CYBERATTAQUES CONTRE LES DISPOSITIFS MÉDICAUX

Qui est responsable ?

A travers le monde, les établissements de santé sont de plus en plus victimes de cybercriminalité. Particulièrement sensibles, les données santé des patients sont devenues une cible. Charge aux établissements d'assurer leur sécurité, de définir les responsabilités et de prévoir une procédure rapide et efficace en cas de cyberattaques.

Maître Alexandra Iteanu

Un virus supplémentaire. En cette période de pandémie, de plus en plus d'établissements de santé subissent des cyberattaques. Dernier exemple en date en France : l'hôpital de Narbonne a subi à la mi-décembre les attaques d'un « cryptovirus », virus infectant les systèmes d'information de l'établissement. Si ici l'objectif de la cyberattaque n'était pas de détourner ou s'approprier les données de santé, celles-ci n'en sont pas moins devenues la nouvelle cible privilégiée des hackers et autres pirates informatiques.

DES DONNÉES SENSIBLES

Très particulières, ces données de santé se distinguent de données plus « classiques », puisqu'elles sont d'une grande sensibilité. Touchant l'intimité profonde des individus, leur vol ou effacement peut s'avérer fatal et augmente donc leur valeur aux yeux des hackers.

La loi elle-même distingue les données de santé des données à caractère personnel ordinaires. Ces dernières sont définies comme des données à caractère personnel « relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne » (article 4-15 du Règlement UE n°2016-679 dit « RGPD »). Considérées comme des données « sensibles », elles bénéficient d'un régime de protection plus strict établi par le RGPD (Règlement général de la protection des données) mais également par la loi française n°78-17 dite « Informatique et Libertés ». (Loi modifiée notamment des suites du RGPD n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

> **« Les objets connectés étant de plus en plus présents (...) leur utilisation nécessite un réel investissement technique et organisationnel »**

En milieu hospitalier ou préhospitalier, et plus particulièrement dans le cadre d'objets connectés (tensiomètres, glucomètres, etc.), ces données de santé sont susceptibles d'être traitées à grande échelle, et pour des périodes plus ou moins longues. Il est alors important de s'assurer de leur sécurité, de bien définir qui sont les responsables de leurs traitements, et de prévoir une procédure rapide et efficace en cas de cyberattaque.

DÉFINIR LES RÔLES SELON DES STATUTS JURIDIQUES DISTINCTS

Les hôpitaux et établissements de santé se dotent de plus en plus de dispositifs médicaux connectés qui permettent un suivi de leurs patients au quotidien. Ces objets connectés collectent ainsi une masse importante de données de santé des patients, allant du rythme cardiaque en passant par le poids ou encore le taux de glycémie... Ces dispositifs médicaux connectés, parce qu'ils collectent des données sensibles, doivent suivre un régime strict, mis en place par les personnes en charge de leur utilisation. Ces personnes sont qualifiées, selon le contexte, de « responsables du traitement » des données de santé, ou de « sous-traitants ».

Le responsable de traitement est défini par le RGPD comme toute personne qui « détermine les moyens et les finalités du traitement » des données de santé. Cette qualification s'opère donc au cas par cas. Dans le cadre des objets connectés en milieu hospitalier, la personne qui définit les modalités et finalités du traitement est dans de nombreux cas l'établissement lui-même, ou le chef d'un des services hospitaliers.

A côté de ce responsable de traitement, un second acteur très important voit son activité encadrée également : le sous-traitant.

Défini à l'article 4-8 du RGPD comme toute personne qui agit « pour le compte du responsable de traitement », il est en général, dans le cadre des objets connectés en milieu hospitalier, l'éditeur du logiciel intégré à l'objet connecté, le fabricant de l'objet en question, ou toute société de maintenance ou de support en lien avec cet objet connecté.

Une fois les rôles attribués, il est nécessaire pour le responsable de traitement et ses éventuels sous-traitants de s'assurer que les mesures techniques et organisationnelles imposées par les textes sont bien mises en place autour des dispositifs connectés. Si ces règles ne sont pas respectées, les sanctions sont lourdes, et peuvent s'élever jusqu'à 20 millions d'euros, ou 4 % du chiffre d'affaires annuel mondial s'il s'agit d'une entreprise. Dans le milieu médical, la Commission nationale de l'informatique et des libertés (CNIL), autorité de contrôle compétente en France, a prononcé le 7 décembre 2020 deux amendes de 3 000 et 6 000 euros à l'encontre de deux médecins libéraux pour avoir insuffisamment protégé les données personnelles de leurs patients et ne pas avoir notifié une violation de données à la CNIL.

© Sylvain Ley

En cas de cyberattaque, des mesures techniques concrètes doivent être prises, comme par exemple changer les mots de passe ou mettre en place des mesures de chiffrement.

CYBERATTAQUE EN MILIEU HOSPITALIER : COMMENT RÉAGIR ?

En cas de cyberattaque, c'est-à-dire de violation de données à caractère personnel, affectant l'objet connecté, le RGPD impose au responsable du traitement, ainsi qu'à ses sous-traitants concernés, une procédure à suivre.

Le responsable de traitement a notamment l'obligation de :

1) notifier la violation de données à caractère personnel à la CNIL dans un délai de 72 heures à compter de la prise de connaissance de la violation ;

2) et dans certains cas notifier les personnes concernées par cette cyberattaque.

Le sous-traitant a lui aussi l'obligation de notifier la violation à son responsable de traitement, dans les meilleurs délais, dès qu'il a pris connaissance de cette cyberattaque.

Responsable de traitement et sous-traitant doivent également tout mettre en œuvre pour remédier à cette violation de données personnelles sur l'objet connecté. Comment ? En prenant des mesures techniques concrètes, comme par exemple changer les mots de passe, ou mettre en place des mesures de chiffrement.

QUID DES PATIENTS IMPACTÉS ?

Les personnes victimes de cyberattaque doivent, dans la plupart des cas, être informées de l'existence de la violation de leurs données de santé, de ses éventuelles conséquences, des mesures prises pour remédier à cette cyberattaque, et enfin se voir communiquer les coordonnées de la personne à contacter.

Il revient ensuite au patient victime de la cyberattaque de demander des précisions sur cette dernière s'il le souhaite, et d'invoquer les droits prévus par le RGPD auprès du responsable de traitement : l'effacement de ses données, ou leur transfert par exemple.

Au final, les objets connectés étant de plus en plus présents à l'hôpital, allant même jusqu'à envisager une « chambre connectée », leur utilisation nécessite un réel investissement technique et organisationnel pour ses acteurs. En amont, il est important de s'assurer que des mesures de protection entourent ces objets connectés et que les sous-traitants en charge de son utilisation sont fiables, pour éviter toutes failles de sécurité. En cas de cyberattaques, une procédure devra être mise en place pour gagner du temps et informer la CNIL et les personnes concernées. ■

Maître Alexandra Iteanu

Avocate au Barreau de Paris, Maître Iteanu est titulaire du Master 2 Droit des Créations Numériques de l'université de Paris XI, ainsi que du LLM Propriété Intellectuelle et Nouvelles Technologies de l'université King's College de Londres. Spécialisée en droit du numérique, son expertise se porte tout particulièrement sur la protection des données personnelles, et plus particulièrement des données de santé.

© DR