Données de santé : pourquoi sont-elles si convoitées ?

Fiche pratique publié le **25/02/2021**, vu **3971 fois**, Auteur : La zone du droit

Ces dernières années, les cyber-délinquants font parler d'eux de plus en plus à travers leurs activités de nuisance qui se caractérisent par le vol massif de données sensibles à l'instar des données de santé.

La notion de données de santé trouve son origine dans la convention n° 108 du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel adoptée par le Conseil de l'Europe. Sans en donner de définition, ce texte prévoit que les données à caractère personnel relatives à la santé sont des catégories particulières de données, qui "ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées".

Aujourd'hui, le RGPD, la loi Informatique et Libertés adaptée en conséquence ainsi que les dispositions du Code de la santé publique constituent le socle de la nouvelle réglementation sur la protection des données personnelles, dont font partie les données de santé. Du fait toutefois de la grande sensibilité de ces données, leur traitement informatisé est rigoureusement encadré par le droit, qui impose des contraintes particulières de fiabilité, de disponibilité et de sécurité, avec quelques spécificités en matière de recherche scientifique.

Les données de santé ont été élevées au rang de données à caractère personnel sensibles par le Règlement Général Sur la Protection des Données à caractère Personnel dit (RGPD) en son article 4.15. Les données à caractère personnel concernant la santé sont les données relatives à la santé physique ou mentale, passée, présente ou future, 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. Selon la CNIL, cette définition comprend :

Les informations relatives à une personne physique collectées lors de son inscription en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services : un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ;

Les informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir des données génétiques et d'échantillons biologiques ;

Les informations concernant une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée (indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro).

Elle permet également d’englober certaines données de mesure à partir desquelles il est possible de déduire une information sur l’état de santé de la personne.

De plus dans le considérant numéro 1 du RGPD, le parlement Européen élève la protection des personnes physiques à l’égard du traitement des données à caractère personnel comme un droit fondamental : « La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. L'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée « Charte ») et l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne disposent que toute personne a droit à la protection des données à caractère personnel la concernant ».

Cependant, en cette période de crise sanitaire, la vigilance contre la piraterie informatique doit être très accrue dans le domaine sanitaire. En effet, depuis le déclenchement de cette crise sanitaire mondiale, les cyber-délinquants usent de tous les stratagèmes pour troubler la quiétude des autorités des gouvernements mondiaux.

Ces dernières années, les cyber-délinquants font parler d’eux de plus en plus à travers leurs activités de nuisance qui se caractérisent soit par les attaques informatiques avec demande de rançon, soit par déni de service ou encore par le vol massif de données sensibles à l’instar des données de santé.

Pourquoi les données de santé suscitent-elles une convoitise de la part des cyber-délinquants ?

I) Les données de santé : une convoitise des cyber-délinquants

Certes, les personnes concernées peuvent s'opposer en théorie à ce que leurs données à caractère personnel soient collectées et traitées en l'absence de leur consentement. Ce consentement doit notamment être explicite lorsque le traitement porte sur des catégories particulières de données, telles que les données sensibles relatives à la santé (RGPD, art. 9).

Aussi, l'exploitation des données de santé représente-elle un « matériel essentiel de la recherche en santé ».

Comme l'a rappelé la Présidente de la CNIL lors de son audition par la commission des lois de l'Assemblée nationale le 8 avril 2020, le cadre juridique protégeant les données à caractère personnel ne s'oppose pas à ce que celles-ci soient utilisées, notamment en matière sanitaire. Le RGPD ainsi que la loi Informatique et Libertés présentent en effet un cadre général de protection des données sensibles, complété par un ensemble de dispositions spécifiquement applicables au cas des données de santé.

Toutefois, ces données sensibles attirent les cyber-délinquants. Cette ruée s’explique par le manque de vigilance des autorités chargées de la préservation et de la confidentialité des données de santé de leurs clients.

On constate également l’impuissance des autorités publiques face au fléau de la cybercriminalité et ces techniques de plus en plus actualisées qui permettent aux cyber-délinquants de se faire plaisir quand ils en ont l’occasion. L’utilisation de moyens moins coûteux pour commettre de grands dégâts est l’art de ces cyber-délinquants.

Les trois grands types de risques de ces attaques incessantes sont la disparition de données, l'accès illégitime aux données et la modification non désirée de données. Si le dossier médical est altéré, cela peut avoir des conséquences graves sur le traitement du patient.

Monsieur Vincent TRELY, Président de l'Association pour la Promotion de la Sécurité de Systèmes d'Information de Santé (APSSIS) expliquait lors d'une interview les motivations qui attirent les cyber-délinquants vers les données de santé.

Premièrement selon lui, nous avons l'espionnage industriel : on subtilise aux laboratoires pharmaceutiques des données relatives à des recherches ou avancées médicales.

