NEWSLETTER

E-Santé

NUMÉRO 12 • 2024

Alexandre FIEVÉE, Avocat Associé

Alice ROBERT, Avocat Counsel

SOMMAIRE

ACTUALITÉ

- Plateforme de prise de rendez-vous médicaux : l'éditeur, sous-traitant, n'a pas à répondre à une demande de droit d'accès. **p. 2**

VU DANS LA PRESSE

- Données de santé : la stratégie interministérielle pour le développement des bases de données et l'usage secondaire des données. **p.3**
- Deux pharmaciens s'écharpent dans un litige « RGPD ». **p.4**
- L'achat en ligne de médicaments nécessite-t-il le consentement des clients au traitement de leurs données de santé ? **p.6**
- IA générative et sécurité : retour sur les recommandations de l'ANSSI. **p.8**
- Le secret médical renforcé par la Cour de cassation à l'occasion d'affaires sur les maladies professionnelles. **p.10**
- Hébergement des données de santé et certification : un nouveau référentiel applicable dès novembre 2024 ! **p.12**
- La réponse d'un professionnel à un avis en ligne n'échappe pas au RGPD. **p.15**

PLATEFORME DE PRISE DE RENDEZ-VOUS MEDICAUX : L'EDITEUR, SOUS-TRAITANT, N'A PAS A REPONDRE A UNE DEMANDE DE DROIT D'ACCES

L'autorité de contrôle belge a considéré que l'éditeur d'une plateforme permettant de prendre des rendez-vous médicaux est un sous-traitant et donc qu'il n'a pas à répondre à une demande de droit d'accès.

Un patient a exercé son droit d'accès auprès de l'éditeur d'une solution logicielle permettant de prendre des rendez-vous, en ligne, auprès de professionnels de santé.

L'éditeur de la solution, indiquant être un sous-traitant, a refusé de faire droit à la demande mais a fourni, après une recherche dans sa base de données, la liste des responsables du traitement, professionnels de santé, à contacter.

Le patient, considérant ce refus comme contraire au RGPD, a déposé une plainte.

L'autorité de contrôle, rappelant que le droit d'accès s'exerce auprès du responsable du traitement, a considéré que l'éditeur de la solution était un sous-traitant :

- D'une part, car la finalité de l'application, à savoir *« permettre la prise de rendez-vous automatisée », est déterminée par le professionnel de santé, la solution logicielle n'étant qu'« un moyen d'atteindre cette finalité »* :
- D'autre part, car le professionnel de santé décide seul du moyen qui est le plus approprié pour atteinte la finalité recherchée, et donc que l'éditeur de la solution n'a qu'un rôle d'intermédiaire, en ce sens qu'il ne fait qu'offrir une application proposant une fonctionnalité de prise de rendez-vous ;
- Enfin, car l'éditeur du logiciel traite les données pour le compte du prestataire de santé, l'éditeur ne disposant en l'espèce d'aucune marge de manœuvre pour traiter les données à caractère personnelles à d'autres fins que celles définies par le professionnel de santé.

En conséquence, l'autorité de contrôle a considéré que l'éditeur de logiciel n'avait effectivement pas à répondre à la demande de droit d'accès de la personne concernée.

Rappelant, enfin, que le sous-traitant est tenu de traiter les données conformément aux instructions du responsable du traitement, l'autorité de contrôle n'a pas reproché à l'éditeur du logiciel d'avoir recherché la présence de la personne concernée dans les bases de données de ses clients, responsables du traitement, mais a, au contraire, considéré qu'*« il s'agit là d'une bonne pratique qui facilite l'exercice des droits de la personne concernée ».*

Compte tenu de tout ce qui précède, l'autorité de contrôle a rejeté la plainte de la personne concernée.

Source : ici

VU DANS LA PRESSE

« DSIH », OCTOBRE 2024

DONNEES DE SANTE : LA STRATEGIE INTERMINISTERIELLE POUR LE DEVELOPPEMENT DES BASES DE DONNEES ET L'USAGE SECONDAIRE DES DONNEES

Partant du constat que les bases de données de santé font partie de notre patrimoine immatériel et national, qu'elles sont créées pour le fonctionnement de notre système de santé ainsi que pour les études et recherches de santé et qu'elles sont une source de connaissances d'une richesse incroyable qu'il faut organiser, faire croître, protéger et partager, une stratégie interministérielle a été définie en vue de coconstruire « une trajectoire commune, cohérente et ambitieuse pour développer les bases de données et l'usage secondaire des données de santé ».

Cette stratégie, mise en consultation publique le 30 septembre dernier, a également pour objectif d'accompagner les acteurs dans la préparation de l'entrée en vigueur du règlement européen sur l'espace européen des données de santé (EEDS), dont les dispositions sur l'usage secondaire des données entreront en application en 2028.

