FINANCEMENT DE LA PRÉVENTION

Propositions du Club Acteurs de la Prévention – 22 novembre 2016

Introduction :

Les données sont le carburant de la révolution numérique, l'élément essentiel pour alimenter la machine. Sans données, il n'existe pas, ou peu de perspectives, excepté la mise en œuvre de solutions applicatives et simplifiées.

Sans les données et leur traitement, la révolution numérique annoncée dans la santé n'aura pas lieu, ou sera très différente.

L'importance des données dans la santé a été perçue très tôt parce qu'elle met en jeu la personne humaine et son intimité : caractéristiques physiques et physiologiques, habitudes de vie, comportements. Les données de santé façonnent l'identité individuelle. Dès lors, si elles constituent un enjeu médical et éthique majeur, elles posent également des questions de liberté individuelle et de choix de société, ne serait-ce qu'à travers l'évolution du système de santé et la prise en charge individuelle et collective.

Il existe un important foisonnement autour de la e-santé qui fait partie des axes de développement identifiés dans le cadre de la révolution numérique. De nombreuses initiatives sont prises par les acteurs privés et publics à tous les niveaux (local, national, européen, mondial…) et à tous les stades (prévention, soins, accompagnement et information). Toutes ces initiatives posent la question de l'équilibre entre la facilité de l'accès aux données et le respect de la vie privée.Dès lors, la collecte, le stockage, la circulation et le traitement des données de santé doivent être encadrés. L'acceptation sociale, sous l'égide de l'action des décideurs politiques et des pouvoirs publics, de l'usage des données de santé en dépend. Car il est important de souligner que les finalités qui peuvent être assignées à l'utilisation des données de santé sont un facteur de progression de la santé, spécialement par la prévention.

Ce premier constat appelle aussitôt une observation. Il faut distinguer les données de santé individuelles des données de santé anonymisées. Il semble dès à présent possible de tracer les premiers contours d'un paysage où les données de santé, selon ce qu'elles renferment, seront traitées différemment. Le droit connait cette distinction. Pour ne citer qu'un seul exemple, le Système d'Immatriculation des Véhicules (SIV) mis en place

en 2009 instaure un régime spécifique avec deux finalités de réutilisation des données possibles, à des fins statistiques ou à des fins de recherche scientifique ou historique d'une part, sans recueil de l'accord préalable des personnes concernées mais sous réserve que les études réalisées ne fassent apparaître aucune information nominative et à des fins d'enquêtes et de prospections commerciales d'autre part, avec l'utilisation des données personnelles sauf opposition, conformément à la législation "informatique et libertés".

Cette séparation des données personnelles et des données anonymisées est-elle pertinente dans la santé ? Est-elle susceptible de répondre de manière concordante aux enjeux de protection individuelle et d'amélioration de la santé par la prévention, de recherche médicale et scientifique ? Est-ce une solution suffisante en soi ou faut-il la compléter d'autres innovations ?

Répondre à ces questions suppose au préalable de faire l'état des lieux.

I. Etat des lieux – Etat du droit

1. Terminologie

➢ Sur l'e-santé

L'e-santé se définit, selon l'OMS, comme :

> « Les services du numérique au service du bien-être de la personne »

Dans un rapport rendu en 2009 par M. Pierre LASBORDES[1], l'e-santé se définit également comme :

> « L'utilisation des outils de production, de transmission, de gestion et de partage d'informations numérisées au bénéfice des pratiques tant médicales que médico-sociales ».

➢ Sur la m-santé

Avec le « m » de « mobile » nous avançons encore de plusieurs décennies: il s'agit des TIC en mobilité: smartphone, tablette mais aussi tous les dispositifs intégrant une connexion à un réseau mobile.

Ces technologies ont émergé dans les années 2000, le professeur Robert S H Istepanian s'attribue la paternité du terme mHealth, utilisé dans une publication pour l'IEEE en 2003 (voir son commentaire sous ce post).

En 2011 l'OMS se risque à une définition dans ce document sur la m-Health :

