



PRINTEMPS 2016 - N°28

LE BIG DATA A L'ASSAUT DE LA SANTE ?

Éditorial

Nouveau cycle

par Michel Rouger, président de l'institut Presaje

En terminant mon hommage à l'équipe de rédaction de nos 80 lettres publiées entre 2002 et 2015 - 53 sous forme papier, 27 sous forme électronique - j'ai annoncé dans notre dernière édition de Presaje.Com un nouveau cycle de publications pour 2016.

[lire la suite page 3]

Vers une dictature scientifique des données personnelles

par Christiane FÉRAL-SCHUHL, avocat associé au barreau de Paris, ancien bâtonnier de Paris

Adélaïde a 35 ans... Elle adore les "applis" mobiles dédiées à la santé et au bien-être. Elle utilise une balance digitale, un tensiomètre, une montre connectée et une variété d'autres capteurs reliés à des cabinets médicaux, des entreprises, des laboratoires ou des organisations quelque part en Europe ou dans le monde. Christiane Féral-Schuhl part d'un exemple fictif pour décrire le basculement très concret de nos contemporains "branchés" dans un monde peu soucieux de la protection de la sphère intime des individus.

[lire la suite page 3]

Transparence, qualité de l'information, protection des données privées : l'action de l'Union européenne

Par Bruno GENCARELLI, chef d'unité « Protection des personnelles » à la Commission

En 2012, la Commission européenne a présenté un projet de réforme de la protection des données personnelles. Que s'est-il passé depuis lors ? Pour

Santé et vie privée à l'heure de l'invasion du numérique planétaire

par Thomas CASSUTO, magistrat, docteur en droit

Comment trouver le bon équilibre entre la recherche du progrès pour tous - que facilite le numérique - et la protection de notre vie privée ? L'Institut Presaje avait organisé en septembre 2015 un colloque avec France Amérique et l'Association française des docteurs en droit sur les conséquences du basculement général des données personnelles dans la fournaise mondiale. Ce numéro de Presaje.Com est consacré aux temps forts des débats animés par Thomas Cassuto.

[lire la suite page 11]

Qui sera le gardien de notre vie intime ?

Par Pascal DURAND, député européen

Autrefois, le patient venait consulter le médecin quand il se sentait mal. Aujourd'hui, on passe d'une logique de la demande à une logique de l'offre. Il circule sur notre planète autant de données électroniques que d'étoiles dans l'univers. Qui organise, qui contrôle, qui finance le traitement des données de santé ? Pour Pascal Durand, qui plaide pour un retour au droit "dur", le Big data pose aussi un problème de souveraineté aux Etats et à l'Europe.

[lire la suite page 12]

Les droits individuels reconfigurés par le Big data

Par Alain-Michel CERETTI, représentant le Défenseur des droits, conseiller droit des maladies du pôle santé

Les questions de santé font partie des

Bruno Gencarelli, l'un des porteurs du projet et négociateur de l'accord de 2015 conclu avec les Etats-Unis, le droit de la protection des données personnelles et plus largement de la vie privée a désormais atteint sa maturité.

[lire la suite page 7]

L'accès aux données personnelles, l'exemple du dossier médical numérique

Par Marjorie OBADIA, procureur adjoint près le TGI de Versailles, ancienne directrice adjointe à la Direction des affaires juridiques AP-HP

La France dispose d'un solide arsenal de protection des données de santé à caractère personnel explique Marjorie Obadia qui a eu l'occasion d'aborder la question des droits des patients et des professionnels de santé à la direction des affaires juridiques de l'Assistance Publique - Hôpitaux de Paris.

[lire la suite page 9]

préoccupations du Défenseur des droits. Le témoignage d'Alain-Michel Ceretti est doublement instructif. A titre professionnel, il dirige une entreprise d'électronique et à titre personnel, son épouse ayant contracté une infection nosocomiale, il a fondé avec elle une association, *Le Lien*, destinée à défendre le droit des malades. C'est ce qui l'a conduit à occuper des fonctions auprès des médiateurs de la République.

[lire la suite page 13]

De l'aide au diagnostic à la révolution du Big data individuel

par Philippe Rouger, European Institute for Systems Biology & Medicine.

Volume, variété, vitesse. La règle des trois V appliquée depuis longtemps aux données de la météorologie, de la finance ou du marketing s'impose désormais dans l'univers de la santé, ouvrant des brèches dans l'espace de vie intime des individus. Mais, explique Philippe Rouger, le Big data n'est que l'une des composantes technologiques de la révolution à venir dans la médecine.

[lire la suite page 16]

Editorial

Nouveau cycle

Par Michel Rouger, président de l'Institut Presaje

En terminant mon hommage à l'équipe de rédaction de nos 80 lettres publiées entre 2002 et 2015 53 sous forme papier, 27 sous forme électronique j'ai annoncé dans notre dernière édition de Presaje.Com un nouveau cycle de publications pour 2016.

Il se met en place avec la lettre numéro 28, réalisée par une nouvelle équipe issue de notre conseil d'administration. Jacques BARRAUX assure la continuité de la rédaction avec Isabelle PROUST et Philippe ROUGER, président des Editions PREMICES en charge de la diffusion de nos publications. Xavier LAGARDE, vice-président de PRESAJE, devient président de ses publications.

Sur le fond, les contenus publiés respecteront les spécialités reconnues comme étant la marque de notre Institut, la Justice, le Droit, l'Economie, la Finance et le Sport. Cette lettre, comme la précédente, traite d'un autre sujet, majeur dans la période que nous vivons, celui de la Santé. Si l'explosion des banques de données gérées par des sociétés américaines vient bouleverser les activités des êtres humains, dans la Santé elles attaquent leurs personnes physiologiques, psychologiques et leur identité génétique.

Pour comprendre ces bouleversements il suffit de faire référence au décryptage du fonctionnement d'une cellule cancéreuse qui ouvrirait la voie à un traitement de ce fléau. Les bases de données actuelles, les moyens de calcul qu'elles offrent, permettront rapidement de traiter les centaines de milliards d'informations utiles pour comprendre les dérèglements d'une seule cellule cancéreuse. À quel prix ? Pour qui ?

