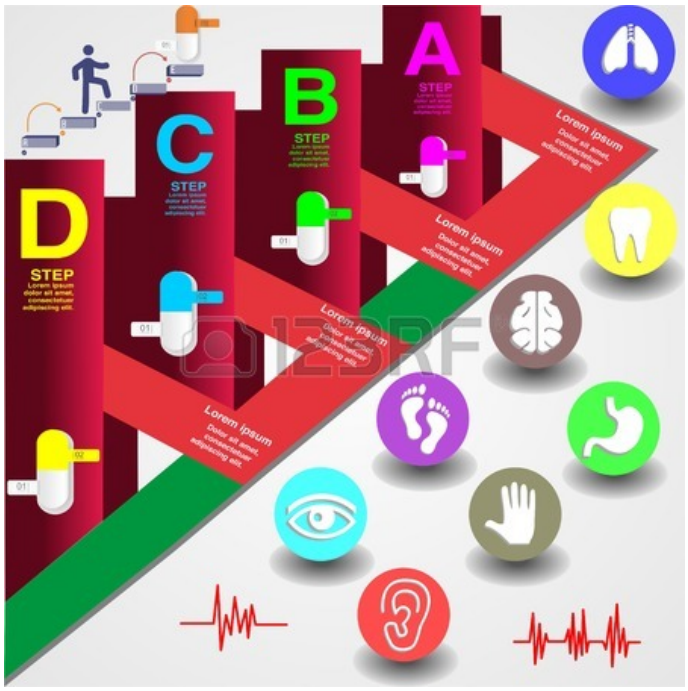
La protection des données médicales web 3.0



La protection des données médicales web 3.0

Par Murielle CAHEN – Avocat

L'avènement du web dit 3.0 laisse place à un constat évident : la quasi-totalité des objets disposent aujourd'hui d'une connexion à l'Internet. Dans cette ère du tout connecté où les flux sont incessants, une catégorie de données reste cependant sujette à une attention particulière : les données dites personnelles, regroupant en leur sein les données médicales.

Avant toute chose, il apparait plus aisé de définir plus précisément ce que l'on entend par une donnée médicale. Dans un premier temps, cette dernière n'est pas nécessairement informatique : une donnée peut en effet être archivée sous la forme d'un écrit. Il en va ainsi des certificats médicaux ou des ordonnances. Ainsi, le terme de donnée médicale englobe tout ce qui a attrait à une méthode de conservation de l'état de santé d'un patient : la question de la protection des données médicales, avec les règles de déontologie et de respect de la vie privée s'y afférant, n'est donc pas récente.

Or l'évolution fulgurante des technologies informatiques peuvent constituer un danger pour la protection des données de santé. Ainsi, ces dernières peuvent se voir perdues, corrompues, détruites voire même détournées. Ainsi, le récent cas de suicide du prévenu suspecté d'avoir volé le dossier médical de Michael Schumacher rappelle que les données médicales, du fait de leur caractère éminemment personnel, restent des données sensibles devant faire l'objet d'une protection particulière.

La France est pionnière en la matière puisqu'elle dispose de ce fait d'un régime juridique protégeant l'ensemble des données personnelles. Ce régime date de la loi du 06 janvier 1978. L'objectif principal de cette loi est d'assurer la sécurité du traitement des données à caractère personnel. Parmi ces dernières on y trouve les données médicales qui font également l'objet de dispositions particulières : le code de la santé publique protège les données médicales, et notamment leur traitement par les professionnels de santé.
Cependant, une donnée informatique est, par définition, immatérielle. Elle suppose donc une localisation sur un serveur. Hélas, dans le cas où un ressortissant français tombe malade dans un pays étranger et est soigné là bas, ses données médicales ne seront pas situés sur le territoire national. La loi française ne s'appliquant que sur le territoire français, le régime de protection des données médicales pourra se voir alors modifié, et certaines atteintes à la confidentialité de données de santé seront peut être tolérées alors qu'elles constituent une infraction au droit français. Dès lors, quelle est la réelle portée juridique de la protection des données médicales à la fois au plan national et international? L'évolution récente de certaines technologies informatiques peut elle rentrer en contradiction avec la confidentialité de données si sensibles?

I. Une protection des données médicales encadrée au plan national.
Il en va de soit, mais la France possède un régime juridique particulier sur la protection des données médicales, ce dit régime étant particulièrement efficace. De plus, la CNIL assure une surveillance particulière des dites données et elle délivre régulièrement des informations pratiques destinés à renseigner les professionnels de la santé.