Plusieurs axes ont été retenus :

- Favoriser la transparence et la confiance des citoyens à travers notamment la mise en place d'une gouvernance nationale lisible représentative, la simplification de l'exercice des droits et l'amélioration de l'information des citoyens et, enfin, la construction d'un cadre sécurisé et de confiance pour la réutilisation des données de santé ;
- Constituer des bases de données d'intérêt réutilisables en particulier par l'enrichissement du patrimoine de bases de données (notamment en anticipant les besoins et en poursuivant les travaux de collecte et de préparation des données), l'anticipation du principe de mise à disposition des données dès la conception (interopérabilité) et la formation de l'écosystème à la réutilisation des données en vue d'une montée en compétence de l'ensemble des acteurs ;
- Réunir les conditions nécessaires au partage et à la réutilisation des données de santé, ce qui pourrait passer par le recensement des bases de données existantes et la construction d'un modèle équilibré de partage des données en favorisant l'émergence d'un cadre et de modalités économiques et financières autour de la donnée ;
- Faciliter et simplifier l'utilisation des données, en encourageant les procédures de mise à disposition des données et en facilitant cette mise à disposition en application de principes harmonisés et en optimisant la mise à disposition des données de la base principale du SNDS.

Les résultats de cette consultation seront présentés le 3 décembre prochain, ainsi que les modalités de mise en œuvre et de suivi.

A suivre…

Source : ici

VU DANS LA PRESSE

« DSIH », OCTOBRE 2024

DEUX PHARMACIENS S'ECHARPENT DANS UN LITIGE « RGPD »

La conformité au RGPD requiert des investissements économiques et humains non négligeables. Aussi, quand un professionnel s'affranchit du respect de cette règlementation, il peut en retirer un avantage, par exemple, en proposant des prix plus bas ou des offres plus attractives. Un concurrent pourrait-il se prévaloir d'un manquement au RGPD de ce professionnel pour faire cesser cette pratique et/ou obtenir des dommages et intérêts ? La Cour de Justice de l'Union Européenne (CJUE) a été récemment saisie de cette problématique et a tranché positivement.[1]

L'affaire opposait deux pharmaciens allemands. Le premier reprochait au second la commercialisation, au mépris des règles du RGPD, sur une place de marché en ligne (Amazon) de médicaments non soumis à prescription médicale. Le non-respect du RGPD résidait, selon le premier pharmacien, dans le fait que le second n'obtenait pas le consentement préalable des clients, personnes concernées, pour le traitement de leurs données de santé.

Le premier a alors formé un recours en justice contre le second afin qu'il soit mis fin à une telle pratique considérée comme déloyale.

A cette occasion, la juridiction allemande saisie du litige a interrogé la CJUE sur le point de savoir si ce type d'action en justice était permise par le RGPD.

La CJUE a jugé qu'aucune disposition du RGPD *« n'exclut expressément la possibilité pour le concurrent d'une entreprise d'introduire un recours devant les juridictions civiles contre cette entreprise sur le fondement de l'interdiction des pratiques commerciales déloyales, en raison de la violation alléguée par cette entreprise d'obligations prévues par ce règlement ».* Cette possibilité *« s'ajoute aux voies de recours »* prévues par le RGPD.

La CJUE souligne, en particulier, que cette possibilité de recours *« est de nature à renforcer l'effet utile [du RPGD] et ainsi le niveau élevé de protection des personnes concernées à l'égard du traitement de leurs données personnelles ».*

Il appartiendra alors à la juridiction nationale allemande de vérifier si la violation présumée du RGPD *« pour autant qu'elle soit établie, est également constitutive d'une violation des pratiques commerciales déloyales telle que prévue par la règlementation nationale pertinente »*.

Que peut-on en retenir ?

Le non-respect du RGPD peut être sanctionné sur le terrain des pratiques commerciales déloyales interdites telles que prévues par une loi locale de l'UE.

En France, les juges ont déjà considéré que le non-respect du RGPD peut constituer un acte de concurrence déloyale.

De façon générale, la Cour de cassation a jugé que *« constitue un acte de concurrence déloyale le non-respect d'une réglementation d'une activité commerciale, qui induit nécessairement un avantage concurrentiel indu pour son auteur*[2]*».*

Aussi, tant le Tribunal Judiciaire de Paris[3] que la Cour d'appel de Paris[4] ont admis l'action en concurrence déloyale du fait d'une violation du RGPD, violation permettant nécessairement *« de bénéficier d'un avantage commercial indu ».*

Cette nouvelle décision de la CJUE ajoute une pierre à l'édifice des recours possibles, dans l'Union européenne, contre un concurrent qui ne respecte pas le RGPD.