Le débat est ouvert dans la communauté scientifique médicale, laquelle, faute de disposer aujourd'hui des moyens de stockage de données et de calculs, reste dépendante des traitements médicamenteux ou chirurgicaux qui ont permis de sérieuses avancées sur cette horrible maladie. A nouveau, à quel prix et pour qui ?

La compétition sera vite ouverte entre deux modes de traitement, qui pourrait en révéler un troisième qui s'écarterait aussi bien des Big data que des Big pharma. Il faudra du temps. C'est pourquoi PRESAJE veut sensibiliser son lectorat sur un sujet qui occupera les prochaines décennies. C'est aussi pourquoi, à raison du poids des images dans la pédagogie de notre époque vous retrouverez l'esprit de nos lettres sous la forme d'images vidéo diffusées sur le site TV duquel PRESAJE a choisi d'être partenaire.

Vers une dictature scientifique des données personnelles ?

Par Christiane FÉRAL-SCHUHL, avocat associé au barreau de Paris, ancien bâtonnier de Paris

Adélaïde a 35 ans... Elle adore les "applis" mobiles dédiées à la santé et au bien-être. Elle utilise une balance digitale, un tensiomètre, une montre connectée et une variété d'autres capteurs reliés à des cabinets médicaux, des entreprises, des laboratoires ou des organisations quelque part en Europe ou dans le monde. Christiane Féral-Schuhl part d'un exemple fictif pour décrire le basculement très concret de nos contemporains "branchés" dans un monde peu soucieux de la protection de la sphère intime des individus.

Il y a trente ans déjà, une petite association, l'AMII (Association médicale d'informatique individuelle), se réunissait au sous-sol du siège de l'Ordre des médecins, dans le 7^{ème} arrondissement. Ses membres, des médecins passionnés d'informatique, réfléchissaient aux

questions liées à l'utilisation des technologies dans leur exercice professionnel, notamment avec la mise en place annoncée de la carte vitale.

J'avais été invitée à participer à certains de leurs débats et je me souviens que, dès cette époque, la question centrale était de savoir à qui appartenait les données de santé. En effet, tous les professionnels intervenant auprès du patient (médecin, infirmière, garde-malade...) n'y avaient pas le même accès. Quid dans ce contexte du secret professionnel ? Plus largement, des règles d'éthique ?

En trente ans, beaucoup de choses se sont passées, en particulier le clonage de la brebis Dolly, et le *Meilleur des mondes* décrit par Aldous Huxley n'est plus de la science-fiction.

Pour répondre à la question posée « vers une dictature scientifique des données personnelles ? », je vous propose de vous présenter une jeune femme que nous appellerons Adélaïde.

L'exemple d'Adélaïde

Agée de 35 ans, Adélaïde est cadre supérieur dans une banque, « pacsée » et mère de deux enfants. Elle a pris l'habitude d'utiliser une balance digitale, un tensiomètre, une montre connectée, des lentilles spéciales qui lui permettent de surveiller son taux de glycémie car elle a été alertée sur les risques de diabète, etc.

Ces différents objets connectés lui permettent de collecter en continu des informations sur son corps et sur son cerveau : poids, calories absorbées et dépensées, température, pression artérielle, souffle, clignements de paupières, variations d'humeur, bâillements... Vous l'avez compris, elle est totalement fan des appli mobiles dédiées à la santé et au bien-être et elle n'a que l'embarras du choix avec plus de 100 000 applications téléchargeables ! Elle s'est même équipée d'un fauteuil « intelligent » qui lui permet d'évaluer en moins de 10 minutes son état de santé, y compris son acuité visuelle et auditive. Son plateau-repas, après son footing, sera programmé pour tenir compte de toutes ces données. Son coach l'accompagne efficacement à distance car il peut analyser les données et ainsi l'aider à atteindre son objectif : perdre trois kilos. Il peut ajuster son régime et son programme sportif au jour le jour.

Ces données sont également télétransmises à une startup américaine, Flatiron Health, qui a pour mission de dépister les éventuels cancers, ainsi qu'à Diabéo, une filiale de Sanofi qui suit l'évolution du taux de glucose dans le sang des patients diabétiques. L'Hôpital américain, également destinataire, est équipé du supercalculateur Watson qui gère son dossier médical, régulièrement mis à jour par les praticiens ayant l'occasion d'examiner Adélaïde. Ce dossier comprend aussi les résultats de toutes les analyses qu'elle a effectuées depuis sa naissance ainsi que les antécédents médicaux familiaux.

Ces informations sont par ailleurs transmises aux services de l'Assurance maladie, qui peut ainsi vérifier qu'Adélaïde prend bien les traitements qui lui sont prescrits, sans oublier son courtier d'assurance santé, qui est parvenu à lui obtenir des réductions sur ses primes d'assurance car il a démontré qu'elle suit un régime strict et applique des règles d'hygiène irréprochables.

Le cabinet d'audit M. est également destinataire de ces données car Adélaïde a été sélectionnée parmi d'autres volontaires pour participer à des essais cliniques qui lui permettront d'obtenir des points de fidélité.

Enfin, le médecin d'Adélaïde est au cœur du dispositif. Il peut ainsi contrôler les éventuels effets secondaires des médicaments en suivant à distance, au moyen d'un algorithme, les douleurs qu'elle ressent de manière aléatoire sur le côté droit et qu'elle lui a signalées. Lorsqu'elles se

produisent, elles provoquent une alerte graduée, en fonction de l'importance de la douleur, sur son ordinateur. Adélaïde n'a pas besoin de se préoccuper de quoi que ce soit : tous ces capteurs travaillent pour elle et son coach numérique, doublé d'un agenda électronique, lui dit, à la seconde près, quelle conduite elle doit tenir. Son alimentation est automatiquement programmée en tenant compte de ses goûts, de ses allergies et de ses intolérances.

Dernier détail : son compte Facebook lui envoie des alertes sur l'état de santé de ses amis, ce qui lui permet d'éviter de rencontrer ceux d'entre eux qui sont enrhumés ou grippés !