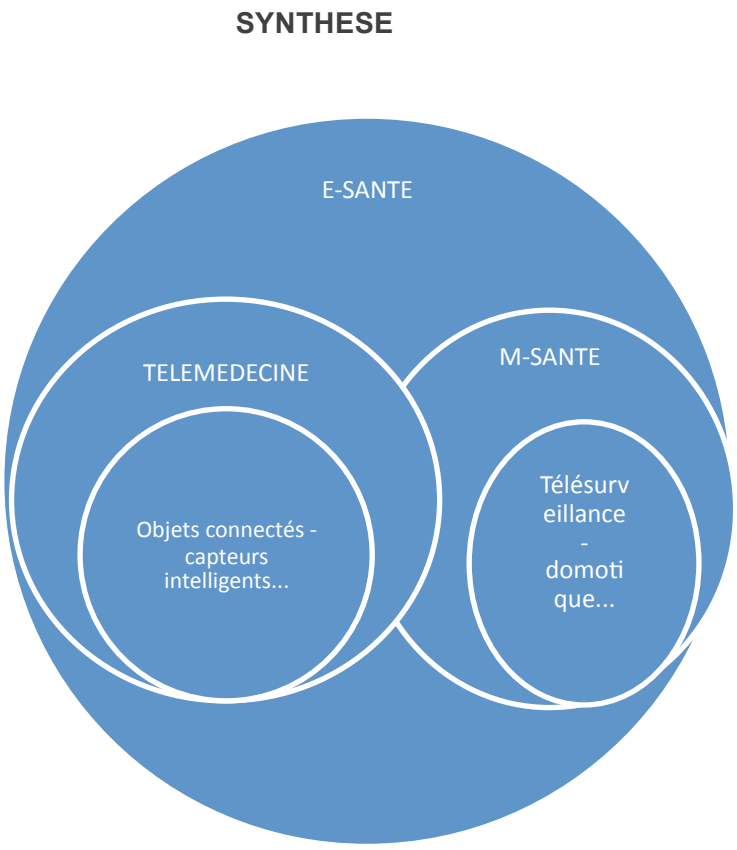
> « Pratiques médicales et de santé publique supportées par des appareils mobiles, tels que les téléphones mobiles, les dispositifs de surveillance des patients, les PDA et autres appareils sans fil. »

[1] La Télésanté : Un atout au service de notre bien-être, Rapport Lasbordes 2009

➢ **Sur la télémédecine**

Seule la télémédecine fait l'objet d'une définition dans le Code de la Santé Publique (CSP) à son article L 6316-1 :

> « Pratique médicale à distance utilisant les TIC. Elle met en rapport, entre eux ou avec un patient, un ou plusieurs professionnels de santé, parmi lesquels figure nécessairement un professionnel médical et, le cas échéant, d'autres professionnels apportant leurs soins au patient. »



2. Législation applicable

Une réglementation européenne et française peut d'ores et déjà être mobilisée pour encadrer le développement de l'e-santé et de la m-santé.

Parallèlement à cette réglementation émergente, de nouvelles pistes de régulation, engagées par de nombreux acteurs publics ou privés, se développent.

A. Sur la réglementation relative aux données personnelles

La réglementation relative au traitement (1) de données à caractère personnel (2) trouve son origine dans le droit de l'union européenne.

1. <u>Sur la notion de données à caractère personnel</u>

La notion de données à caractère personnel est définie dans la directive 95/46/CE comme :

> « toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale. »

Le projet de règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) publié le 6 avril 2016, et qui devrait être applicable au cours de l'année 2018 modifie cette définition :

> « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée"); est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale; »

Ce même projet définit par ailleurs pour la première fois les données concernant la santé :

> « devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil1 au bénéfice de cette personne physique; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques; et toute information concernant, par exemple, 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 la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro. »

2. <u>Sur l'encadrement du traitement de données à caractère personnel</u>

La notion de traitement des données est définie dans la directive 95/46/CE :

> « Toute opération ou ensemble d'opérations effectuées ou non à l' aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte , l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l' utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage , l'effacement ou la destruction. »

Outre la notion de traitement, la modification des données est évoquée par la directive européenne, mais aussi la collecte.

Toute la chaîne, de la donnée à l'utilisateur, est ainsi concernée par la réglementation européenne.

Le projet de règlement européen rappelé ci-dessus définit le traitement des données de la façon suivante :

> « Les données à caractère personnel doivent être:
>
> a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);
>
> b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);
>
> c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);
>
> d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);
>
> e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);
>
> f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);
>
> 2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité). »

B. Sur la réglementation relative aux dispositifs médicaux (DM)

La directive européenne sur les dispositifs médicaux 93/42/CE, qui définit la notion des DM (1) et fixe les exigences et moyens de vérification de la conformité (2), est actuellement en cours de révision (3).

1. Sur la définition d'un dispositif médical

L'article 1 de la directive précitée pose les différents critères propres à caractériser un dispositif médical.

> Aux fins de la présente directive, on entend par:
>
> a) «dispositif médical»: tout instrument, appareil, équipement, matière ou autre article, utilisé seul ou en association, y compris le logiciel nécessaire pour le bon fonctionnement de celui-ci, destiné par le fabricant à être utilisé chez l'homme à des fins:
>
> - de diagnostic, de prévention, de contrôle, de traitement ou d'atténuation d'une maladie,
>
> - de diagnostic, de contrôle, de traitement, d'atténuation ou de compensation d'une blessure ou d'un handicap,
>
> - d'étude ou de remplacement ou modification de l'anatomie ou d'un processus physiologique,
>
> - de maîtrise de la conception, et dont l'action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens;

2. Sur le classement des DM

La classe du dispositif médical est déterminée en fonction de l'utilisation à laquelle le fabricant destine le produit.