Un conseil : ne négligez pas votre conformité au RGPD et vérifiez si vos principaux concurrents sont de « bons élèves » afin d'envisager, le cas échéant, un recours contre eux…

[1]CJUE, 4 octobre 2024, Affaire C-21/23.

[2]Cass. Com., 17 mars 2021, n°19/10414.

[3]TJ Paris, 15 avril 2022, n°19/12628.

[4]CA de Paris, 9 novembre 2022, n°21/00180.

VU DANS LA PRESSE

« DSIH », OCTOBRE 2024

L'ACHAT EN LIGNE DE MEDICAMENTS NECESSITE-T-IL LE CONSENTEMENT DES CLIENTS AU TRAITEMENT DE LEURS DONNEES DE SANTE ?

Nous savons que la notion de donnée de santé doit être interprétée très largement. Toutefois, dans certaines circonstances, la question se pose de savoir si on est en présence ou non de données concernant la santé. Cette question a été posée à la Cour de Justice de l'Union Européenne (CJUE), qui a dû se prononcer sur le fait de savoir si, lors d'une commande en ligne de médicaments, les éléments nécessaires à leur individualisation doivent s'analyser comme des données de santé.

L'affaire opposait deux pharmaciens allemands. Le premier reprochait au second la commercialisation sur une place de marché en ligne (Amazon), au mépris des règles du RGPD, de médicaments non soumis à prescription médicale. Le non-respect du RGPD résidait, selon le premier pharmacien, dans le fait que le second n'obtenait pas le consentement préalable des clients, personnes concernées, pour le traitement de leurs données de santé (article 9 du RGPD).

Le premier a alors formé un recours en justice contre le second afin qu'il soit mis fin à une telle pratique considérée comme déloyale.

A cette occasion, la juridiction allemande saisie du litige a interrogé la CJUE sur le point notamment de savoir si l'article 9 du RGPD doit être interprété en ce sens que les informations que les clients saisissent lors de la commande en ligne de médicaments - nom, adresse de livraison, éléments nécessaires à l'individualisation des médicaments – constituent des données concernant la santé.

La CJUE a d'abord indiqué que *« lorsque les données sur les achats des médicaments permettent de tirer des conclusions sur l'état d'une personne identifiée ou identifiable »*, elles doivent être considérées comme étant *« des données concernant la santé ». Il suffit ainsi, a ajouté la Cour, que ces données « soient de nature à révéler, par une opération intellectuelle de rapprochement ou de déduction, des informations sur l'état de santé de la personne concernée ».*

A cet égard, la juridiction européenne a estimé qu'il importe peu que les médicaments puissent être destinés non pas au client qui réalise la commande mais à des personnes tierces. La CJUE en a conclu que *« les informations que les clients d'un exploitant d'une pharmacie saisissent lors de la commande en ligne de médicaments dont la vente est réservée aux pharmacies sans être soumise à prescription médicale constituent des données concernant la santé (…), même si c'est seulement avec une certaine probabilité, et non avec une certitude absolue, que ces médicaments sont destinés à ces clients ».*

La Cour a précisé enfin que le fait que de telles informations constituent des données de santé ne fait pas obstacle à leur traitement par l'exploitant de la pharmacie, mais à condition que l'une des conditions de l'article 9-2 du RGPD soit respectée, en l'occurrence soit que le client a donné son consentement (article 9-2 a)), soit que le traitement est nécessaire aux fins de la prise en charge sanitaire (article 9-2 h)).

C’est à la juridiction allemande qu’il reviendra de répondre à la question de la licéité de ce traitement, qui, en l’espèce, ne repose pas sur le consentement. Affaire à suivre…

Source : ici

VU DANS LA PRESSE

« DSIH », JUILLET 2024

IA GENERATIVE ET SECURITE : RETOUR SUR LES RECOMMANDATIONS DE L'ANSSI

Innover et optimiser dans le secteur de la santé, grâce à l'IA générative : oui, mais avec sécurité ! L'ANSSI a récemment émis des recommandations visant à « sensibiliser les administrations et les entreprises aux risques liés à l'IA générative, ainsi qu'à promouvoir les bonnes pratiques à mettre en œuvre ». Professionnels de santé, établissements de santé, établissements médico-sociaux, industriels, vous êtes tous concernés !

L'IA générative, à savoir *« un sous-ensemble de l'intelligence artificielle, axé sur la création de modèles qui sont entraînés à générer du contenu (texte, images, vidéos, etc.) à partir d'un corpus spécifique de données d'entraînement »,* présente des enjeux indéniables en santé, notamment dans l'accompagnement de l'activité des professionnels de santé ou encore l'optimisation de la recherche.

