Tribunal de grande instance de Marseille, 7 juin 2017 (Données à caractère personnel, données sensibles, données de santé, données médicales, loi Informatique et Libertés, responsable de traitement, autorisation de la CNIL, hébergement de données en santé)

07/06/2017

Le 12 février 2013, Mme W. dépose plainte pour violation du secret professionnel à l'encontre de l'Hôpital N. après avoir trouvé sur un moteur de recherche son nom et prénom, le dossier de la naissance de son fils avec son numéro de sécurité sociale et des informations personnelles relatives à son état de santé. Le praticien est identifiée être à l'origine du cahier des charges de la base de données médicales en ligne. En effet, dans le cadre d'un appel d'offre publique, ce dernier avait fait appel à une société informatique pour créer un portail de saisie des données après que les données médicales lui aient été transmises puis hébergées chez un hébérgeur extérieur.

L'Office Central de Lutte contre les Atteintes à l'Environnement et à la Santé Publique rappelle à cette occasion le statut particulier des données de santé : « les données médicales sont des informations sensibles qui nécessitent un haut niveau de sécurité, et en application des dispositions de la loi Informatique et Libertés du 16 janvier 1978, par principe, elles ne peuvent être divulguées que dans des conditions définies par la loi, et imposent aux professionnels de santé, comme aux responsables de fichiers, de prendre des mesures nécessaires pour garder notamment leur confidentialité, leur accessibilité qu'à des personnes habilitées ». Le non-respect de cette obligation de sécurité, par négligence ou par l'absence de mesures de sécurité, est prévu et sanctionné par cette même loi et l'article 226-17 du code pénal. Les réseaux de santé qui souhaitent partager les données médicales via internet doivent effectuer une demande d'autorisation préalable auprès de la Commission nationale informatique et Libertés (CNIL) (articles 26 et 27 de la Loi). Aussi « l'hébergeur des données de santé consiste en une activité d'externalisation, de détention ou 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 ». Aux termes de l'article L. 1111-8 du Code de la santé publique, les hébergeurs de données médicales doivent être agréés.

Le juge du tribunal de grande instance de Marseille déclare coupable le praticien « pour le traitement de données à caractère personnel sans autorisation » dans la mesure où elle reconnait en tout état de cause avoir procédé au traitement informatisé des données médicales sans avoir reçu l'autorisation de la CNIL. Elle est condamnée au paiement d'une amende de 5000 euros.