Cette description n'est pas futuriste : tous les dispositifs évoqués existent d'ores et déjà, en 2015. Non seulement ils permettent à Adélaïde de conserver une bonne santé, mais celle-ci peut légitimement penser qu'elle participe au bien collectif.

Elle pourra vous expliquer que l'analyse de ces données, avec celle de millions d'autres, permettront de réduire la mortalité (certaines applications permettent de prévoir la diffusion des épidémies à partir des données ou de dépister des maladies par la génétique), de prévenir un risque de maladie à partir du génome (médecine prédictive), notamment les pathologies chroniques dont les paramètres sont bien identifiés et reliés à des mécanismes physiologiques clairs (par exemple pour suivre l'évolution du taux de glucose dans le sang et partager les données par smartphone vers le médecin). Elle vous dira que cela permet d'adapter les traitements à certains types de patients, en fonction de leur profil génétique (médecine personnalisée) et d'aider les professionnels à poser des diagnostics ou faire un choix de traitement pour les patients, de vérifier les effets secondaires des médicaments pour mieux les prévenir, par exemple en croisant les données enregistrées par l'assurance maladie, on pourrait observer le taux d'hospitalisation des patients prenant tel ou tel médicament (pharmacovigilance)...

Des données sensibles

Ces données, recueillies à la fois à l'occasion des diverses activités d'Adélaïde et lors des examens médicaux qu'elle subit, sont toutefois considérées comme *sensibles* car elles révèlent toutes les fragilités de cette jeune femme, par exemple sa vulnérabilité au stress ou aux épidémies, ou encore ses risques cardio-vasculaires.

En fait, il s'agit de données « ultra » sensibles qui touchent à la sphère s'agit de données que, parfois, l'on ne partage même pas avec ses proches les plus intimes.

Ces données sont d'autant plus sensibles qu'elles ne désignent pas forcément un comportement actif, qui pourrait être contrôlé, mais des caractéristiques propres à une personne.

On touche à ce que le professeur Gérard Cornu appelle, « *la sphère d'intimité chacun* ». ».

Rappelons ce qu'écrivait le professeur Jean Carbonnier à cet égard : « *Il sied d'accorder à l'individu une sphère secrète de vie d'où il aura le pouvoir d'écarter les tiers*. » »

Un consentement et une sécurité renforcés pour l'individu

D'où l'importance, dès qu'il s'agit des données de santé de l'individu, de renforcer le principe de l'autodétermination informationnelle, c'est-à-dire la possibilité pour chacun de décider de communiquer ou de ne pas communiquer ses données.

D'où l'importance également de renforcer la sécurité des données de santé. C'est dans cet objectif que le législateur a exigé que l'hébergement informatique des données médicales soit assuré par

un hébergeur agréé (Agence des systèmes d'informations partagées de santé - ASIP santé), garantissant de hauts niveaux de sécurité, et a fixé des règles de sécurité et de confidentialité pour tous les établissements de santé : exigence d'anonymat, chiffrement des données, recours au codage des données nominatives, etc.

Un sentiment trompeur de sécurité

À la question posée « *Allons-nous vers une dictature scientifique des personelles ?* », il est probable qu'Adélaïde répondrait par la négative : « *Ce n'est pas une dictature. Je maîtrise la situation, j'améliore mon bien-être, je vais peut-être réussir à me débarrasser de ces trois kilos qui me pourrissent la vie, je suis autonome dans la gestion de ma santé.* »

Adélaïde ignore probablement que toutes ces données sont collectées à son insu via les historiques de navigation sur les moteurs de recherche, les blogs, les sites, et qu'il est désormais possible d'analyser les conversations sur Facebook : 51 % d'entre elles porteraient sur des questions de santé, permettant d'alerter sur l'état contagieux de ses « amis » !

Elle ne sait sans doute pas que ces données sont croisées, reformatées, optimisées, exploitées également à son insu, vendues à prix d'or.

Elle ignore que même les bases de données publiques anonymisées peuvent permettre une identification indirecte des personnes, car celles-ci sont toujours désignées par un même numéro d'anonymat.

Elle n'imagine pas que les algorithmes utilisés pour optimiser le fonctionnement d'un certain nombre de services présentent le risque « d'enfermement de l'internaute dans une personnalisation dont il n'est pas maître. »¹, ni même qu'ils sont faillibles et qu'ils peuvent provoquer une erreur, par exemple à la suite d'un bug dans un logiciel d'aide au diagnostic. Le patient risque de se trouver enfermé dans une situation dont, loin de la maîtriser, il lui sera très difficile de sortir.

Enfin, elle ne sait pas que ces données pourraient tomber entre les mains de personnes non autorisées. Par exemple un employeur éventuel qui n'a aucune envie de recruter une personne qui risque d'être malade un jour sur deux. La capacité de travail ou la résistance au stress pourraient devenir des critères de sélection.

De leur côté, les compagnies d'assurance pourraient envisager de proposer des offres plus onéreuses à des personnes en situation de maladie, de faiblesse ou de vulnérabilité, ou encore présentant des antécédents familiaux. Les banques pourraient sélectionner les dossiers de prêts.

Le responsable du service de bioéthique de l'UNESCO m'expliquait il y a déjà quelques années que les maladies génétiques peuvent désormais être anticipées au moins deux générations à l'avance...

Adélaïde croit qu'elle reste libre, à tout moment, de collecter et de communiquer ou non ces données. Elle ne se rend pas compte qu'un jour, peut-être, ceux qui refuseront de le faire seront considérés comme ayant quelque chose à cacher.

« La vie privée, un problème de vieux cons ? »

D'ores et déjà, 7 millions de Français ont été séduits par la santé connectée et, d'après Mark Zuckerberg, le fondateur de Facebook, on assiste à l'émergence d'une nouvelle norme sociale à ce sujet : « *Les gens sont désormais très à l'aise avec l'idée de partager davantage d'informations,*

de manière plus ouverte et avec davantage d'internautes. » Certains considèrent même que le débat sur la vie privée est complètement dépassé, à l'instar de son ouvrage « La vie privée, un problème de vieux cons ? ».