La mise en œuvre d'un tel outil n'est toutefois pas sans soulever des problématiques de différentes natures : vie privée et protection des données personnelles, propriété intellectuelle, secret des affaires, éthique, sécurité, etc.

L'ANSSI s'est récemment penchée sur l'aspect sécurité de l'IA générative et a formulé une trentaine de recommandations.

Sans se livrer à une analyse exhaustive de ces recommandations, un échantillonnage met en lumière l'importance d'agir avec prudence, en ayant une vision à la fois transversale et adaptée à chaque situation.

- **Mise en œuvre d'une IA générative : des mesures de sécurité spécifiques à intégrer par phase**

Mettre en œuvre une IA générative, implique, selon l'ANSSI, trois phases cycliques : entrainement, intégration et déploiement, production.

Au-delà de la nécessité de mener une analyse de risques particulière en amont de la première phase, compte tenu notamment de la spécificité des attaques en matière d'IA générative, il est fondamental de travailler sur des mesures de sécurité spécifiques à chacune de ces trois phases. En effet, l'ANSSI souligne que chaque phase peut concerner des environnements et des utilisateurs particuliers.

Pour évaluer les mesures de sécurité à mettre en place, l'ANSSI recommande aussi de tenir compte :

- Des interactions entre les différents systèmes : intégrations internes et externes de l'IA générative avec un SI existant ;
- Des différentes parties prenantes à l'IA générative, selon l'organisation du partage de responsabilité retenue (sans oublier la sous-traitance associée).

- **Conception d'une IA générative : des réflexes de prudence à adopter**

Parmi les recommandations données par l'ANSSI, on peut relever la nécessité de réaliser une évaluation du niveau de confiance des sources de données externes utilisées dans l'IA générative ou encore de recourir à des modèles d'IA sécurisés, à l'état de l'art.

L'ANSSI recommande également de tenir compte des enjeux de la confidentialité, en particulier, face à la complexité de l'accès à une IA générative sur l'application *« du besoin d'en connaître »* des utilisateurs. Par exemple, des données sensibles (i) peuvent figurer dans des requêtes d'utilisateur et les réponses associées et (ii) alors faire l'objet d'un stockage temporaire au stade du traitement, et potentiellement d'une utilisation afin de réentrainement du modèle. Ce faisant *« la question du besoin d'en connaître doit ainsi se reposer à chaque réentraînement du modèle, y compris sur des données issues de l'usage du modèle en production »*.

L'ANSSI insiste sur le fait que l'IA générative *« ne doit pas pouvoir prendre des décisions critiques ayant un impact fort sur le métier ou la protection des biens et des personnes, sans un contrôle humain ». « L'usage automatisé de systèmes d'IA pour des actions critiques sur le SI »* doit ainsi être proscrit conduisant à une définition et une configuration strictes des rôles et droits des administrateurs. Par ailleurs, il convient de prévoir *« un mode dégradé des services métier sans système d'IA ».* Il s'agit de mettre en place *« au minimum une procédure de contournement du système d'IA pour les utilisateurs »* et ce, *« afin de prévenir des dysfonctionnements ou des incohérences dans les réponses apportées par le modèle d'IA ».*

- **Utilisation d'IA génératives tierces : *« des points de vigilance à prendre compte »***

L'ANSSI revient sur l'importance de ne pas transmettre de données sensibles aux *« services d'IA générative tiers grand public »* (exemples : ChatGPT, Gemini, Copilot, DeepL, etc.). L'utilisation d'outils d'IA générative sur Internet à des fins professionnelles et impliquant des données sensibles (y compris pour *« générer des jeux de données synthétiques pour l'entrainement et le fine-tuning d'un modèle d'IA »*) est ainsi à bannir.

En outre, l'ANSSI recommande de revoir régulièrement (i) la configuration des droits d'accès des IA génératives tierces sur les données/applications métiers avec lesquelles elle peut établir, par défaut, une connexion pouvant être très large, mais (ii) également les mises à jour tant fonctionnelles que sécuritaires de l'outil et ses incidences éventuelles sur les besoins d'en connaître des utilisateurs.

Chaque acteur concerné en santé est donc invité à suivre ces *« bonnes pratiques » de sécurité, lesquelles viennent ainsi s'ajouter aux « référentiels de conformité »* à respecter dans la mise en œuvre ou l'utilisation d'une IA générative (parmi lesquels l'IA Act, le RGPD ; les recommandations de la CNIL, etc.).

