou domestique, au sens de cette disposition, lorsqu'elle a pour objet de rendre des données à caractère personnel accessibles à un nombre indéfini de personnes, ou lorsque cette activité s'étend, même partiellement, au domaine public et, par conséquent, sort de la sphère privée du responsable du traitement des données », ce qui était le cas en l'espèce ;

- Dans un troisième temps, considéré que le couple n'avait pas de base légale pour traiter les données personnelles de la plaignante et de son enfant d'autant que si ces personnes « *avaient été floutées, le responsable du traitement aurait tout de même atteint son objectif* ».

Compte tenu de ce qui précède, l'autorité de contrôle a adressé au couple un rappel à l'ordre.

Source : ici

LES PROFESSIONNELS DE SANTE PEUVENT UNIQUEMENT ACCEDER AUX DOSSIERS MEDICAUX DE LEURS PATIENTS

L'autorité de contrôle chypriote a sanctionné un professionnel de santé ayant eu accès à un dossier médical qui n'était pas celui de son patient.

L'état chypriote a mis en place le « *système général de santé* », portail connecté permettant à tous les professionnels de santé d'accéder aux dossiers médicaux des chypriotes, à condition cependant pour le professionnel de santé (i) de fournir le nom, la date de naissance et un numéro d'identification unique de la personne et (ii) de démontrer être autorisé à accéder au dossier médical de la personne (autorisation du patient, existence d'une relation de patientèle, etc.).

Une personne a constaté qu'un professionnel de santé qui lui était inconnu avait eu accès à son dossier médical et a déposé une plainte auprès de l'autorité de contrôle.

Pour sa défense, le professionnel de santé a avancé deux hypothèses :

- Il a pu avoir accès au dossier médical du patient par erreur ;
- Il a pu être sollicité, par téléphone, en urgence par le patient afin d'obtenir un avis sur ses examens médicaux et aurait demandé un rendez-vous médical en urgence. Le professionnel de santé aurait ainsi accédé au dossier médical, mais aucun rendez-vous n'aurait été pris par la suite.

En tout état de cause, le professionnel de santé considérait que l'accès au dossier médical avait été réalisé sans intention malveillante et dans le strict respect total du secret médical.

Le plaignant indiquait, de son côté, ne pas connaitre le praticien, n'avoir jamais fréquenté son cabinet et ne l'avoir jamais appelé.

L'autorité de contrôle a :

- Rejeté l'hypothèse de l'erreur de patient, les chances de se connecter sur le profil de la mauvaise personne étant « infinitésimales » ;
- Rejeté l'hypothèse de l'appel, le professionnel de santé n'étant pas en mesure de prouver que les informations avaient été directement obtenues auprès de la personne concernée.

En outre, l'autorité a considéré que l'absence d'intention malveillante et le respect du secret médical n'avaient aucune incidence sur l'illicéité du traitement.

Compte tenu de ce qui précède, l'autorité de contrôle a (i) considéré que le professionnel de santé avait violé les principes de licéité, de loyauté et de transparence et (ii) infligé au médecin une amende de 1500 €.

Source : ici

L'EMPLOYEUR, QUI COMMUNIQUE LES DONNEES PERSONNELLES DE SON SALARIE, DOIT L'EN INFORMER

L'autorité de contrôle italienne a sanctionné un employeur qui avait transmis à une banque les données personnelles de son salarié sans l'en informer.

Un salarié, responsable du service de restauration, avait la charge du versement des recettes de l'établissement sur le compte courant de la société, grâce à une carte bancaire de dépôt nominative.

Ayant ouvert un nouveau compte courant auprès d'une autre banque, l'employeur a transmis à la nouvelle banque les données personnelles de son salarié afin que cette banque édite une nouvelle carte bancaire de dépôt, également nominative.

Le salarié, contacté par la banque, a considéré que son employeur avait traité ses données personnelles en violation du RGPD, et a déposé une plainte auprès de l'autorité de contrôle italienne.

Pour sa défense, l'employeur indiquait :

- Qu'en plus de ne transmettre que les informations strictement nécessaires à la banque, il avait mis en place une mention d'information à destination de son personnel ;
- Qu'en raison « *du rôle et des fonctions de l'employé* », le traitement réalisé reposait sur une base légale valide, à savoir l'exécution du contrat de travail.

