TRAITEMENT ILLICITE DE DONNÉES RELATIVES À LA SANTÉ

UNLAWFUL PROCESSING OF DATA RELATING TO HEALTH

Par Pierre DESMARAIS* et Maël BERTHO*

RÉSUMÉ

Pour la première fois, un médecin hospitalier a été condamné par une juridiction pénale pour traitement illicite de données concernant une patiente. Cette décision devrait conduire les professionnels de santé hospitaliers à une vigilance accrue en matière de traitement de données personnelles de santé.

MOTS-CLÉS

Données personnelles, Traitement illicite, Médecin hospitalier, Condamnation.

SUMMARY

For the first time, a hospital doctor has been convicted by a criminal court for the unlawful processing of data concerning a patient. This decision should lead hospital health professionals to greater vigilance in the processing of personal health data.

KEYWORDS

Personal data, Unlawful processing, Hospital doctor, Conviction by a criminal court.

Un médecin de l'Assistance publique-Hôpitaux de Marseille (AP-HM) a été condamné, le 7 juin 2017, à une amende de 5 000,00 euros pour traitement illicite de données relatives à la santé. On peut légitimement se mettre à la place de cette mère de famille qui, tapant par curiosité son nom dans un moteur de recherche bien connu un soir de février 2013, accède en toute liberté à un mystérieux site internet comprenant notamment le dossier médical de sa grossesse en 2008. Le « dossier enfant » comportait des données personnelles « sensibles », puisqu'outre ses nom et prénom, étaient mentionnés son numéro de sécurité sociale ainsi que des informations sur l'état de santé du bébé et divers commentaires médicaux.

A la suite de l'enquête, ont été renvoyés devant le tribunal correctionnel le pédiatre ayant constitué cette base de données, le directeur du service d'information et de l'organisation de l'AP-HM en poste au moment des faits ainsi que le gérant de la société DBSI, propriétaire du nom de domaine utilisé par le site litigieux.

Les poursuites ont été diligentées pour traitement de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre, concernant les deux premiers, et pour hébergement de données de santé sans l'agrément prévu à l'article L1111-8 du Code de la Santé Publique.

Ce dernier se tirera indemne de la procédure, les juges, faisant application du principe d'interprétation stricte de la loi pénale, ayant souligné que la propriété du nom de domaine ne permettait pas de retenir la qualification d'hébergement illicite de données de santé.

Le directeur de l'information et de l'organisation de l'AP-HM n'a pas été condamné, aucun élément du dossier ne démontrant qu'il avait connaissance de

* Cabinet Pierre Desmarais avocats ; pierre@desmarais-avocats.fr

l'externalisation effective des données et des conditions de leur hébergement.
Le médecin a reconnu les faits, tout en soutenant que la direction de l'AP-HM avait toujours été au fait des conditions d'hébergement des données, ce qui a logiquement conduit à sa condamnation pour traitement illicite de données à caractère personnel.
Bien qu'il ressorte implicitement du jugement que le Tribunal considère que le médecin a agi en qualité de responsable de traitement, on ne peut que regretter, ici, que les juges soient restés flous sur la question.
En effet, on sait que le Règlement Général relatif à la Protection des Données (RGPD) prévoit expressément la possibilité de déclarer un sous-traitant co-responsable de traitement.
Voilà en tous cas une décision qui devrait conduire les professionnels de santé hospitaliers à une vigilance accrue en matière de traitement de données relatives à la santé. ■

TGI DE MARSEILLE, 6E CH. CORR., JUGEMENT DU 7 JUIN 2017

Le Procureur de la République, AP-HM / M. X., Mme Y. et M. Z.

Monsieur X. a été cité à l'audience du 16/11/2016 par Monsieur le Procureur de la République suivant acte de la Selas Officiales M.A, Huissier de justice, délivré le 03/10/2016 à étude (AR non rentré).
La citation est régulière en la forme ;
L'affaire a été renvoyée contradictoirement à l'audience du 22/05/2017.
Monsieur X. a comparu à l'audience assisté de son conseil ; il y a lieu de statuer contradictoirement à son égard.
II est prévenu pour avoir, à Marseille, entre le 12 février 2010 et le 12 février 2013, en tous cas sur le territoire national et depuis temps non couvert par la prescription, en sa qualité de responsable de la Direction des Systèmes d'Information et de l'Organisation (DSIO) de l'AP-HM, procédé ou fait procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés, en l'espèce en n'ayant pas assuré la protection, la confidentialité et la sécurité des dossiers médicaux informatisés hospitaliers concernant des enfants et des femmes hospitalisés dans l'unité de néonatalogie de l'hôpital Nord de l'AP-HM et en participant à leur externalisation dans le cadre du développement d'un projet de réseau de santé pour des enfants nés prématurés.
faits prévus par ART.226-17 C.PENAL. ART.34, ART.2 LOI 78-17 DU 06/01/1978. et réprimés par ART.226-17, ART.226-22-2, ART.226-31 C.PENAL.