Source : ici

VU DANS LA PRESSE

« LA VEILLE ACTEURS DE SANTÉ », OCTOBRE 2024

LE SECRET MEDICAL RENFORCE PAR LA COUR DE CASSATION A L'OCCASION D'AFFAIRES SUR LES MALADIES PROFESSIONNELLES

L'employeur est-il légitime à accéder à tous les documents ou données de santé du salarié ayant conduit à la reconnaissance de la maladie professionnelle ? Jusqu'où le secret médical peut-il être levé en cas de contestation par l'employeur d'une maladie professionnelle ? Quatre affaires récentes permettent à Alexandre Fievée, avocat associé, et à Alice Robert, avocat counsel du cabinet Derriennic Associés de faire un point précis sur l'état du droit en France aujourd'hui pour les lecteurs de La Veille Acteurs de Santé.

A l'occasion de quatre affaires similaires concernant un même employeur[1], la Cour de cassation a été saisie de cette problématique et a tranché en faveur de la protection du secret médical.

Les éléments de l'affaire

Comme dans tout contentieux portant sur la contestation par l'employeur de la reconnaissance d'une maladie professionnelle, ces affaires opposaient un employeur à la caisse primaire d'assurance maladie (la *« caisse »*).

Dans ces affaires, la caisse a reconnu la qualification de *« maladie professionnelle »* car la maladie, objet du litige, figurait dans le tableau n°42 des maladies professionnelles intitulé *« atteinte auditive provoquée par les bruits lésionnels »*[2].

Pour parvenir à une telle conclusion, la caisse avait préalablement procédé à une enquête et constitué un dossier, conformément à la procédure de reconnaissance de maladie professionnelle[3].

Pour mémoire, ce dossier comprend la déclaration de maladie professionnelle et les divers certificats médicaux détenus par la caisse, les constats faits par la caisse, les informations échangées par le salarié et par l'employeur, ainsi que les éléments communiqués par la caisse régionale[4]. Ce dossier peut être consulté par l'employeur à l'issue l'instruction[5].

Le secret médical au cœur de la controverse

L'employeur, qui a eu accès au dossier, a reproché à la caisse de ne pas y avoir joint l'examen audiométrique ayant fondé la reconnaissance de la maladie professionnelle. A noter qu'une évaluation audiométrique, répondant à des conditions strictes, est exigée par le tableau n°42. Du fait de cette carence, l'employeur considérait que la décision de la caisse de prise en charge de la maladie professionnelle lui était inopposable.

La caisse estimait, quant à elle, que ces examens d'audiométrie étaient couverts par le secret médical et n'avaient donc pas à figurer au dossier. Aussi, la caisse avait précisé que ses services administratifs n'avaient pas eu accès à cet examen détenu par le service médical, ce dernier ne pouvant lui transmettre en raison de ses obligations légales et déontologiques, sauf en cas d'expertise.

Comment alors articuler le respect des droits de la défense de l'employeur et la protection du secret médical ?

La Cour de cassation et son revirement de jurisprudence

La Cour de cassation a, au cours de ces dernières années, adopté différentes positions sur cette problématique.

Elle avait eu l'occasion de faire primer le secret médical en considérant que des examens médicaux n'avaient pas à figurer dans le dossier de la caisse[6]. Mais, concernant plus spécifiquement l'examen audiométrique prévu au tableau n°42 des maladies professionnelles, la Cour de cassation avait, en revanche, estimé que cet examen *« échappe au secret médical »* en considérant qu'il s'agit d'un *« élément nécessaire à la réunion des conditions du tableau n°42 ».*

Dans notre affaire, la Cour de cassation n'a pas suivi sa dernière jurisprudence en estimant que *« l'audiogramme mentionné au tableau n°42 des maladies professionnelles constitue un élément du diagnostic couvert par le secret médical, de sorte qu'il n'a pas à figurer dans les pièces du dossier constitué par les services administratifs de la caisse »*.

La Cour de cassation a notamment justifié son *« revirement de jurisprudence »* comme suit :

- Sa jurisprudence passée [faisant échapper l'examen audiométrique au secret médical] pose des difficultés *« au regard des obligations déontologiques auxquelles sont soumis les professionnels de santé »* ;
- L'équilibre entre le droit de la victime – le salarié – au respect du secret médical et le droit de l'employeur à une procédure contradictoire est *« préservé par la possibilité pour l'employeur contestant le caractère professionnel de la maladie de solliciter du juge la désignation d'un expert à qui seront remises les pièces composant le dossier médical de la victime »* [7].

Ce que l'on peut retenir de cette décision

Les éléments de diagnostics (examens médicaux), y compris ceux visés dans les tableaux de maladie professionnelle, n'ont pas à figurer dans le dossier de la caisse d'assurance maladie et, ainsi, n'ont pas à être communiqués à l'employeur.

Cette décision confirme la portée large du secret médical. En effet, l'employeur, qui ne peut accéder directement aux examens médicaux justificatifs, devra, en cas de difficulté/contestation s'en remettre à une expertise médicale (l'expert désigné pourra, quant à lui, être destinataire des examens médicaux).