Je reste également convaincue que c'est à l'individu et à nul autre de choisir ce qu'il rend public ou non. A lui et à lui seul de décider si, comme le suggère Stefan Zweig « seule l'illusion rend heureux, non le savoir », ou si, selon la vision de Rousseau, « le monde de l'illusion vaut mieux que la réalité car nous y trouvons plus de plaisir ».

S'il est parfois préférable de ne pas savoir, à tout le moins, posons en règle que c'est toujours à l'individu de choisir !

¹ Rapport Conseil d'Etat 2014

Transparence, qualité de l'information, protection des données privées : l'action de l'Union européenne

Par Bruno GENCARELLI, chef d'unité « Protection des personnelles » à la Commission

En 2012, la Commission européenne a présenté un projet de réforme de la protection des données personnelles. Que s'est-il passé depuis lors ? Pour Bruno Gencarelli, l'un des porteurs du projet et négociateur de l'accord de 2015 conclu avec les Etats-Unis, le droit de la protection des données personnelles et plus largement de la vie privée a désormais atteint sa maturité.

Le droit de la protection des données personnelles, et plus largement de la vie privée, a fait l'objet d'une constitutionnalisation à travers la Charte des droits fondamentaux, dont l'article 8 est désormais contraignant. Il a également trouvé une base juridique spécifique dans le Traité européen, qui permet à l'Union européenne de légiférer en la matière, et du reste un très important paquet législatif est actuellement en cours de négociation. Enfin, le droit de la protection des données personnelles fait l'objet d'une jurisprudence abondante et particulièrement protectrice à la Cour de justice, que ce soit à propos du rôle des autorités de contrôle indépendantes (les CNIL), du droit des individus et en particulier du droit à l'oubli, ou encore de la prise en compte de la protection des données dans les domaines sensibles comme la prévention et la répression des infractions pénales.

La matière première de l'économie numérique

Ces évolutions juridiques n'ont fait qu'accompagner l'ampleur prise par la collecte, le traitement et le partage des données à caractère personnel, qui sont devenues la véritable matière première de l'économie numérique. Ces données irriguent la recherche et constituent désormais un aspect essentiel de très nombreuses activités.

Une nouvelle pertinence pour la protection des données personnelles

La question de la protection des données met en évidence un paradoxe.

Alors qu'on parle d'étanchéité pour des données dites sensibles ou ultra-sensibles les données de santé, on s'aperçoit que les données en question peuvent être agrégées et combinées avec d'autres : les frontières tombent. On observe également que des notions comme le principe de finalité sont brouillées : il devient difficile d'anticiper quel usage sera fait des informations recueillies.

L'émergence du *Big data* a ainsi paradoxalement pour effet de conférer une nouvelle pertinence à la notion de protection des données privées, alors que cette notion pouvait paraître dépassée et, si j'ai bien compris, réservée aux « *vieux cons* »

Vers de nouvelles avancées législatives ?

La nécessité de protéger la vie privée est déjà prise en compte dans le droit national, depuis la loi Informatique et liberté de 1978, et dans le droit européen, depuis la directive de 1995.

Nous nous efforçons maintenant d'obtenir de nouvelles avancées. Le consentement à la communication des données devrait être explicite. La qualité de l'information fournie pourrait être meilleure, et les pages en petits caractères, que personne ne lit, pourraient être remplacées par des icônes ou par des symboles graphiques. Les finalités du traitement des données devraient être spécifiées. Le droit applicable devrait être clairement déterminé : dès qu'il y a ciblage d'un utilisateur européen et/ou fourniture d'un service, le droit européen devrait s'appliquer, indépendamment de la localisation de la société. La question des transferts internationaux devrait également être clarifiée, sachant que, le plus souvent, les données recueillies traversent l'Atlantique. Nous travaillons aussi sur les questions de discrimination, notamment à propos des profils de santé qui pourraient constituer une barrière à l'embauche.

La réforme du cadre législatif en matière de protection des données est en voie d'adoption. Elle en est actuellement à la phase des *trilogues*, c'est-à-dire de la négociation finale entre les trois institutions, Parlement, Conseil et Commission. Le nouveau cadre législatif comportera trois grands axes.

Rationalisation et simplification

Le premier concerne la rationalisation et la simplification du cadre réglementaire en matière de protection des données. L'adoption d'un règlement au lieu d'une directive permettra de mettre fin à la fragmentation des droits nationaux, dans une matière qui est par définition transfrontalière.

La simplification se traduira par la suppression de nombreuses obligations de notification d'autorisations préalables, qui se sont avérées peu efficaces en matière de protection des données. On passera d'un système *ex ante* à un système *ex post*, avec des mécanismes internes de contrôle (évaluation d'impact, obligation de documentation...) et des mécanismes externes, comportant notamment la possibilité de sanctions financières crédibles.

Cette démarche de simplification et d'harmonisation, qui traverse l'ensemble du texte, se heurte à certaines limites, notamment dans le domaine qui nous intéresse aujourd'hui, celui de la santé. C'est en effet un domaine où les compétences de l'Union européenne sont limitées et où les États membres sont soucieux de préserver certains particularismes nationaux.

Notre proposition prévoyait, par exemple, l'adoption de mesures communes de réduction des risques, comme le recours à la pseudonymisation, mais les résistances des États membres se sont avérées relativement fortes en la matière.

Renforcement des droits des individus

Le deuxième axe est le renforcement et la mise à jour des droits des individus. À partir du socle que constituent le droit national, le droit européen de 1995 et les droits tels que l'accès à l'information et à sa rectification, nous proposons d'introduire des droits nouveaux tels que le droit à la portabilité des données. Un individu devrait pouvoir faire déplacer ses données d'un

fournisseur de services à un autre, ce qui lui permettrait de choisir celui qui lui apporte davantage de garanties en matière de protection et de sécurité des données. La concurrence serait ainsi renforcée et les barrières à l'entrée abaissées.

La mise en œuvre du droit

Le troisième axe est celui de la mise en œuvre du droit. En 2014, on a constaté une augmentation de 50 % des incidents de sécurité. Compte tenu de la valeur des données personnelles, les conséquences de ces incidents sont de plus en plus sérieuses, et ce risque concerne aussi bien le secteur privé que le secteur public.