L'autorité de contrôle a considéré :

- D'une part, que la mention d'information mise en place par l'employeur n'était pas suffisante car « *la formulation est très générale et, en tout état de cause, insuffisante pour informer de manière adéquate les personnes concernées sur les sujets ou les catégories de sujets auxquels les données peuvent être communiquées, sur le type de personne concernée par la communication, sur les finalités et sur la légitimité qui sous-tend le traitement en question* » ;

- D'autre part, que « *ni l'exécution du contrat ni l'intérêt légitime du responsable du traitement ne peuvent être considérés comme des bases juridiques appropriées* » :

    - Concernant l'exécution du contrat, l'autorité de contrôle a estimé que le traitement n'était pas « *objectivement nécessaire à l'exécution du contrat* », pour preuve, le salarié était toujours en poste et toujours responsable du service de la restauration même après s'être opposé au traitement de ses données personnelles dans le cadre de la création de la carte de dépôt ;

    - Concernant l'intérêt général, l'autorité de contrôle a constaté que le responsable du traitement n'avait pas procédé à une mise en balance pour évaluer la possibilité de recourir à cette base légale.

Compte tenu de ce qui précède, l'autorité de contrôle a infligé à l'employeur une amende de 1000 euros et l'a enjoint à se mettre en conformité au RGPD en « rédigeant une note d'information appropriée ».

Source : ici

SECURITE DES DOSSIERS PATIENT INFORMATISES : LA CNIL MET LA PRESSION SUR LES ETABLISSEMENTS DE SANTE

Dans une communication récente, la CNIL a mis en avant l'insuffisance des mesures mises en œuvre par les établissements de santé visant à garantir la sécurité de leurs dossiers patients informatisés (DPI). Le grief principal est le suivant : trop de personnel au sein de ces organismes aurait accès aux données de santé des patients. Les enjeux éthiques et juridiques sont énormes. Des mesures d'amélioration sont proposées par la CNIL, valables pour toutes les structures de soins où de nombreuses personnes ont accès aux dossiers des patients. Nos avocats en droit de la e-santé vous éclairent.

La sensibilité du dossier patient informatisé (DPI)

Le dossier patient informatisé (DPI), fichier dans lequel est centralisé l'ensemble des données de santé des patients pris en charge par l'établissement de santé ou toute structure de soins, permet aux professionnels de santé de ce lieu d'exercice d'accéder facilement à leurs informations médicales.

Compte tenu du volume et de la sensibilité des données qu'il contient, le DPI doit, selon la CNIL, faire l'objet de *« mesures de sécurité renforcées* ». Mais, force est de constater que ces mesures sont bien souvent insuffisantes, ne serait-ce qu'en raison de l'application d'une politique de gestion des habilitations inadaptée, permettant notamment à des catégories de personnels d'accéder à des données qu'elles n'ont pas besoin de connaître.

Les mesures de sécurité préconisées par la CNIL

Afin de renforcer la sécurité du dossier patient informatisé, la CNIL préconise le choix de règles répondant à l'exigence selon laquelle un professionnel de santé ou un agent/personnel ne peut accéder qu'aux données qu'il a strictement besoin de connaître.

Dans la définition de ces règles, deux critères peuvent être retenus :

- Le critère du « *métier exercé* », qui signifie qu'un agent/personnel responsable de l'accueil des patients dans la structure de soins ne doit accéder « *qu'au dossier administratif du patient et non aux données médicales* », alors qu'un médecin ou un professionnel de santé pourra, bien entendu, accéder au dossier administratif mais « *également aux données médicales* » ;

- Le critère de l'équipe de soins [telle que définie par la loi (art. L.1110-12 du Code de la santé publique)], qui signifie que seuls les professionnels effectivement impliqués dans la prise en charge d'un patient ou dans les soins qui lui sont prodigués doivent pouvoir avoir accès aux données couvertes par le secret médical.

Consciente des enjeux et des nécessités du métier et des situations d'urgence dans lesquelles se trouve confronté le personnel de ces établissements, la CNIL précise toutefois que les habilitations accordées peuvent être complétées d'un « *mode bris de glace* », afin de permettre aux agents/personnels administratifs et professionnels de santé d'avoir accès à d'autres données pour tout patient.