Pour déterminer à quelle classe le dispositif appartient, l'annexe IX révisée de la directive 93/42/CEE décrit les règles de classification applicables.

3. Sur la révision actuelle de la réglementation relative aux dispositifs médicaux

Le 26 septembre 2012, la Commission européenne a proposé de réviser le cadre réglementaire applicable aux dispositifs médicaux en remplaçant les directives actuelles par deux règlements : l'un portant sur les dispositifs médicaux, l'autre sur les dispositifs médicaux in vitro.

Le nouveau cadre devrait être effectif à l'échéance de 2018.

C. Sur la réglementation relative à la télémédecine

Un décret n°2010-1229 du 19 octobre 2010, est venu définir les actes concernés et leurs conditions de mise en œuvre et de prise en charge financière, codifié aux articles L. 6316-1 et suivants et R. 6316-1 et suivants du code de la sécurité sociale.

La télémédecine regroupe 5 actes :

- Téléconsultation,
- Télé-expertise,
- Télésurveillance médicale,

- Téléassistance médicale,
- Réponse médicale apportée dans le cadre de la régulation médicale.

L'article R. 6316-5 du code de la santé publique dispose que :

> Les actes de télémédecine sont pris en charge dans les conditions prévues aux articles L. 162-1-7, L. 162-14-1, L. 162-22-1, L. 162-22-6, L. 162-32-1 et L. 165-1 du code de la sécurité sociale.

Deux « verrous » au déploiement de la télémédecine, suite aux propositions du Rapport Lasbordes de 2009, ont été ainsi levés :

- Le principe de l'interdiction du partage d'acte,
- Le principe du remboursement réservé aux actes réalisés en présence physique du patient.

On retiendra les 3 points forts la caractérisant :

- se pratique à distance,
- a recours aux Technologies de l'Information et de la Communication – TIC,
- intègre un professionnel médical (médecin, aide-soignant, infirmier,…).

La Commission européenne se donne jusqu'à 2020 pour élaborer un cadre juridique de la télémédecine qui soit partagé par tous les Etats membres.

D. Sur la réglementation relative aux droits des consommateurs

Si la directive relative aux droits des consommateurs 2011/83/CE, exclut expressément le champ de la santé, elle couvre en revanche les applications relatives au style de vie et au bien-être.

Les exigences essentielles portent sur l'information à délivrer dans le contexte d'une vente à distance (ou d'un téléchargement en ligne) et sur le délai de rétraction accordé au consommateur.

3. Sur les institutions

Les pouvoirs publics ont pris conscience de la nécessité de créer les conditions du développement d'un « écosystème de l'e-santé » avec la volonté de le développer autour de 4 grands axes (développement de la médecine connectée, encouragement de co-innovation entre professionnels de santé, citoyens et acteurs économiques, simplification des démarches administratives, renforcement de la sécurité des systèmes d'information[2]).

Cependant , le secteur de la santé et plus spécialement de la e-santé est marqué par une présence importante d'acteurs publics ou privés à tel point qu'il est parfois difficile de discerner les champs de compétence propre à chaque entité et qu'il est prudent de ne pas prétendre à l'exhaustivité.

[2] Stratégie nationale e-santé 2020 annoncée par le Ministre des Affaires Sociales et de la Santé du 4 juillet 2016

Certaines sont spécifiques à la santé, d'autres, par leurs missions, sont susceptibles d'agir sur les données de santé.

1. La CNIL
2. La CADA
3. La HAS

La HAS, autorité publique indépendante, contribue à la régulation du système de santé par la qualité. Elle exerce ses missions dans les champs de l'évaluation des produits de santé, des pratiques professionnelles, de l'organisation des soins et de la santé publique.

A ce titre, elle établit les procédures de certification et d'agrément en relation avec les logiciels des professionnels de santé

La loi du 13 août 2004 relative à l'assurance maladie charge la HAS d'établir une procédure de certification des Logiciels d'Aide à la Prescription (LAP). Elle a été complétée par la loi du 29 décembre 2011 relative au renforcement de la sécurité sanitaire du médicament et des produits de santé.

Ces travaux concernent :
Les Bases de données sur les Médicaments ;
Les Logiciels d'Aide à la Prescription en médecine ambulatoire ;
Les Logiciels hospitaliers d'Aide à la Prescription ;
Les Logiciels d'Aide à la Dispensation d'officine.

4. La DSSIS (délégation à la stratégie des systèmes d'information de santé)

Placée sous l'autorité du secrétariat général des ministères chargés des affaires sociales, la délégation à la stratégie des systèmes d'information de santé (DSSIS) a pour objectif principal de favoriser le développement des usages des technologies numériques par les professionnels dans l'ensemble du champ sanitaire et médico-social, afin d'optimiser la prise en charge des patients et d'améliorer la qualité des soins.