Or, il ne peut pas y avoir de règle de droit crédible s'il n'existe pas de sanction crédible attachée à sa violation. C'est pourquoi nous proposons de permettre aux CNIL européennes d'imposer des sanctions financières proportionnelles au poids des entreprises en cause, c'est-à-dire calculées par rapport à leur chiffre d'affaires.

Au-delà de ce système de sanction, nous proposons un véritable changement de gouvernance en matière de protection des données. Aujourd'hui, chaque CNIL agit sur son propre territoire, alors que les affaires dont nous parlons sont transfrontalières et ont un impact pour l'ensemble des citoyens européens ou pour une grande partie d'entre nous.

C'est pourquoi nous proposons la création d'un guichet unique pour les recours. L'instruction des dossiers serait assurée par l'une des autorités nationales qui devrait décider des mesures à prendre avec les autres autorités concernées. Il ne s'agirait pas de créer une super autorité européenne mais bien un système reposant sur la mise en réseau des CNIL européennes et sur leur collaboration.

L'accès aux données personnelles, l'exemple du dossier médical numérique

Par Marjorie OBADIA, procureur adjoint près le TGI de Versailles, ancienne directrice adjointe à la Direction des affaires juridiques AP-HP

La France dispose d'un solide arsenal de protection des données de santé à caractère personnel explique Marjorie Obadia qui a eu l'occasion d'aborder la question des droits des patients et des professionnels de santé à la direction des affaires juridiques de l'Assistance Publique – Hôpitaux de Paris.

D'après l'article 2 de la loi Informatique et liberté de 1978, texte particulièrement protecteur, une « donnée à caractère personnel » se définit comme « toute information relative à une personne physique identifiée ou qui peut être identifiée, par un référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ».

Quant aux « données de santé à caractère personnel », elles recouvrent bien plus données liées à la personne physique elle-même. Selon le projet de Règlement européen relatif aux données personnelles, il s'agit de « toute information relative à la santé physique ou mentale d'une personne, ou à la prestation de services de santé à cette personne ».

La loi Informatique et liberté interdit la collecte et le traitement des données personnelles concernant les origines raciale ou ethnique, les opinions politiques, syndicales, philosophiques et religieuses des personnes, mais également les données concernant la santé et tout particulièrement la vie sexuelle, à l'exception « des traitements nécessaires aux fins de la

médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou à la gestion des services de santé, et mis en œuvre par un membre d'une profession de santé ».

Les droits du patient

Depuis la loi Kouchner de 2002, le patient a un droit d'accès aux données le concernant, et en particulier au dossier médical constitué par les établissements publics de santé comme ceux de l'AP-HP. Il s'agit aussi bien du dossier médical papier, comprenant les comptes-rendus d'hospitalisation et de consultation, les examens de laboratoire, ou encore l'imagerie médicale, que du dossier informatique ou informatisé.

L'établissement de santé est le gardien et non le propriétaire de ces données. Il doit en assurer la bonne tenue et la communication au patient, ce qui pose souvent des problèmes très concrets d'extraction de données issues de systèmes d'information et de répertoires très divers en fonction des services et des spécialités présents au sein d'un même hôpital. Le dossier en question doit être exhaustif et la jurisprudence de la CNIL en excepte uniquement les notes personnelles du médecin.

Le dossier médical étant considéré comme un document administratif, il existe une jurisprudence parallèle, celle de la CADA (Commission d'accès aux documents administratifs). L'approche de la CADA est sans doute moins protectrice du patient que celle de la CNIL, qui s'efforce souvent de prémunir le patient contre lui-même. À un établissement de santé qui se demandait s'il avait le droit de communiquer à un patient son dossier médical à travers une simple adresse mail, comme celui-ci l'exigeait, la CADA a répondu que le patient était un adulte censé mesurer les risques qu'il prenait pour lui-même ou pour autrui et en assumer la responsabilité.

En ce qui concerne le dossier médical informatisé, l'article 39 de la loi de 1978, rappelé à l'article 43 du même texte, prévoit que le patient a le droit de demander la rectification, le complément ou l'effacement de certaines mentions « *pour un motif légitime* ». La jurisprudence est toutefois assez restrictive sur cette notion de « *motif légitime* ». Le patient a également le droit de s'opposer à ce que les données à caractère personnel le concernant fassent l'objet d'une collecte ou d'un traitement, sauf si ce traitement répond à une obligation légale ou si ce droit est expressément écarté par la disposition spéciale de la CNIL qui a autorisé le traitement en question. En vertu des articles 25 et 26 de la loi de 1978, la CNIL jouit ainsi d'une prérogative que ses détracteurs jugent abusive sur le traitement et la conservation des données dites sensibles, en particulier toutes les données qui pourraient être visées par l'interdiction concernant la vie privée, les origines raciales ou les mœurs figurant à l'article 8.

Enfin, le patient a droit à une information a priori et systématique sur son droit d'accès aux données le concernant et de rectification de ces données, ainsi que sur les droits généraux liés à la personne.

Les droits des professionnels de santé

La loi Informatique et liberté pose que l'ensemble des données médicales liées au parcours de santé du patient dans l'établissement doivent être accessibles, dans son intérêt, à tous les professionnels de santé qui le prennent en charge.

Le Code de la Santé publique définit l'équipe de soin de façon très restrictive : il s'agit des professionnels de santé directement concernés par la prise en charge médicale du patient. L'article 25 du projet de loi Santé marque à cet égard une ouverture, puisque l'équipe médicale serait élargie à l'ensemble des professionnels participant directement ou indirectement aux actes de

diagnostic et aux actes thérapeutiques, de compensation du handicap ou de prévention de la perte d'autonomie, c'est-à-dire à la sphère non seulement médicale mais médico-sociale et sociale.

Le consentement du patient ne serait requis que pour des personnes extérieures à cette équipe de soin entendue au sens large.

Les droits des chercheurs

Je n'ai pas le temps de développer beaucoup le dernier point, sur l'accès aux données personnelles au titre de la recherche et des études sur les politiques de santé publique.