[1] Cass. Civ. 3ème, 13 juin 2024, n°22-15.721.

[2] Pour mémoire, une maladie professionnelle est considérée comme telle, soit parce qu'elle figure dans le tableau des maladies professionnelles (ces maladies étant présumées avoir été contractées dans le cadre professionnel si elles répondent aux conditions figurant audit tableau), soit parce qu'elles répondent à des conditions strictes (maladies essentiellement et directement causées par le travail habituel et entraînant le décès ou une incapacité permanente d'au moins 25%).

[3] Article R.461-9 du Code de la sécurité sociale.

[4] Article R.441-14 du Code de la sécurité sociale.

[5] Article R.441-14 du Code de la sécurité sociale.

[6] Exemples : Cass. Civ. 2ème, 17 janvier 2008, n°07-13.356 ; Cass. Civ. 2ème, 5 avril 2012, 10-28.484 ; Cass. Civ. 2ème, 30 mars 2017, 16-14.674 ; Cass. Civ. 2ème, 29 mai 2019, n° 18-14.811.

[7] Dans ce sens : CEDH, décision du 27 mars 2012, Eternit c. France, n° 20041/10.

VU DANS LA PRESSE

« LA VEILLE ACTEURS DE SANTÉ », JUIN 2024

HEBERGEMENT DES DONNEES DE SANTE ET CERTIFICATION : UN NOUVEAU REFERENTIEL APPLICABLE DES NOVEMBRE 2024 !

Un nouveau référentiel pour la certification HDS a été publié au Journal officiel mi-mai. Ce document est porteur de nombreuses modifications pour l'activité d'hébergement externalisé des données de santé personnelles… Et traite entre autre de la délicate question de la souveraineté qui fait tant débat. Une explication de texte d'Alexandre Fievée, avocat associé, et d'Alice Robert, Avocat Counsel du cabinet Derriennic Associés pour La Veille Acteurs de Santé.

L'exigence d'une certification HDS

Toute personne physique ou morale à l'origine de la production ou du recueil de données de santé à caractère personnel à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, ou le patient lui-même, le cas échéant, doit faire appel à un prestataire titulaire d'une certification *« HDS »* lorsqu'elle/il externalise l'hébergement de telles données[1].

Cette certification vise à assurer *« que les hébergeurs de données de santé mettent en œuvre des systèmes de gestion de la sécurité des systèmes d'information à l'état de l'art des normes internationales »*.

La certification repose alors sur une évaluation de conformité dudit prestataire à un référentiel, le *« référentiel de certification HDS »*, dont la dernière version avait été approuvée par arrêté du 11 juin 2018.

Ce référentiel définit les exigences applicables à la certification *« HDS »* incluant le respect d'un certain nombre de règles et de normes, dont des normes ISO. Concrètement, l'hébergeur choisit un organisme certificateur qui doit être accrédité par le COFRAC (ou tout équivalent européen), lequel procède à un audit de conformité au référentiel. Tout certificat de conformité HDS est délivré pour une durée de 3 ans, étant précisé qu'un audit de surveillance annuel est effectué.

La nécessité d'une mise à jour du référentiel

Après 5 ans et des retours d'expériences, l'Agence Numérique de la Santé, sous l'égide de la Délégation ministérielle du numérique en santé, a lancé un chantier de révision du référentiel de certification HDS.

Certains points du référentiel nécessitaient effectivement des clarifications ou, à tout le moins, des compléments et adaptations avec un triple objectif :

- Améliorer la lisibilité des garanties apportées par un hébergeur certifié sur les prestations réalisées pour un client donné (professionnel de santé, patient…) ;
- Clarifier les obligations contractuelles de l'hébergeur déjà définies dans le Code de la santé publique[2] ;

- Renforcer les exigences de protection des données personnelles au regard des transferts en dehors de l'Union européenne.

C'est dans ce cadre, qu'un nouveau référentiel de certification HDS a été élaboré, en collaboration avec la CNIL, puis approuvé par un arrêté du 26 avril 2024, publié le 16 mai dernier.

Ce qu'il faut en retenir : l'activité « 5 », la conformité contractuelle, la souveraineté des données et la sécurité

Le nouveau référentiel HDS contient de nombreuses modifications et précisions d'exigences par rapport au référentiel de 2018. Parmi les nouveautés apportées, quatre points méritent une attention particulière.

Point 1 – Le premier point concerne l'activité 5 dite *« d'administration et d'exploitation d'applications du système d'information contenant des données de santé »,* une des 6 activités d'hébergement concernées par la certification et qui n'était pas sans poser de difficultés d'appréciation.