A. Un cadre juridique et réglementaire efficace.
Comme dit précédemment, la France s'est dotée la première d'un régime juridique spécifique aux données personnelles et à l'utilisation des données personnelles. En effet, la loi dite Informatique et Liberté promulguée le 06 janvier 1978 a pour objet spécifique de protéger le traitement des données à caractère personnel. Comme indiqué ci-dessus, le caractère sensible de cette catégorie de données, qui permet ainsi de catégoriser les individus en fonction de leur ethnie, sexe, état de santé, etc., justifie à lui seul la mise en place d'une protection. Si cette loi s'attache à traiter de la protection de l'ensemble des données dites à caractère personnel, la loi dite « Kouchner » promulguée le 4 mars 2002 a pour objet de s'intéresser particulièrement aux données médicales. Ainsi, l'article L1111-7 du Code de la santé publique met en place pour les patients les conditions d'accès à leurs données relatives à leur santé. Lorsqu'un individu souhaite avoir accès à n'importe quel document dont le contenu est relatif à son état de santé (par exemple une feuille de consultation ou une ordonnance médicale), ce dernier peut demander directement ou par le biais d'un médecin l'accès à ce document.
Cependant, l'article L1111-8 du Code de la santé publique s'attache plus précisément à la licéité de l'hébergement et du traitement de données de santé. Ainsi, dans le cadre d'opérations de soins ou de diagnostic, les données de santé récupérées peuvent uniquement être hébergées auprès de personnes physiques ou morales qui sont agréées à cet effet. De plus, cet hébergement de donnée de santé ne peut être effectué qu'après consentement exprès de la personne concernée. Enfin, les dispositions du code de la santé publique rappellent que le traitement de telles données doivent évidemment respecter les conditions posées parla loi Informatique et Libertés. Les professionnels de la santé sont encadrés lorsqu'ils sont amenés à traiter avec des données médicales. De plus, le secret médical imposé par la déontologie des professions relatives au milieu de la santé interdit toute divulgation de donnée médicale à autrui sans accord de ce dernier ou au détriment des conditions posées par la loi.

B. Des recommandations pratiques délivrées par la CNIL.
La CNIL accorde une attention particulière à la manière dont sont effectuées des traitements de données à caractère personnel. Pour se faire, la CNIL utilise souvent des recommandations faites aux entreprises ou aux professionnels concernés afin de rappeler les pratiques idéales à effectuer suivant la situation. Dans le cas de la protection des données médicales, la CNIL s'est prononcé sur les modalités optimales à adopter dans le cas où un professionnel de santé héberge ou traite des données médicales.
La CNIL commence par rappeler la nécessité première de maintenir le degré de confidentialité des données de santé au même rang que celui du secret médical. Pour se faire, la CNIL donne des indications d'ordre technique qui, si elles peuvent paraître acquises pour de plus en plus de gens aujourd'hui au regard de l'ouverture du milieu informatique au grand public, restent nécessaires, voire indispensables dans certains cas, pour s'assurer d'un minimum de sécurité sur les données hébergées : un mot de passe doit être mis en place sur l'ordinateur et ce dernier doit faire l'objet d'un arrêt complet à chaque absence du professionnel de santé. De plus, il est recommandé par la CNIL de ne jamais faire de copie de son mot de passe pouvant être lue ou interceptée par un tiers non autorisé à accéder au système informatique. A ce titre, rappelons simplement que la simple intrusion dans un système informatique sans autorisation constitue à lui seul un délit pénal. De plus, la CNIL recommande pour le professionnel médical de disposer de supports de sauvegardes externes permettant d'éviter la perte de données.
Dans le cas où un traitement de données médicales fait l'objet d'une mise en réseau, la CNIL recommande alors une gestion plus poussée des mots de passe : ces derniers doivent être distincts suivant l'utilisateur qui utilise l'ordinateur et trois erreurs consécutives doivent, à l'instar des erreurs lors de l'entrée d'un code PIN erroné, bloquer le système. De plus, la CNIL ne recommande pas à ce qu'un compte d'un utilisateur puisse être ouvert sur plusieurs postes différents : cela signifie ainsi que le professionnel médical n'est pas présent devant l'un de ses postes, ce qui rend accessible les données à un tiers. De plus, les données médicales doivent faire l'objet d'un cryptage : c'est obligatoire pour les données personnelles. Ainsi, outre une intégrité des données qui doit constamment être vérifiée au plan informatique, la confidentialité de ces dernières doit être assurée par un chiffrement total ou partiel des données nominatives en fonction des cas. Enfin, dans le cas où l'accès au réseau se fait via Internet, un système de pare-feu est hautement recommandé pour prévenir de toute tentative d'interception des données médicales lorsque ces dernières font l'objet d'un flux.

II. Une protection des données médicales incertaine au plan international.
La loi française n'est applicable en France, et certaines législations internationales semblent ne pas accorder autant d'importance à la protection des données personnelles. De plus, l'ouverture des réseaux au monde entier amène à un risque : le législateur n'a pas le temps d'adapter la loi à la technique informatique.