Nous devons être attentifs à l'article 43 du projet de loi de Marisol Touraine qui prévoit que les chercheurs puissent avoir accès non seulement à la base de données SNIIRAM mais à la base PMSI (Programme de médicalisation des systèmes d'information) et à d'autres bases nationales.

Santé et vie privée à l'heure de l'invasion du numérique planétaire

par Thomas CASSUTO, magistrat, docteur en droit

Comment trouver le bon équilibre entre la recherche du progrès pour tous – que facilite le numérique - et la protection de notre vie privée ? L'Institut Presaje avait organisé en septembre 2015 un colloque avec France Amérique et l'Association française des docteurs en droit sur les conséquences du basculement général des données personnelles dans la fournaise mondiale. Ce numéro de Presaje.Com est consacré aux temps forts des débats animés par Thomas Cassuto.

Mon smartphone est doté d'une application grâce à laquelle il me suffit de poser mon pouce sur l'écran pour connaître ma pression artérielle. Je constate que celle-ci est actuellement de 115 sur 73 et ce résultat vient probablement d'être envoyé aux quatre coins du monde. Sans doute vais-je recevoir prochainement des incitations à adopter un nouveau régime alimentaire ou à acheter des produits susceptibles d'améliorer mon fonctionnement cardio-vasculaire.

Lorsque j'ai téléchargé ce logiciel, j'ai vraisemblablement accepté des conditions générales dont je n'ai compris ni le sens ni la portée. En particulier, je n'ai pas de certitude sur la juridiction à laquelle je devrais faire appel si cette application me donnait des informations erronées et si, par exemple, elle me laissait penser que je suis en bonne santé alors que je suis malade.

Autre exemple de l'arrivée du *Big data* dans le domaine de la santé : depuis 2008, moteur de recherche Google se dit capable de prévoir l'apparition des épidémies de grippe avec dix à quinze jours d'avance sur les organismes de veille sanitaire, simplement en dénombant les requêtes formulées sur ce thème. Des données personnelles peuvent donc être recueillies même sans passer par une application telle que celle que j'ai installée sur mon smartphone.

Ne peut-on craindre que toutes ces données parviennent un jour chez nos assureurs et que ceux-ci, lorsqu'ils constateront que nous ne sommes pas en bonne santé, s'opposent à nos demandes de crédit ou nous imposent des surprimes ?

Qui sera le gardien de notre vie intime ?

Par Pascal DURAND, député européen

Autrefois, le patient venait consulter le médecin quand il se sentait mal. Aujourd'hui, on passe d'une logique de la demande à une logique de l'offre. Il circule sur notre planète autant de données électroniques que d'étoiles dans l'univers. Qui organise, qui contrôle, qui finance le traitement des données de santé ? Pour Pascal Durand, qui plaide pour un retour au droit "dur", le Big data pose aussi un problème de souveraineté aux États et à l'Europe.

Au cours de l'Antiquité, un basculement s'est opéré entre le monde des Grecs, qui terminaient leurs lettres par « *Sois heureux* », et celui des Romains, qui les concluaient par « *Porte-toi bien* ». On est passé du souhait d'une vie harmonieuse à une préoccupation centrée sur le *mens sana in corpore sano*. Aujourd'hui, non seulement nos concitoyens continuent à se préoccuper de leur santé, mais ils revendiquent le droit de ne plus être malades, et bientôt peut-être le droit de ne plus mourir. Le corps médical et le monde de la santé tout entier sont désormais confrontés à cette logique du zéro risque.

Face à cette situation, on peut aller soit vers le meilleur, soit vers le pire des mondes. Le rôle de la science, mais aussi des juristes, est de trouver un juste équilibre. À un moment où on n'entend parler que de soft law et où l'on nous explique que les professions peuvent s'autoréguler sans qu'il soit besoin de légiférer, j'apprécie les propos des porteurs du projet de réforme présenté par la Commission européenne sur l'impossibilité d'affirmer un droit sans prévoir les sanctions correspondantes. L'ex avocat que je suis se réjouit de constater que la Commission se met à nouveau à aimer le droit « dur », sans lequel, effectivement, il n'y a pas de vie en société possible.

Qui financera le traitement des données de santé ?

Il existe d'ores et déjà, sur notre planète, autant de données électroniques que d'étoiles dans l'univers. Le problème n'est plus de collecter les données : elles s'offrent spontanément. Dans le passé, c'était le médecin qui interrogeait le patient venu le consulter : « *Comment vous sentez-vous ? Avez-vous mal plutôt ici ou plutôt là ?* » Désormais, le patient envoie lui-même ses données au médecin. Parfois même, les informations sont transmises aux médecins sans le consentement du patient, ou avec un consentement fictif. Le vrai problème n'est donc plus celui de la collecte, mais celui du traitement. Qui va traiter toutes ces données ? À quel coût ? Et qui prendra ce coût en charge ?

Qui financera le traitement des données du *Big data* en matière de santé ? Il est peu probable que ce soit l'État, compte tenu du déficit auquel il est confronté. Sa prise en charge sera vraisemblablement assurée soit par un partenariat public-privé, soit directement par des acteurs privés, comme c'est déjà le cas, pour l'essentiel, aux États-Unis.

De la documentation à la manipulation ?

Ceci entraînera un autre type d'évolution. Dans le passé, lorsqu'un patient consultait un médecin, c'était généralement parce qu'il se sentait mal, même s'il y a toujours eu des hypocondriaques. Désormais, on passe de la logique de la demande à celle de l'offre : les gens vont être sollicités en permanence par des offres de santé : « *Attention à votre pression artérielle ! Faites-vous suffisamment de sport ? Comment va votre cœur ?* » On peut craindre alors de passer de la documentation à la manipulation.

Qui sera le gardien de notre vie intime ?

Jacques Ellul observait que la technique allait toujours plus vite que son environnement socio-économique et juridique et, sur ce point, il avait raison. La captation des données électroniques est une réalité objective et acquise : quoi que nous fassions, les données seront collectées. Nous allons maintenant devoir « *courir* » derrière ce nouveau phénomène et poser des garde-fous pour éviter les dérives.