Vient ensuite le chantage. Les dossiers médicaux de patients sont volés aux hôpitaux pour les restituer moyennant une rançon. « Le cryptage est également à la mode en France : les pirates cryptent les données informatiques des établissements de santé et les décryptent contre une certaine somme d'argent »

En outre, d'ici 2022, selon le *Gartner*, plus de 30% des datacenters des hôpitaux seront hébergés dans le Cloud. Pourtant, d'après une enquête menée par Netwrix 1 en 2019, un organisme de santé sur trois ne protège pas suffisamment ses données alors que le secteur de la santé est une des cibles privilégiées des attaques informatiques. 26 % des acteurs du secteur déclarent avoir subi au moins un incident de sécurité lié au Cloud sur l'année écoulée.

Selon une enquête publiée par « *Libération* » le 23 février 2021, les données médico-administratives confidentielles de presque un demi-million de Français ont été dérobées dans les fichiers de laboratoire de biologie médicale avant d'être rendues accessibles en ligne.

Cette fuite massive a révélé ou affiché l'identité, le numéro de téléphone, l'adresse postale, le numéro de sécurité social, la date d'hospitalisation, CPAM, le ou les médecin (s) du patient, l'assurance/mutuelle du patient, CMU, adresse mail du patient.

Comme le rapporte « *Libération* » les personnes figurant sur le fichier informatique sont des cibles de choix pour du phishing personnalisé, risque d'usurpation d'identité, fausses ordonnances, message de détresse factices reprenant les problèmes de santé mentionnés.

Par ailleurs, cette fuite serait le résultat d'un différend entre plusieurs hackers qui n'ont pas trouvé de terrain d'entente pour l'exploitation commerciale de ces données très sensibles.

II) Les données de santé : un trésor pour les cyber-délinquants

A la recherche d'une source d'enrichissement, le vol des données de santé devient le grenier financier par excellence des cyber-délinquants. Elles sont aussi un véritable patrimoine, de plus en plus convoitées également par les géants du numérique en vue d'une monétisation. On les trouve aussi bien dans la mesure des constantes biologiques que dans l'application des plans de soins ou encore dans le contrôle technique des bâtiments.

Les cyber-délinquants se spécialisent de plus en plus dans le vol des données de santé en vue de leur vente aux différents géants du numérique qui ne peuvent que s'en réjouir. C'est un vrai business pourvoyeur de biens mal acquis.

Par ailleurs, les vols des données de santé ne profitent pas qu'aux géants du numériques. Ils profitent à bien d'autres acteurs. En effet, le vol d'informations sanitaires peut s'avérer être une affaire juteuse pour les compagnies d'assurances complémentaires et les laboratoires : pour les assurances, elles leur permettent d'ajuster les tarifs de manière plus précise. Quant aux industries

pharmaceutiques, elles pourraient établir des statistiques d'une importance capitale avec ces informations, dans le but d'orienter le marketing des médicaments.

Ces cyber-délinquants procèdent par la technique dite de rançongiciel: un code malveillant séquestre les données d'équipements informatiques infectés jusqu'à ce que la victime paie une rançon qui s'effectue généralement avec une cryptomonnaie telle que le Bitcoin.

Selon Vincent TRELY, Président du conseil d'administration de l'APSSIS, interrogé en février 2019 par *Korii*, un média du groupe Slate, « les données se revendent entre 30 et 200 bitcoins, donc en tout entre 30 000 et un million d'euros ».

On se rend compte du réel intérêt pour les cyber-délinquants de s'attaquer aux données de santé.

Pour finir, c'est le lieu de rappeler que face à la multiplication des cyber-attaques, surtout en ce qui concerne les données sensibles de santé, le Président Emmanuel MACRON a présenté le jeudi 18 Février 2021 la stratégie française en matière de cybersécurité, après un échange par visio-conférence avec les directeurs des hôpitaux de Dax et Villefranche-sur-Saône, récemment victimes de rançongiciels, a annoncé l'Elysée.

Il est prévu à cet effet une enveloppe d'un milliard d'euros, dont 720 millions de fonds publics, pour renforcer la filière et tripler son chiffre d'affaires à 25 milliards d'euros en 2025.

Pour l'heure, nous conseillerons à tous et surtout aux habitants du Nord-Ouest de la France, de changer tous leurs mots de passe et de faire très attention aux mails qu'ils recevrons ces temps-ci.

Sources :

La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental (https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679)

Urgence cybersécurité pour les organismes de santé (https://www.gatewatcher.com/fr/nos-actualites/blog/urgence-cybersecurite-pour-les-organismes-de-sante)

Sécurité des données de santé (https://healthcare.orange.com/fr/dossiers/securite-des-donnees-desante/#:~:text=Les%20trois%20grands%20types%20de,sur%20le%20traitement%20du%20patient)

Fuite de données un piratage resté trop longtemps secret : (https://www.liberation.fr/societe/fuite-de-donnees-un-piratage-reste-trop-longtemps-secret-20210223_T7FJKWWB2BG33J7QLUON5ZQJXM/)

Les données de santé : un trésor mondial (https://www.lemonde.fr/sciences/article/2020/03/02/les-donnees-de-sante-un-tresor-mondialement-convoite_6031572_1650684.html)

Les données de santé attirent les hackers (https://sante.lefigaro.fr/actualite/2015/02/13/23393-donnees-sante-attirent-hackers)