Madame Y. a été citée à l'audience du 16/11/2016 par Monsieur le Procureur de la République suivant acte de la SCP Rosa, Huissier de justice, délivré le 16/08/2016 à personne.
La citation est régulière en la forme ; il est établi qu'elle en a eu connaissance ;
L'affaire a été renvoyée contradictoirement à l'audience du 22/05/2017.
Madame Y. a comparu à l'audience assistée de son conseil ; il y a lieu de statuer contradictoirement à son égard.
Elle est prévenue pour avoir, à Marseille, entre le 12 février 2010 et le 12 février 2013, en tous cas sur le territoire national et depuis temps non couvert par la prescription, y compris par négligence, procédé ou fait procéder à des traitements de données à caractère personnel sans autorisation préalable de la Commission Nationale de l'Informatique et des Libertés (CNIL), en l'espèce en ayant fait traiter des données informatisées de santé concernant des enfants et des femmes hospitalisés dans l'unité de néonatalogie de l'hôpital Nord de l'AP-HM au sein de laquelle elle exerçait en qualité de pédiatre, dans le cadre du développement d'un projet de réseau de santé pour des enfants nés prématurés, sans autorisation préalable de la CNIL.
faits prévus par ART.226-16 AL.1 C.PENAL. ART.25, ART.26, ART.27, ART.2 LOI 78-17 DU 06/01/1978. et réprimés par ART.226-16 AL.1, ART.226-31 C.PENAL.

Monsieur Z. a été cité à l'audience du 16/11/2016 par Monsieur le Procureur de la République suivant acte de la SCP Castanie, Huissier de justice, délivré le 26/08/2016 à étude (AR non rentré).
La citation est régulière en la forme ;

L'affaire a été renvoyée contradictoirement à l'audience du 22/05/2017.
Monsieur Z. a comparu à l'audience assisté de son conseil ; il y a lieu de statuer contradictoirement à son égard.
Il est prévenu :
pour avoir, à Frocourt (60) et à Marseille, entre le 12 février 2010 et le 12 février 2013, en tous cas sur le territoire national et depuis temps non couvert par la prescription, en sa qualité de gérant de la société DBSI, procédé à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés, en l'espèce en créant un portail de saisie de données informatisées de santé concernant des enfants et des femmes hospitalisés dans l'unité de néonatalogie de l'hôpital Nord de l'AP-HM dans le cadre d'une prestation relative à un projet de réseau de santé pour des enfants nés prématurés, sans s'assurer de la sécurisation de ce portail,
faits prévus par ART.226-17 C.PENAL. ART.34, ART.2 LOI 78-17 DU 06/01/1978. et réprimés par ART.226-17, ART.226-22-2, ART.226-31 C.PENAL.
pour avoir, à Frocourt (60) et à Marseille, entre le 12 février 2010 et le 12 février 2013, en tous cas sur le territoire national et depuis temps non couvert par la prescription, en sa qualité de gérant de la société DBSI, hébergé ou fait héberger des données à caractère personnel sans agrément délivré par le ministre chargé de la santé,en l'espèce en choisissant en connaissance de cause un hébergeur rémunéré par lui qui n'était pas agréé et qui n'était pas sécurisé alors qu'il s'agissait de traiter de données informatisées de santé concernant des enfants et des femmes hospitalisés dans l'unité de néonatalogie de l'hôpital Nord de l'AP-HM.
faits prévus par ART.L1115-1, ART.L.1111-8, ART.R.1111-15, ART.R.1111-15-1, ART.R.1111-16 C.SANTE.PUB. et réprimés par ART.L.1115-1 C.SANTE.PUB.