D'autres mesures peuvent venir compléter cet arsenal, comme la mise en place d'une politique d'authentification robuste, qui devrait prévoir à minima :

- Un identifiant unique par utilisateur et interdire les comptes partagés entre plusieurs utilisateurs
- Le recours à des mots de passe suffisamment complexes.

L'implémentation d'un dispositif de journalisation permettant de tracer les accès au DPI est également recommandée par la CNIL : « *cette traçabilité doit non seulement permettre d'indiquer qui s'est connecté à la base de données à quel moment, mais, plus précisément, qui a accédé à quoi. Des contrôles réguliers de ces accès doivent être opérés, afin d'identifier ceux susceptibles d'être frauduleux ou illégitimes. Il est vivement recommandé de disposer d'un système d'analyse automatique des journaux de connexion afin de repérer les accès qui semblent anormaux.* »

Les enjeux

D'un point de vue éthique, les enjeux sont tout aussi importants. Le respect de la sécurité (et notamment de la confidentialité des données de santé) doit être au centre des préoccupations des professionnels de santé, en vue notamment de garder un haut niveau de confiance entre eux et leurs patients.

D'un point de vue juridique, les enjeux sont énormes. En application du RGPD, la sanction encourue, en cas de manquement à l'obligation de sécurité, est de 2% du chiffre d'affaires annuel mondial. D'ailleurs, dans une affaire récente, l'autorité espagnole de protection des données n'a pas hésité à sanctionner un hôpital qui n'avait pas mis en place les mesures permettant de limiter l'accès au dossier clinique aux seuls professionnels de santé ayant besoin d'en connaître (AEPD, décision n°PS/00587/2021).

En France, à la suite des contrôles réalisés depuis 2020, plusieurs établissements de santé ont fait l'objet de mise en demeure de prendre des mesures adaptées. La CNIL prévoit, pour 2024, des mesures correctrices contre d'autres établissements disposant de DPI.

A suivre…

Source : ici

ENTREPOTS DE DONNEES DE SANTE ET CLOUD NON-SOUVERAIN SONT-ILS COMPATIBLES ?

Le Health Data Hub a récemment été autorisé à recourir à l'hébergeur Microsoft pour un entrepôt de données de santé portant le nom « EMC2 ». Est-ce que cela signifie qu'il est désormais possible d'héberger des entrepôts de données de santé sur des cloud non-souverains ? Les enjeux associés à cette problématique sont considérables. Aussi, les débats associés à une telle autorisation ne cessent de proliférer.

Le cas de l'entrepôt de données de santé « EMC2 » du Health Data Hub

Le Health Data Hub, « *chargé par la loi de recueillir les bases de données de santé les plus importants du pays,* » a conclu un contrat de services avec l'Agence européenne des médicaments (EMA). C'est dans ce cadre qu'intervient *« le projet EMC2* » afin, en particulier, d'observer et évaluer la prise en charge des patients, d'évaluer l'utilisation et/ou les pratiques, l'efficacité et la sécurité en vie réelle des produits de santé, en particulier les médicaments et les dispositifs médicaux inscrits au remboursement ou en accès précoce.

Aussi, ce projet porte sur la création d'un entrepôt de données de santé pour des analyses pharmatico-épidémiologiques. « *Un appariement entre les données de la base principale du système national des données de santé (SNDS) et les dossiers médicaux fournis par les établissements de santé partenaires* » y est prévu.

Le Health Data Hub a saisi la CNIL d'une demande d'autorisation pour mettre en œuvre cet entrepôt de données de santé.

A noter, effectivement, qu'un entrepôt 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* », tel que le projet « EMC2 », doit être conforme au référentiel CNIL 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* » , pour pouvoir être mis en œuvre par l'organisme, responsable de traitement, concerné.

En cas de conformité, une déclaration de conformité auprès de la CNIL suffit. A défaut, une autorisation spécifique préalable de la CNIL doit être obtenue. En l'occurrence, le projet « EMC2 » ne répondait pas à toutes les exigences prévues dans ledit référentiel et nécessitait donc une autorisation.

La possibilité d'hébergement temporaire sur un cloud non-souverain, faute de mieux

Le projet « EMC2 » prévoyait de recourir à l'hébergeur Microsoft Ireland Ltd (avec la solution Microsoft Azure), dont la maison mère est située au Etats-Unis. La question des ingérences extraterritoriales se pose.