Le nouveau référentiel en propose une définition détaillée comme suit : l'activité *5 « consiste en la maitrise des interventions sur les ressources mises à la disposition du client de l'Hébergeur »*. Aussi, elle *« comprend l'intégralité des activités annexes suivantes »* :

- *« La définition d'un processus d'attribution et de revue annuelle de droits d'accès nominatifs, justifiés et nécessaires » ;*
- *« La sécurisation de la procédure d'accès » ;*
- *« La collecte et la conservation des traces des accès effectués et de leurs motifs » ;*
- *« La validation préalable des interventions (plan d'intervention, processus d'intervention) ».*

« La validation des interventions consiste à s'assurer qu'elles ne dégradent pas la sécurité de l'information hébergée ni pour le client concerné ni pour les autres clients de l'Hébergeur. Cette validation peut être effectuée dans les cas suivants : » (i) *« a priori, pour les interventions que le client pourrait effectuer en autonomie »* et (ii) *« lors de la demande d'intervention lorsqu'il sollicite l'Hébergeur ».*

Le référentiel rappelle que ces opérations *« sont intrinsèques et obligatoires »* aux activités 1 à 4, de sorte que c'est seulement lorsque l'hébergeur exerce uniquement ces opérations qu'il doit être certifié pour l'activité 5.

Point 2 – Le deuxième point concerne les exigences en termes de conformité contractuelle. Le nouveau référentiel impose, en effet, que l'hébergeur fournisse un modèle de contrat conforme aux exigences indiquées dans le référentiel, lesquelles reprennent essentiellement celles prévues au Code de la santé publique[2].

L'hébergeur doit également être plus transparent sur les garanties qu'ils apportent directement, ou celles de son/ses sous-traitant(s), en devant remplir, dans certains cas, une matrice type à intégrer dans ses contrats.

Point 3 – Le troisième point porte sur des exigences en matière de souveraineté des données.

Le référentiel requiert effectivement désormais que l'hébergement physique des données personnelles de santé soit effectué exclusivement dans l'Espace Economique Européen (EEE). En outre, si l'hébergeur ou ses sous-traitants (i) accèdent à distance, depuis un pays tiers à l'EEE, aux données, ou (ii) sont soumis à des lois d'un pays tiers n'assurant par un niveau de protection adéquat au sens du RGPD, alors l'hébergeur *« doit en informer ses clients dans le contrat et lui préciser les risques associés, ainsi que les mesures techniques et juridiques mises en œuvre pour les limiter ».* Par ailleurs, l'hébergeur a l'obligation de publier, sur son site internet, une cartographie *« des éventuels transferts des données qu'il héberge vers un pays n'appartenant pas à l'EEE ».*

Point 4 – Le quatrième et dernier point concerne les exigences en termes de sécurité, le référentiel précisant *« l'articulation entre les exigences de la certification HDS et celles de la certification SecNumCloud proposée par l'ANSSI »* et intégrant des évolutions de la norme ISO 27001.

Une entrée en vigueur le 16 novembre 2024

Ce nouveau référentiel entre en vigueur le 16 novembre 2024. Il sera ainsi applicable aux hébergeurs qui présenteront une demande de certification (que ce soit des premières demandes de certification ou des demandes de renouvellement d'une telle certification), à compter de cette date. Pour les hébergeurs déjà certifiés, ils devront se conformer à ce nouveau référentiel au plus tard le 16 mai 2026.

Il convient donc, dès à présent, de réaliser un audit des activités d'hébergement des données de santé externalisées afin de définir et de mettre en œuvre, dans les délais, un plan de mise en conformité.

[1] Article L.1111-8 du Code de la santé publique.
[2] Article R.1111-11 du Code de la santé publique.

DOCTRINE

RGPD

La réponse d'un professionnel à un avis en ligne n'échappe pas au RGPD

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 de l'application du RGPD à la réponse publiée par un professionnel de santé à un avis en ligne, publié par une patiente après une consultation chez ce professionnel.

En application de l'article 4 du RGPD, le traitement se définit comme toute opération portant sur des données personnelles, quel que soit le procédé utilisé. La définition est très large et englobe notamment la collecte de données personnelles, leur enregistrement, leur conservation, leur extraction, mais également leur communication ou leur diffusion.

La publication de données personnelles sur un site en ligne (ou sur les réseaux sociaux) s'analyse donc comme un traitement de données personnelles soumis au RGPD, à moins qu'il ne s'agisse d'un traitement réalisé dans le cadre d'une activité strictement personnelle ou domestique (article 2, paragraphe 2, c) du RGPD)[1].