SUR L'ACTION PUBLIQUE

Le 12 février 2013, Madame W. déposait plainte auprès des services de gendarmerie de B., lieu de son domicile, en expliquant que la veille vers 23 heures, alors qu'elle faisait des recherches sur Internet et avait tapé par curiosité son nom et son prénom sur le moteur de recherche Google, un résultat s'était affiché, avec ses nom, prénom et l'inscription « dossier enfant » avec son numéro de sécurité sociale (sans la clé) ; après avoir cliqué sur ce résultat, il était apparu un site, « http://www.dbsi.eu/n et d/ consultation dossier enfant.asp », qui comportait un menu déroulant comprenant des noms et prénoms précédés d'un numéro de sécurité sociale.
Elle indiquait qu'en cliquant sur son nom, le dossier de la naissance de son fils, Jean François né le 22 juin 2008 à Marseille à l'Hôpital Nord, était apparu, comportant des informations telles que notamment l'état du bébé, des commentaires médicaux, qu'elle ne connaissait qu'en partie.
Elle précisait qu'elle pouvait avoir accès aux autres dossiers qui ressortaient de ce site, qu'il y avait également des onglets qui permettaient de modifier ou supprimer les dossiers.
Elle déposait plainte du chef de violation du secret professionnel à l'encontre de l'Hôpital Nord, qu'elle avait par ailleurs alerté de la situation.
Le lendemain, à 17 heures, le directeur de l'Hôpital Nord avisait les gendarmes de ce qu'il avait retrouvé le responsable du serveur incriminé, et qu'il lui avait demandé de fermer son site.
Les gendarmes constataient alors que le site en question n'était effectivement plus accessible sur les pages internet.
A la suite de cette plainte, à la demande des services de gendarmerie, l'Office Central de Lutte contre les Atteintes à l'Environnement et à la santé Publique (Argueil 94), fournissait un document qui exposait le statut particulier des données de santé, et précisait le droit d'accès au dossier médical, les obligations des hébergeurs de santé notamment. Il fournissait également des informations sur le site « dbsi.eu ».
Il en ressortait ainsi que le nom du domaine de ce site avait été acheté par Monsieur Z., gérant de la SARL DBSI, sise à Frocourt, radiée depuis le 28 août 2009, laquelle avait pour activité le traitement de données, la réalisation de logiciels, de conseils en systèmes informatiques.
Monsieur Z. avait créé une nouvelle société, avec la même activité, depuis le 20 juillet 2011, soit la société ANLY6, sise à la même adresse.
Ce document rappelait par ailleurs que les données médicales sont des informations sensibles qui nécessitent un haut niveau de sécurité, et en application des dispositions de la loi Informatique et Liberté du 16 janvier 1978, par principe, elles ne peuvent être utilisées et divulguées que dans des conditions définies par la loi, et imposent aux professionnels de santé, comme aux responsables de fichiers, de prendre les mesures nécessaires pour garder notamment leur confidentialité, leur accessibilité qu'à des personnes habilitées notamment en raison de leurs fonctions.
Il était par ailleurs rappelé que le non respect de cette obligation de sécurité, par négligence ou par l'absence de mesures de sécurité, est prévu et sanctionné par la Loi Informatique et Liberté et l'article 226-17 du Code pénal.
Ainsi, ces données médicales ne peuvent être utilisées et communiquées que dans des conditions définies par la loi ; les réseaux de santé qui souhaitent mettre en œuvre un dossier médical partagé accessible via internet par les professionnels de santé, doivent

notamment effectué une demande d'autorisation préalable auprès de la Commission Nationale de l'Informatique et des Liberté en application des articles 26 et 27 de la loi 7817 du 6 janvier 1978, dite loi Informatique et Libertés.
Il est également précisé que l'activité d'hébergement des données de santé consiste en une activité d'externalisation, de détention et de conservation de ces données recueillies ou produites à l'occasion d'un acte de prévention, de diagnostic ou de soin, et confiées à un tiers, afin d'assurer leur pérennité et leur confidentialité ; un contrat lie l'hébergeur et la personne ou l'organisme à l'origine du dépôt des données.
En application des dispositions de l'article L111-8 du Code de la santé publique, les hébergeurs de données médicales doivent être agréés