Le Conseil d'État a déjà eu à se prononcer à propos des appareils respiratoires utilisés pour lutter contre les apnées du sommeil. Sachant que ces appareils ont un coût, la tentation était grande, pour l'État qui est en déficit, de contrôler si les patients les utilisent ou non et, le cas échéant, de leur imposer des sanctions. De même, on pourrait imaginer que les pouvoirs publics cherchent à vérifier si les patients prennent bien leurs médicaments, ce qui nécessiterait qu'ils pénètrent dans la sphère d'intimité des personnes. Fort heureusement, le Conseil d'État s'est opposé à ce que nous entrions dans une telle logique. Mais il y a de quoi s'inquiéter pour l'avenir, surtout sachant que nous aurons de plus en plus affaire à des acteurs privés. Pour paraphraser une formule d'Antoine Garapon, qui sera le gardien de notre vie intime

Préserver la souveraineté des États et de l'Europe

Cela m'amène à une question essentielle, celle de la souveraineté. Nous évoquons l'évolution des textes sur la protection des données personnelles au niveau français et européen. Mais le droit n'existe qu'à travers la souveraineté. Or, le Traité transatlantique qui est en train d'être négocié a vocation à supprimer les juridictions nationales, voire européennes, pour aller vers une juridiction supranationale.

Dans ces conditions, quel sera l'organe juridictionnel chargé de faire en sorte que tous les textes dont nous discutons soient respectés et appliqués ? Allons-nous confier le contrôle des grands groupes industriels qui sont en train de collecter des données personnelles à de simples juridictions arbitrales, qui n'auront de compte à rendre à aucun État ni à aucun parlement ou instance

Ne soyons pas naïfs : au moment où le *Big data* va jouer un impact majeur sur notre vie, nous ne devons surtout pas renoncer à nos systèmes de contrôle, qu'ils soient médicaux ou judiciaires. Il en va de la survie de nos valeurs et même, j'oserais dire, de notre civilisation.

Les droits individuels reconfigurés par le *Big data*

Par Alain-Michel CERETTI, représentant le Défenseur des droits, conseiller droit des maladies du pôle santé

Les questions de santé font partie des préoccupations du Défenseur des droits. Le témoignage d'Alain-Michel Ceretti est doublement instructif. A titre professionnel, il dirige une entreprise d'électronique et à titre personnel, son épouse ayant contracté une infection nosocomiale, il a fondé avec elle une association, *Le Lien*, destinée à défendre le droit des malades. C'est ce qui l'a conduit à occuper des fonctions auprès des médiateurs de la République.

Jusqu'à ce jour, le pôle santé de l'institution du Défenseur des droits n'a eu à traiter qu'un faible nombre de dossiers liés à la question du *Big data*. En 2014 et 2015 tous portent sur la divulgation d'informations personnelles via Internet, à la suite d'incidents techniques ou de manipulations

erronées. Le pôle santé n'a pas constaté de volonté de nuire ni de problème

L'intérêt des données de santé pour les acteurs publics et privés

Le *Big data* représente un outil précieux pour de nombreux acteurs publics et privés de la santé. Pour une agence régionale de santé par exemple, connaître le nombre de personnes souffrant du diabète de type 2 et leur profil en termes d'âge facilite la mise en place de moyens correspondant aux besoins. Mais c'est également un outil de décision industrielle et commerciale pour les acteurs fabriquant des dispositifs médicaux et des médicaments liés à cette pathologie. Les données du *Big data* devraient également permettre aux industriels de mieux gérer les risques liés à leurs produits, grâce au suivi des personnes y ayant eu recours.

Le SNIIRAM

En France, il existe d'ores et déjà une grande base de données, le SNIIRAM (Système National d'Information Interrégimes de l'Assurance Maladie), qui collecte les informations sur les soins reçus par les assurés et permet aux territoires de santé de se doter des moyens nécessaires. Cette base présente l'intérêt de couvrir l'ensemble de la population française, alors que dans les pays où les patients doivent recourir à des assurances privées, les données sont fragmentées entre plusieurs entreprises. Le système français bénéficie aussi d'outils très performants de suivi des profils des patients et de la façon dont ils sont pris en charge.

La loi qui est actuellement en préparation va ouvrir la base du SNIIRAM aux industriels en leur imposant un certain nombre de conditions. En particulier, l'exploitation des données ne devra pas revêtir de caractère commercial, formule qui va probablement entraîner énormément de contentieux.

Par ailleurs, le législateur distingue les données qui ne permettent pas d'identifier les personnes et celles qui permettent de le faire par recoupement ou « rechaînage ». L'utilisation des unes sera complètement ouverte et celles des autres soumise à conditions.

Les données issues des objets connectés

À côté de cette base de données officielle, il existe de très nombreuses autres données, en particulier celles recueillies par les objets connectés, dont on ne sait pas vraiment quelles sont leur qualité ni leur fiabilité, sans parler de leur statut juridique. Combien de fois chacun de nous a-t-il cliqué sur une case pour certifier qu'il avait pris connaissance des conditions générales d'utilisation d'une application, sans même avoir ouvert la page correspondante ?

Certaines de ces applications sont gratuites, d'autres payantes. Dans le premier cas, en l'absence de bannières publicitaires, on peut se demander comment l'éditeur du logiciel gagne de l'argent. Souvent, il propose des services payants ou des dispositifs médicaux à connecter au smartphone, mais on peut supposer aussi qu'il revend les données à des tiers.

C'est ainsi qu'on a vu récemment publier une étude sur l'évolution du poids en fonction des âges dont la source était *Withing*, célèbre fabricant de balances électroniques. D'aucuns considéreront que ce n'est pas grave : « *Quelle importance si Withing utilise gratuitement mes données, dans la mesure où il me fournit en contrepartie un service qui m'intéresse ?* » On peut cependant craindre que ce genre d'utilisation ne soit qu'un début.

La certification des applications

Il y a quelques années, on trouvait dans les supermarchés des yaourts censés exercer un effet bénéfique sur la santé. Une réglementation a été mise en place et, désormais, aucun fabricant de produits alimentaires ne peut se prévaloir de résultats en matière de santé sans les avoir démontrés. Il devra en être de même en ce qui concerne les applications concernant la santé.