Certes, la Commission européenne a reconnu que le cadre de transfert des données « Etats-Unis/UE » assure un niveau de protection adéquat (décision d'adéquation du 10 juillet 2023). Pour autant, selon la CNIL, le risque d'accès aux données hébergées chez Microsoft par les autorités américaines demeure.

Ainsi, « *pour les bases de données les plus sensibles* » telles que les bases de données de santé, la CNIL recommande de recourir à un hébergeur exclusivement soumis droit européen et certifié « SecNumCloud » . Les entrepôts de données de santé appariées avec le SNDS font d'autant plus l'objet d'une vigilance particulière, *« malgré le fait que le ces données soient pseudonymisées* », dans la mesure où *« la CNIL a toujours demandé aux porteurs de projet, publics et privés, de s'assurer que l'hébergeur des données n'est pas soumis à une législation extra-européenne* ».

La circulaire de la Première Ministre du 31 mars 2023 demande effectivement, rappelle la CNIL, que les autorités publiques s'assurent que « *les données d'une sensibilité particulière hébergées dans le cloud ne soient pas soumises à des lois extra-européennes* ». Ainsi, le choix du Health Data Hub *« apparaît en très nette contradiction avec [ces] éléments* ».

On aurait alors pu s'attendre à un refus de la CNIL d'autoriser l'entrepôt de données de santé « EMC2 », hébergé chez Microsoft.

Mais, après avoir notamment *« déplor[é] qu'aucun prestataire susceptible de répondre actuellement aux besoins exprimés par le [Health Data Hub] ne protège les données contre l'application de lois extraterritoriales de pays tiers* » la CNIL a décidé d'autoriser la mise en œuvre de l'entrepôt de données de santé *« EMC2* » avec un hébergement chez Microsoft pour une durée de 3 ans. Il faut savoir que, pour répondre aux demandes de la CNIL, une expertise, pilotée par la délégation numérique en santé (DNS), la direction interministérielle du numérique (DINUM) et l'Agence Numérique en santé, avait été réalisée *« aux fins de déterminer si le projet EMC2 pouvait, sans compromettre le projet vis-à-vis des conditions fixées par [l'Agence européenne du médicament], être mis en œuvre via un prestataire soumis uniquement aux lois de l'Union européenne* ».

Le rapport d'expertise, établi dans des délais relativement courts, avait répondu par la négative.

Un sujet au cœur des débats et une position du Conseil d'Etat à venir

Cette position de la CNIL donne lieu à d'importants débats.

En particulier, cette décision interroge compte tenu :

- d'un côté, de la récente décision de la Commission européenne considérant que le niveau de protection de données personnelles du cadre de transfert de données UE/Etats-Unis est équivalent à celui de l'Union européenne et

- de l'autre côté, des exigences nationales en termes de souveraineté.

Des critiques se sont également élevées contre la CNIL dans la mesure où elle reconnaît le non-respect du projet « EMC2 » aux exigences nationales de souveraineté tout en validant ce projet, tandis que d'autres projets similaires hébergés par Microsoft auraient déjà été refusés par la CNIL.

La position du Conseil d'Etat, saisi dans le cadre d'un recours en annulation initié par l'Internet Society France, est ainsi particulièrement attendue. A suivre…

Source : ici

IA ET SANTE : VERS UNE REFORME DE LA LOI « INFORMATIQUE ET LIBERTES » POUR FACILITER L'INNOVATION ET LA RECHERCHE

La Commission de l'IA (Intelligence artificielle) préconise la suppression des procédures d'autorisation préalable d'accès aux données de santé et la réduction des délais de réponse de la CNIL. Retour sur ce rapport tant attendu, qui a été présenté mercredi dernier au Président Emmanuel Macron.

Le rapport de la Commission de l'intelligence artificielle, en quelques mots

En septembre dernier, le Gouvernement a installé la Commission de l'intelligence artificielle pour « contribuer à faire de la France un pays à la pointe de la révolution de l'IA ». La Commission a remis, mercredi 13 mars 2024, son rapport au Président Emmanuel Macron. Ce rapport contient 25 recommandations pour que la France puisse tirer partie de la révolution technologique de l'IA. La recherche dans le secteur de la santé est au cœur des réflexions. La question de la protection des données personnelles l'est également.