* * *

Le 6 mars 2013, Monsieur V., directeur des Affaires Juridiques de l'Assistance Publique des Hôpitaux de Marseille, mandaté par l'Assistance Publique des Hôpitaux de Marseille, déposait plainte, à la suite de la plainte de Madame W.
Il exposait que lorsque la Direction avait été avisée du problème, il avait aussitôt demandé à la Direction Informatique de sécuriser les données ; il a joint le courrier adressé en ce sens à la Société DS ANALY SIX.
Il expliquait qu'aux termes d'une enquête diligentée en interne, le Docteur Y. avait été identifiée comme étant la responsable de la mise en place de la base de données, qui lui permettaient à elle et son service de suivre les patients, que le site d'hébergement (DS ANALY6) n'était pas agréé par l'ASIP Santé, que le processus d'identification et d'authentification pour accéder aux données du site n'était pas sécurisé et pouvait être contourné.
Entendue par les services de police le 29 novembre 2013, Madame Y. expliquait qu'elle était médecin depuis 1992, et praticien hospitalier, responsable de l'Unité fonctionnelle de néonatalogie et du Pôle Réanimation néonatale du Professeur S., à l'Hôpital Nord de Marseille depuis 1996.
De cette audition, il ressort qu'elle était bien à l'origine du cahier des charges de la base de données.
Ainsi de mai 2006 à mai 2007, elle a participé à la création de ce cahier des charges, les médecins du service devant remplir un formulaire Word avec des renseignements médicaux sur des patients (antécédents, grossesses, historique de l'hospitalisation du bébé, etc.).
De mai 2007 à janvier 2009, des essais de saisies dans le service ont été mis en place pour développer le projet avec l'APHM, tout en travaillant également à la faisabilité du projet dans le cadre de l'appel d'offre publique du réseau « Naître et Devenir ».
Le but était de créer un dossier médical et de suivi, une base de données épidémiologiques pour le suivi des bébés prématurés, pour améliorer la collaboration entre les acteurs médicaux par un partage des informations, notamment en cas de transfert vers d'autres hôpitaux, et également évaluer le service de néonatalogie et le réseau de suivi ; ces informations devaient être à l'usage uniquement des professionnels médicaux.
Madame Y. a contacté la société DBSI de Monsieur Z. pour la création du portail de saisie des données et elle a transmis à cette société les données médicales.
Le projet n'a pas été retenu par le réseau « Naître et Devenir » le 19 février 2009, mais il a obtenu un avis favorable de la Commission de l'Innovation de l'APHM dès le 13 janvier 2009.
Madame Y. soutient ainsi que la Direction du Service Informatique de l'APHM était parfaitement informée du fait que la société DBSI hébergeait les données médicales, sans que rien ne soit fait pour valider ou non cet hébergeur, ou pour faire héberger ces données directement par l'hôpital.
Elle admet en tout état de cause qu'elle savait que le traitement informatisé, automatisé de ces données médicales, dont elle est à l'origine, n'avait pas reçu l'autorisation de la CNIL.
En ce qui concerne Monsieur Z., il a expliqué avoir été contacté en 2008 par Madame Y., pour le réseau »Naître et Devenir » dans le cadre d'un projet de constitution d'une base de données « patients » sur les grands prématurés, pour collecter toutes les informations de santé d'avant la naissance jusqu'à l'âge de trois ans, l'idée étant de collectionner le maximum de données afin d'évaluer les risques encourus ; il s'agissait d'un outil informatique et statistique pour réaliser des analyses des données. Il a confirmé que son projet n'avait pas été retenu par le réseau » Naître et Devenir », mais que Madame Y. l'a retenu pour faire un test sur l'Hôpital Nord.
Il a expliqué qu'il a ainsi constitué le logiciel entre 2009 et 2011, qui comprenait la mise en ligne d'un portail de saisie sur internet, lequel était hébergé chez l'hébergeur Hosteur.com à Marseille, lequel n'était pas agréé pour les données de santé; ce portail était accessible avec un login et un mot de passe.
Il a confirmé à l'audience avoir créé le logiciel et l'avoir mis sur un site provisoirement, pour vérifier son bon fonctionnement, en précisant que lorsque le logiciel est mis sur le site, il ne contient encore aucune donnée.
Enfin, en ce qui concerne Monsieur X., il était Directeur du Service d'Information et de l'Organisation de l'AP-HM au moment des faits.
Il a exposé que le docteur Madame Y. avait un projet de développement d'un système informatique visant à collecter des données sur des grossesses, mais que son service n'y a finalement pas donné suite, n'ayant ni le

temps, ni les ressources nécessaires, que le docteur Madame Y. a mené seule son projet.
Il a affirmé ne pas avoir participé à la demande de développement et d'hébergement, celui-ci ayant été géré par Madame Y. à l'insu de son service.