A. Une absence de concertation internationale préjudiciable.
Avant toute chose, il est à noter que la majorité des autres états étrangers n'adopte pas de position hostile par rapport à la protection des données personnelles, bien au contraire. Ainsi, concernant les états européens, la plupart de ces derniers ont adopté une CNIL (ou un équivalent) permettant ainsi une certaine uniformisation de la protection des données personnelles, et donc par ce biais des données médicales. De plus, lorsqu'un traitement de données personnelles d'un citoyen français doit être effectué dans un pays étranger, un accord de la CNIL est obligatoire. Il existe ainsi des cas de figure où des données médicales d'un ressortissant français peuvent être amenées à être traitées dans un pays étranger à l'européenne.
L'exemple des États-Unis constitue peut-être le meilleur exemple de risque potentiel d'atteinte à la protection des données médicales d'un citoyen français. Prenons le cas où lors du séjour d'un français aux États-Unis, ce dernier doit subir une hospitalisation imprévue dans un établissement de santé américain. Théoriquement, et dans la grande majorité des cas, les données médicales des patients français n'ont aucune raison d'être détournées de leur utilisation. Or il existe un principe en droit américain nommé le « Patriot Act ». Ce dernier permet au gouvernement américain de disposer librement des données personnelles d'un individu sur le fondement d'une seule suspicion de terrorisme ou d'espionnage. Si l'existence d'un tel principe est hautement compréhensible au regard de l'importance accordée par le gouvernement américain à tout ce qui concerne la sécurité nationale, le fondement d'une seule suspicion sans autre preuve apparait bien léger pour assurer une protection des données médicales. De plus, la cybercriminalité est un rempart à une bonne protection des données médicales lorsque des pare-feu ne sont pas suffisamment élaborés pour prévenir de telles attaque. Ainsi, entre les mois d'avril et juin 2014, Community Health Systems, un spécialiste de la gestion d'hôpitaux américains, a subi des cyber-attaques qui ont subtilisé plusieurs millions de données personnelles. S'il n'est fait état d'aucune subtilisation de données médicales au sein des données volées, cette possibilité relance la nécessité d'une protection informatique nécessaire pour se prémunir de ce genre de piratage.

B. Un état technique avancé, ou le risque d'un retard juridique.
Aujourd'hui, il apparait pratiquement impossible de faire disparaitre la carte vitale du système médical français : la gestion des données de santé apparait bien trop longue au regard du nombre de patients à gérer. A ce titre, l'évolution informatique mêlée à des impératifs de gestion médicale ne pose pas de problème juridique en soit. Toutefois, des technologies nouvelles ne sont pas encore appréhendées parla loi. Il en va par exemple du Cloud computing : aucun stockage physique n'est effectué sur le disque dur de l'ordinateur et tout se retrouve localisé dans des datacenters qui peuvent être localisés dans des pays étrangers. Certaines entreprises louent d'ailleurs des services de cloud à des professionnels. Or dans le cas où un professionnel médical stockerait des données de santé de cette manière, outre un accord de la CNIL nécessaire, que se passe-t-il dans le cas où un patient souhaite avoir accès à ses données de santé ? De plus, lorsque des données, notamment personnelles, se retrouve massivement stockées en un point physique fixe, les risques de cyber-attaques se retrouvent augmentées. En 2009, le gouvernement français avait élaboré le projet « Andromède » qui prévoit de stocker sous la forme d'un « cloud souverain » les données nationales du gouvernement, de son administration et d'autres entreprises. Ce projet permettrait ainsi d'alléger considérablement les risques associées à une « volatilité » des données que l'on peut constater aujourd'hui. En effet, ces dernières se retrouveraient toutes sous l'égide de la loi française, aucun problème de localisation des serveurs ne pourrait être relevé et le travail de surveillance de la CNIL serait considérablement allégé. Pour autant, si les données médicales ne semblent pas faire l'objet d'un stockage massif dans des serveurs cloud étrangers, la question mérite néanmoins réflexion en ce que les dispositions relatives au bon traitement des données médicales par le droit français se voit d'un coup quasiment réduites à néant. Enfin, une législation numérique européenne serait la bienvenue puisque les données médicales se verraient enfin asservies à un régime juridique dans l'ensemble de l'Europe.
Par Me Murielle CAHEN
Sources :
http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/un-imperatif-la-securite/

http://www.ordre.pharmacien.fr/content/download/123311/645012/version/1/file/J23-Dossier-CommentGarantirSecuriteDonneesSante.pdf

http://www.ordre.pharmacien.fr/Le-patient/La-protection-des-donnees-de-sante

http://www.linformaticien.com/actualites/id/33884/4-5-millions-de-donnees-medicales-derobees-aux-etats-unis.aspx

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.juritravail.com/Actualite/fichiers-libertas/Id/176621
Par Murielle CAHEN – Avocat