En synthèse, il ressort du rapport que :

- L'IA est une révolution technologique incontournable ;
- Cette révolution technologique affecte tous les domaines d'activité ;
- L'IA ne doit susciter ni excès de pessimisme, ni excès d'optimisme (« Nous n'anticipons ni chômage de masse, ni accélération automatique de la croissance ») ;
- L'Europe et la France ont des atouts pour être des acteurs de cette révolution ;
- L'Europe et la France doivent relever le défi de l'IA, « *faute de quoi nous n'aurons pas la maîtrise de notre avenir* »

Afin de gagner le défi de l'IA, la Commission propose six grandes lignes d'actions :

- Lancer immédiatement un plan de sensibilisation et de formation de la nation ;
- Réorienter structurellement l'épargne vers l'innovation et créer, à court terme, un fonds « France & IA » de 10 Md euros ;
- Faire de la France un pôle majeur de la puissance de calcul ;
- Faciliter l'accès aux données ;
- Assumer le principe d'une « exception IA » dans la recherche publique ; et
- Promouvoir une gouvernance mondiale de l'IA.

L'accès aux données, le défi de l'IA

Premier constat : l'IA permet d'appréhender un volume considérable de données disponibles, que l'intelligence humaine ne peut pas traiter. « Plus de 5 millions d'articles scientifiques sont publiés chaque année, dont la moitié dans le seul domaine de la recherche médicale, indique la Commission. Il est évidemment impossible qu'un chercheur ou une équipe de chercheurs, même de haute volée, puisse les lire, et encore moins les évaluer et les analyser.

Deuxième constat : les données constituent un ingrédient indispensable aux développements récents de l'intelligence artificielle. Et si ces données ne sont pas nécessairement personnelles, force est de constater que nombre d'entre elles ont un caractère personnel.

« *Exploiter le potentiel de l'intelligence artificielle et permettre son déploiement au service de l'humain exige par conséquent que les chercheurs, les développeurs et les innovateurs disposent d'un accès à des données massives, fiables, aisément manipulables et dont la représentativité et la qualité peuvent être évaluées,* souligne la Commission*. Dans un contexte d'évolution technologique rapide et de concurrence accrue, cet accès doit en outre pouvoir leur être ouvert rapidement et les données être utilisées sans contraintes excessives, au risque de favoriser davantage encore les acteurs en place ou de voir d'autres s'approprier nos recherches et nos innovations, en nous devançant dans leur expérimentation et leur diffusion*. »

Troisième constat : l'accès aux données est souvent compliqué et les contraintes sont considérées comme excessives par les acteurs de l'IA, quels qu'ils soient (entreprises, chercheurs, laboratoires, institutions publiques et privées, associations).

Les contraintes règlementaires

Les contraintes sont de deux ordres.

Tout d'abord, la Commission considère que certaines règles et pratiques françaises sont plus contraignantes que le cadre européen en matière de traitement de données personnelles. Si le RGPD a, avec les principes de liberté et de responsabilité, renversé complètement la logique du droit qui prévalait en France depuis la loi « Informatique et Libertés » du 6 janvier 1978 (en application de laquelle les traitements des données à caractère personnel reposaient sur des procédures d'autorisation ou de déclaration préalables auprès de la CNIL), les contraintes sont encore trop fortes dans le secteur de la santé. « Il demeure des procédures d'autorisation préalables non prévues par le droit européen, regrette la Commission.

C'est en particulier le cas pour l'accès aux données de santé pour la recherche. Une procédure simplifiée de déclaration de conformité à des méthodologies de référence existe mais elle est loin d'être généralisée. En pratique, la procédure simplifiée reste l'exception par rapport à la procédure d'autorisation préalable car le moindre écart par rapport à ces méthodologies implique d'en passer par une autorisation préalable qui peut impliquer jusqu'à trois niveaux d'autorisation préalable. »

Ensuite, la Commission estime qu'il existe « *un décalage croissant entre la logique centrée sur la protection de l'individu et l'évolution des modes d'utilisation collective des données* ». Selon la Commission, plusieurs notions clés du RGPD sont peu adaptées face au fonctionnement de l'IA : la notion de « responsable du traitement », « pour laquelle la répartition des responsabilités entre le développeur qui a procédé à l'entraînement d'une IA générative et qui la met à disposition de tiers et l'utilisateur final du système pour ses propres besoins n'apparaît pas forcément aller de soi » ; la notion de « finalité du traitement », « qui conditionne la nature des données pouvant légalement être utilisées et sur laquelle porte le consentement des personnes concernées est également plus complexe à appréhender, eu égard aux nombreuses utilisations possibles d'une IA générative une fois celle-ci entraînée » ; la notion même de « donnée personnelle », « *qui constitue la clé d'application du RGPD, suscite des interrogations dans un contexte croissant d'utilisation de données collectives* ».