En 2013, on dénombrait aux États-Unis 165 000 objets connectés susceptibles d'avoir impact sur la santé et vendus comme tels. On en est aujourd'hui à plus de 300 000 et de nouveaux objets apparaissent chaque jour. Le secteur connaît actuellement une bulle et comme toujours dans ce cas, de très nombreux acteurs, petits, moyens et grands, se positionnent. Il est nécessaire que les pouvoirs publics instaurent une régulation pour ne pas laisser les consommateurs démunis devant la multiplication des objets et les risques qu'ils peuvent présenter.

Des premières sanctions viennent d'ailleurs de tomber aux États-Unis : la *Federal Trade Commission*, en charge de ces questions, a infligé une amende de 150 000 \$ à la société Carrot Neurotechnology pour avoir indiqué sans preuve scientifique suffisante que son application pouvait améliorer la vision.

En France, le Conseil de l'Ordre demande des mesures similaires, mais je n'ai pas vu de disposition de ce type dans le projet de loi Santé.

L'aide au diagnostic

Depuis quelques années, il existe des logiciels d'aide au diagnostic. En France, les sociétés proposant ces applications doivent être agréées par la Haute Autorité de Santé pour que leur produit puisse être installé sur l'ordinateur d'un médecin.

Le logiciel *Watson*, développé par IBM, est capable de réaliser des calculs à une vitesse extraordinaire, ce qui peut s'avérer extrêmement précieux dans le traitement des cancers, pour lequel on s'oriente vers une approche individuelle sur la base du séquençage ADN des tumeurs. Le nombre des messages chimiques transmis par une tumeur cancéreuse est d'environ trois milliards, ce qui représente dix téraoctets d'informations. Aucun être humain, si compétent soit-il, ne pourrait gérer une telle masse d'information. Le logiciel d'IBM est capable d'établir la cartographie de la tumeur en moins d'une seconde à partir de ces données et de définir le traitement adéquat.

Le risque de dépendance à des entreprises privées

Le premier séquençage complet d'un génome humain, réalisé en 2003, avait coûté deux milliards d'euros. Aujourd'hui, le prix d'un séquençage n'est plus que de mille dollars, et il va probablement tomber à cent ou même à dix dollars assez rapidement, ce qui va créer un véritable marché.

Google et Apple ont pris une avance considérable dans ce domaine. Si la France ne se dote pas d'une plateforme sécurisée permettant de recueillir ce type de données et de s'en servir pour des traitements, elle risque de se retrouver, vis-à-vis de ces firmes américaines, dans la même situation de dépendance qu'au lendemain de la guerre en matière d'antibiotiques.

De l'aide au diagnostic à la révolution du Big data individuel

Par Philippe ROUGER, *European Institute for Systems Biology & Medicine*

Volume, variété, vélocité. La règle des trois V appliquée depuis longtemps aux données de la météorologie, de la finance ou du marketing s'impose désormais dans l'univers de la santé, ouvrant des brèches dans l'espace de vie intime des individus. Mais, explique Philippe Rouger, le Big data n'est que l'une des composantes technologiques de la révolution à venir dans la médecine.

Lors des multiples conférences qui se tiennent sur le thème de la santé et de la médecine, on entend généralement des médecins expliquer comment ils comptent utiliser les outils du *Big data*. Essayer de comprendre comment le Big data va lui-même exploiter les techniques de la médecine serait sans doute plus intéressant si l'on veut comprendre quels sont les enjeux et les risques que représentent les évolutions actuelles.

Le terme de *Big data* a été rapidement récupéré par le marketing et appliqué à toutes sortes de produits mettant en œuvre des données, qu'il s'agisse de statistiques, d'analyse de données ou encore d'*open data*, ce qui a créé une certaine confusion. En réalité, on peut parler de *Big data* lorsque les trois V suivants sont réunis : un énorme *volume* de données, une très grande *variété* dans la nature de ces données, et enfin une extrême *vélocité* dans leur production. Les données du *Big data* se renouvellent en effet tous les jours, voire toutes les heures ou même à chaque instant.

La première application du *Big data* s'est faite dans la météorologie, pour laquelle on a créé l'expression de *data science*. Au fil du temps et de l'amélioration des algorithmes et outils de calculs appliqués à ces données, les prévisions sont devenues de plus en plus justes, d'abord à un jour, deux jours, trois jours, puis à une semaine et davantage.

Une autre application spectaculaire est celle de la finance : des serveurs à haute fréquence analysent en temps réel des volumes colossaux de données, identifient des tendances et passent automatiquement des ordres d'achat ou de vente. Aujourd'hui, 60 % des ordres donnés en Bourse sont formulés par des machines.

Les applications du Big data à la santé

Dans le domaine de la santé, le *Big data* va tout d'abord permettre d'améliorer le diagnostic des maladies chroniques grâce au recueil et à l'analyse d'un très grand volume de données. Il servira également à compiler l'ensemble des données administratives et à mieux les gérer. Enfin, on commence à voir se dessiner la notion de *Big data* individuel, qui permettra à chaque personne d'accéder à ses données génétiques mais aussi aux données biologiques résultant de ses interactions avec son environnement et évoluant en permanence, ce qui représentera un volume de données incommensurable. Cette approche est encore émergente et, pour le moment, n'est pas autorisée en France ni dans une partie de l'Europe.

Une révolution pour la médecine

À mon sens, le *Big data* ne suffira pas en lui-même à révolutionner la santé. Il faudra, pour cela, qu'il s'accompagne d'autres révolutions technologiques qui auront également un impact très important sur la santé, comme le développement de la télémédecine, les autoanalyseurs, les nanotechnologies, les objets connectés. Tous ces outils généreront des données qui pourront être recueillies et traitées dans le cadre du *Big data*, ce qui permettra, sinon de révolutionner la médecine, du moins de la faire fortement progresser.

La newsletter PRES@JE.COM

Une publication de l'Institut PRESAJE

(Prospective, Recherche et Etudes Sociétales Appliquées à la Justice et à l'Economie)

30 rue Claude Lorrain 75016 Paris – Tél. 01 46 51 12 21

Courriel : contact@presaje.com – www.presaje.com

Directeur de la publication : Michel Rouger