* * *

Madame Y. qui n'a pas contesté avoir fait procéder à un traitement informatisé de données médicales sans autorisation de la CNIL, sera déclarée coupable de l'infraction reprochée à cet égard.
En ce qui concerne Monsieur Z., l'infraction qui lui est reprochée relative au traitement de données sans précautions pour préserver leur sécurité, suppose, en application de l'article 34 de la loi n°78/17 du 6 janvier 1978, que son auteur soit le responsable du traitement.
Faute pour Monsieur Z. de revêtir cette qualité de responsable du traitement, il doit être relaxé du chef de cette infraction.
Par ailleurs, la seconde infraction reprochée, prévue à l'article L115-1 du Code de la Santé Publique, sanctionne le fuit d'héberger des données de santé sans être titulaire de l'agrément prévu à l'article L1111-8 ; or, en l'espèce, il est constant que la société de Monsieur Z. n'est pas l'hébergeur des données médicales, et les dispositions légales précitées ne sanctionnent en aucun cas le fait d'avoir fait héberger des données de santé par un héberger non agrée.
Ce dernier sera donc également relaxé du chef de cette infraction.
Enfin, en ce qui concerne Monsieur X., en premier lieu, à l'examen du document « portant délégation de signature » en vigueur à la date des faits, ce document réalise, notamment en son article 16, pour ce dernier une réelle délégation de pouvoir, puisqu'il lui est attribué le pouvoir de signer notamment tous actes administratifs, documents et correspondances concernant les affaires de sa direction.
Sur l'infraction reprochée, malgré les déclarations constantes de ses co-prévenus, force est de constater qu'aucun document ne vient démentir ses affirmations également constantes selon lesquelles il n'a pas eu connaissance de l'externalisation effective des données médicales, et de leur hébergement chez un héberger non agréé.
Il sera en conséquence relaxé du chef de l'infraction reprochée.

SUR L'ACTION CIVILE

Attendu que l'**AP-HM Assistance Publique des Hôpitaux de Marseille** s'est constituée partie civile.
Qu'elle sollicite la condamnation de Monsieur Z. lui payer :

– la somme de 10 000 euros au titre du préjudice moral et d'image subi du fait de ses agissements,
– la somme de 4 000 euros au titre des frais irrépétibles.
– les dépens de l'instance.

Qu'il convient de déclarer recevable la constitution de partie civile de l'AP-HM Assistance Publique des Hôpitaux de Marseille.
Qu'au vu des éléments du dossier et des débats, il convient de la débouter de ses demandes en l'état de la relaxe intervenue à l'égard de Monsieur Z.

DÉCISION

Le tribunal, statuant publiquement, en premier ressort et contradictoirement à l'égard de Monsieur X., de Madame Y., de Monsieur Z. et de l'AP-HM Assistance Publique des Hôpitaux de Marseille.

SUR L'ACTION PUBLIQUE

Relaxe Monsieur X. et le renvoie des fins de la poursuite sans peine ni droit fixe de procédure.
Relaxe Monsieur Z. et le renvoie des fins de la poursuite sans peine ni droit fixe de procédure.
Déclare Madame Y. coupable d'avoir commis les faits. pour les faits de TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL SANS AUTORISATION commis à Marseille, entre le 12 février 2010 et le 12 février 2013,
Condamne Madame Y. au paiement d'une amende de cinq mille euros (5 000 euros) ;
En application de l'article 1018 A du code général des impôts, la présente décision est assujettie à un droit fixe de procédure de 127 euros dont est redevable Madame Y.

SUR L'ACTION CIVILE

Déclare recevable la constitution de partie civile de l'AP-HM Assistance Publique des Hôpitaux de Marseille.
La déboute de ses demandes en l'état de la relaxe intervenue à l'égard de Monsieur Z.
Le tout en application des articles 406 et suivants et 485 du Code de procédure pénale et des textes susvisés.

Le Tribunal : Christine Mee (vice-présidente), Anouk Bonnet (juge), Corinne Janackovic (juge rapporteur), Béatrice Mouries (greffière)

Avocats : Me Philippe Carlini, Me Nicolas Courtier, Me Nadia Laib, Me Pierre Ceccaldi ■