Même l'anonymisation des données personnelles qui permet de « sortir » du régime de protection des données personnelles du RGPD, ne semble pas adaptée car « *la technologie ouvre de plus en plus loin des possibilités de réidentification de données anonymisées* ».

Quelles solutions ?

La Commission recommande « de supprimer des procédures d'autorisation préalable d'accès aux données de santé et de réduire les délais de réponse de la CNIL ». Elle ajoute que cette évolution devrait s'accompagner d'une réforme du mandat confié à la CNIL, pour y intégrer un « *objectif d'innovation* ». Elle termine en suggérant l'idée d'une « gouvernance collective » de la donnée qui pourrait poser « *les jalons d'une évolution du cadre juridique qui prendrait mieux en considération l'évolution des modes d'utilisation des données*. »

Affaire à suivre…

Source : ici

DOCTRINE

RGPD

Le consentement : une base légale parfois inadaptée

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 la question du consentement donné par des patients en vue de la publication par un hôpital d'informations les concernant sur un compte Instagram.

Un traitement doit reposer sur une des six bases légales visées à l'article 6.1 du RGPD. À défaut, le traitement est considéré comme illicite. Les six bases légales sont : (i) le consentement (la personne concernée a consenti au traitement de ses données) ; (ii) le contrat (le traitement est nécessaire à l'exécution ou à la préparation d'un contrat avec la personne concernée) ; (iii) l'obligation légale (le traitement est imposé par un texte légal) ; (iv) la mission d'intérêt public (le traitement est nécessaire à l'exécution d'une mission d'intérêt public) ; (v) l'intérêt légitime (le traitement est nécessaire à la poursuite d'intérêts légitimes de l'organisme qui traite les données) ; (vi) la sauvegarde des intérêts vitaux (le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée, ou d'un tiers).

La Cnil rappelle régulièrement que le RGPD « *ne crée pas de hiérarchie entre les différentes bases légales* »[1] et explique, à cet égard, que le consentement ne prévaut pas sur les autres bases légales : « *La base légale appropriée doit être déterminée par le responsable du traitement de manière adaptée à la situation et au type de traitement, au cas par cas* »[2].

Par ailleurs, si le traitement porte sur des catégories particulières de données à caractère personnel (données dites « *sensibles* » visées à l'article 9.1 du RGPD, telles que les données de santé, les données concernant la vie sexuelle, l'origine raciale, etc.), il appartient à l'organisme de se prévaloir d'une des exceptions visées à l'article 9.2 et ce, pour déroger au principe d'interdiction du traitement de ces données. Parmi ces exceptions figure le consentement de la personne concernée.

En d'autres termes, un traitement portant sur des données sensibles ne peut intervenir que si les deux conditions cumulatives suivantes sont réunies : d'une part, le traitement repose sur une des bases légales prévues à l'article 6 du RGPD et, d'autre part, une des exceptions mentionnées à l'article 9.2 du RGPD est applicable au traitement concerné. Dans ces situations, le consentement peut être utilisé pour répondre aux deux conditions susvisées.