En d'autres termes, il n'est pas fait application du RGPD si la sphère publique n'est pas impactée. En revanche, dès lors que les données ont été rendues accessibles à un nombre indéfini de personnes, par exemple, en raison de leur mise en ligne, le traitement est soumis au RGPD. Il appartient alors à celui qui est à l'origine de cette publication – le responsable du traitement – de respecter les termes du RGPD et notamment les principes de licéité, de limitation des finalités et de minimisation des données, tels que visés à l'article 5 paragraphe 1 du RGPD. Le responsable de traitement se doit, par ailleurs, de veiller au respect de l'interdiction de principe des traitements de données dites « *sensibles* » (données de santé, etc.), telle que posée à l'article 9, paragraphe 1 du RGPD, sauf s'il est en mesure de se prévaloir de l'une des exceptions visées au paragraphe 2 du même article (consentement de la personne concernée, sauvegarde des intérêts vitaux de la personne, etc.).

L'affaire[2]

Une patiente s'est rendue au cabinet médical d'un médecin spécialisé en gynécologie.

Ce dernier lui a diagnostiqué une infection. Quelques jours après cette visite, la patiente a publié, sous un nom d'emprunt, un avis en ligne indiquant en substance : « *Je ne le recommande pas comme médecin. Il s'est comporté avec condescendance à mon égard, sans aucune trace d'empathie et n'a absolument pas tenu compte de moi en tant que patiente, même lorsque j'étais désespérée et que je me suis mise à pleurer. Ne m'a même pas demandé la raison de ma visite et m'a immédiatement renvoyé vers son assistante.* » Le lendemain, le médecin a réagi, en publiant la réponse suivante : « *J'ai diagnostiqué son infection vaginale et l'ai traitée de manière professionnelle. Vous avez pu venir le jour même et n'avez rien eu à payer. Malheureusement, ce n'est pas suffisant pour vous et maintenant vous me reprochez un manque d'empathie... De mon côté, j'attends également un certain degré de coopération et d'attention afin de pouvoir mener à bien l'entretien médical.* »

À la suite de la publication de cette réponse, la patiente a déposé une plainte auprès de l'autorité autrichienne de protection des données, qui s'est saisie du dossier.

Considérant que la publication en ligne du commentaire litigieux du professionnel de santé ne pouvait s'analyser comme un traitement relevant d'une activité strictement personnelle ou domestique au sens de l'article 2, paragraphe 2, c) du RGPD, l'autorité a estimé que le RGPD s'applique au cas d'espèce, et ce d'autant qu'il ne fait aucun doute que le médecin a, en publiant le commentaire litigieux, traité des données personnelles concernant la patiente, données qualifiées par ailleurs de données de santé s'agissant du diagnostic médical. Par conséquent, l'autorité a recherché si une exception (article 9, paragraphe 2) au principe d'interdiction portant sur le traitement des données de santé pouvait s'appliquer au cas d'espèce.

Une telle publication ne pouvant se fonder sur aucune des exceptions énumérées à l'article 9 paragraphe 2 du RGPD, l'autorité autrichienne de protection des données a considéré que le médecin avait violé le RPGD. Par ailleurs, ce dernier a enfreint le principe de limitation des finalités énoncé à l'article 5, paragraphe 1, a), dans la mesure où « *il n'existait aucun lien concret, cohérent ou suffisamment étroit entre la finalité de la collecte des données et leur traitement ultérieur* », et ce d'autant que « *la personne concernée ne pouvait prévoir que [le médecin] publierait des données relatives à son diagnostic médical en réponse à son commentaire.* »

Quelles recommandations ?

Les publications en ligne, dès lors qu'elles comportent des données personnelles concernant une personne physique, tombent sous le coup du RGPD. Il convient, en conséquence, d'être extrêmement prudent et de s'assurer que ce traitement repose sur une base légale (principe de licéité). Par ailleurs, il est fondamental pour l'auteur de la publication de vérifier, dès lors que des données dites « *sensibles* » sont publiées, s'il peut se prévaloir de l'une des exceptions de l'article 9 paragraphe 2 du RGPD. À défaut de pouvoir s'en prévaloir, son traitement doit être considéré comme illicite. S'agissant de surcroît d'un professionnel de santé, comme dans l'affaire susvisée, il est évident que, au-delà du RGPD, il y aussi une vraie problématique d'atteinte au secret médical.

Alexandre FIEVEE
Avocat associé
Derriennic Associes

Notes

(1) Expertises, n° 493, septembre 2023, p. 282 ; CJUE, 6 novembre 2003, C-101/01 ; CJUE, 11 décembre 2014, C-212/13 ; GPDP, 27 avril 2023, n° 9896468 ; Autorité de protection des données belge, 24 novembre 2020, DOS-2019-04412 ; Autorité de protection des données islandaise, 14 juin 2023, affaire n° 2022030544 ; Autorité de protection des données belge, 20 mars 2023, DOS-2022-00945 ; AEPD, EXP202204530, 28 août 2023.

(2) Autorité autrichienne de protection des données, 2023-0.420.407, 29 juin 2023.