L'affaire[3]

Une personne a déposé une plainte auprès de l'autorité danoise de protection des données, après avoir constaté qu'une photo la représentant avait été publiée sur le compte Instagram de l'hôpital où elle était prise en charge. Au cours de son enquête, l'autorité a constaté que l'hôpital en question publiait régulièrement, sur ce compte, des photos et vidéos de la vie quotidienne du centre, accompagnées parfois des noms et des informations relatives à la santé des patients (dont des enfants), susceptibles d'être directement identifiés. Le compte, actif depuis 2015, disposait de plus de 15 000 abonnés et avait partagé plus de 1 400 messages. Selon le centre hospitalier, ces publications, qui avaient pour but d'informer le monde extérieur sur ses activités, étaient parfaitement licites en ce qu'elles reposaient sur le consentement des patients en application des articles 6.1 a)

et 9.2 a) du RGPD : « *Le consentement est obtenu par écrit avant la publication du message, et l'octroi du consentement n'affecte pas le traitement médical proposé au patient. La sélection des patients tient compte de leur santé physique et de leur force, et le patient dispose d'un temps de réflexion avant de signer le formulaire de consentement. Le patient a également la possibilité d'approuver le contenu de la publicité.* »

Rappelant les termes de l'article 4.11 du RGPD concernant la définition du « *consentement*[4] » et les lignes directrices du CEPD sur ce sujet[5], l'autorité danoise de protection des données a souligné que « *le consentement ne peut généralement pas être considéré comme donné librement si la personne concernée ne dispose pas d'un véritable libre choix. Toute pression ou influence inappropriée sur le libre arbitre de la personne concernée rend le consentement invalide.* » À cet égard, l'autorité cite les dispositions du considérant 43 du RGPD, selon lesquelles : « *Pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière.* »
Selon l'autorité danoise de protection des données, il convient donc, pour apprécier la validité du consentement, de vérifier si le responsable du traitement et la personne concernée peuvent être considérés comme égaux dans la situation en cause et si la personne concernée a l'impression de disposer d'un véritable choix.

Tel n'est pas le cas lorsque la personne concernée se trouve dans une « *situation vulnérable* » comme pourrait l'être un patient lorsqu'il est hospitalisé ou lorsqu'il suit un traitement : « *Une telle vulnérabilité crée une inégalité entre le patient et l'hôpital et le personnel hospitalier, ce qui peut entraîner le risque que le patient subisse des pressions lorsqu'on lui demande son consentement.* ». Par ailleurs, elle ajoute que « *le fait que l'hôpital soit une autorité publique offrant un service de soins de santé dont la personne concernée a besoin peut affecter le sentiment du patient d'avoir un véritable libre choix ou constituer une pression pour le patient.* »

L'autorité danoise a estimé qu'en l'espèce l'objectif d'informer le monde extérieur sur les activités de l'hôpital aurait pu être atteint d'une manière moins intrusive pour les droits fondamentaux des personnes et que la publication des données personnelles des patients sur le compte Instagram n'était pas conforme au RGPD, compte tenu de ce qui précède au regard des exigences relatives à un consentement valide. L'autorité a donc fait injonction au centre hospitalier de supprimer le compte litigieux.

Quelles recommandations ?

La détermination de la base légale d'un traitement n'est pas toujours un exercice facile. La Cnil recommande de se poser les questions suivantes pour guider la réflexion[6] : (i) est-ce que les textes imposent ou excluent une base légale spécifique ? (Exemple : le RGPD interdit de fonder les traitements qu'une autorité publique met en œuvre dans l'exécution de ses missions sur son « *intérêt légitime* ») ; (ii) quel est le contexte général de mise en œuvre du traitement ? (Exemple : si le traitement est mis en œuvre dans le contexte d'un contrat entre l'organisme et une personne, la base légale sera « *l'exécution du contrat* ») ; (iii) est-ce que les conditions propres à la base légale sont bien remplies ? (Exemple : le « *consentement* » doit être libre, spécifique, éclairé et univoque pour être valablement recueilli et constituer dès lors la base légale du traitement).

Dans l'affaire en cause, aucune base légale ne semblait justifier la publication des photos de patients sur le compte Instagram de l'hôpital...

Alexandre FIEVEE
Avocat associé
Derriennic Associes

Notes

(1) https://www.cnil.fr/fr/les-bases-legales/liceite-essentiel-sur-les-bases-legales

(2) https://www.cnil.fr/fr/les-bases-legales/liceite-essentiel-sur-les-bases-legales

(3) Autorité danoise de protection des données, 27 novembre 2023.

(4) RGPD ; article 4.11 : « "consentement" de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

(5) CEPD, Lignes directrices5/2020 sur le consentement au sens du règlement (UE)2016/679 ;

(6) https://www.cnil.fr/fr/les-bases-legales/liceite-essentiel-sur-les-bases-legales

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

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 :
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