Pour préparer les orientations nationales pour la « e-santé », la DSSIS (délégation à la stratégie des systèmes d'information de santé) collabore étroitement avec les directions d'administration centrale du ministère, la CNAMTS, la CNSA, la CNIL, les agences régionales de santé (ARS) et les autres ministères concernés (ministère de l'industrie, ministère de l'enseignement supérieur et de la recherche…).

Au titre de ses missions de pilotage et de coordination, il faut citer :

‣ La maîtrise d'ouvrage stratégique des systèmes d'information de santé et médico-sociaux et du déploiement des technologies numériques appliquées à la santé.

‣ La participation aux organes de pilotage mis en place au niveau national en matière d'informatisation de la santé et du secteur médico-social.

‣ La préparation des décisions du Conseil national de pilotage des ARS en matière de systèmes d'information et veiller à leur mise en œuvre.

‣ Le pilotage du schéma directeur des systèmes d'information des ARS et la mise en œuvre des projets correspondants.

‣ La tutelle sur l'ASIP Santé.

‣ L'orientation et la coordination de l'action du ministère à l'échelle européenne et internationale dans les domaines des technologies numériques et des systèmes d'information.

5. L'ASIP Santé

Création par décret en 2009 de l'Agence des Systèmes d'Information Partagés de Santé (ASIP Santé) qui est née de la volonté des pouvoirs publics d'installer une agence d'Etat référente et fédératrice de la e-santé en France.

Son rôle est de favoriser le développement des systèmes d'information partagés dans les secteurs de la santé et du médico-social.

L'ASIP Santé a vocation à développer, coordonner et participer à la régulation de la e-santé en France. Elle offre des produits et des services qui permettent de structurer et de développer la e-santé.

Elle contribue à l'élaboration des normes et référentiels.

Ainsi, à titre d'exemple, L'ASIP Santé définit, assure la maintenance et publie des référentiels nationaux sur lesquels s'appuient les systèmes d'information de santé (SIS). Ces référentiels recouvrent les domaines de l'identification, de l'interopérabilité et de la sécurité. Elle instruit les dossiers de demande d'agrément à l'hébergement des données de santé à caractère personnel.

Elle homologue les logiciels de DMP (Dossier médical Personnel), le processus d'homologation visant à s'assurer de la conformité d'un logiciel aux spécifications fonctionnelles et techniques des interfaces DMP afin de garantir l'interopérabilité et la sécurité du service.

6. La CNAMTS

La Caisse nationale de l'assurance maladie des travailleurs salariés (Cnamts) est un établissement public national à caractère administratif, jouissant de la personnalité juridique et de l'autonomie financière. Elle est soumise à une double tutelle : celle du ministère chargé de la Sécurité sociale et celle du ministère de l'Économie et des finances.

L'Assurance Maladie a vu ses compétences élargies, l'un des enjeux de l'élargissement de son périmètre d'intervention étant d'assurer la cohérence de la politique de santé.

L'Assurance Maladie est désormais associée à la définition de la politique hospitalière et de la politique du médicament. Elle se voit confier des pouvoirs nouveaux dans le domaine des soins de ville.

L'objectif est de gérer de manière cohérente les biens et services de soins, les relations avec les professionnels de santé, le partage des données de santé.

7. L'ANSM

L'Agence nationale de sécurité du médicament et des produits de santé (ANSM) a été créée par la loi du 29 décembre 2011 relative au renforcement de la sécurité sanitaire des médicaments et des produits de santé, dont les DM et DMDIV.

L'ANSM s'est substituée le 1er mai 2012 à l'Agence française de sécurité sanitaire du médicament et des produits de santé (Afssaps) dont elle a repris les missions, droits et obligations. Elle a été dotée de responsabilités et de missions nouvelles, de pouvoirs et de moyens renforcés.

L'ANSM est un établissement public placé sous la tutelle du ministère chargé de la santé.

8. L'ETALAB

La politique d'ouverture et de partage des données publiques (« Open data ») est pilotée, sous l'autorité du Premier ministre, par la mission Etalab.

La mission Etalab fait partie de la Direction interministérielle du numérique et du système d'information et de communication de l'Etat (DINSIC) au sein du Secrétariat général pour la modernisation de l'action publique.

Elle coordonne l'action des services de l'Etat et de ses établissements publics pour faciliter la réutilisation la plus large possible de leurs informations publiques.

Elle administre le portail interministériel data.gouv.fr destiné à rassembler et à mettre à disposition librement l'ensemble des informations publiques de l'Etat, de ses établissements publics et, si elles le souhaitent, des collectivités territoriales et des personnes de droit public ou de droit privé chargées d'une mission de service public.

Elle poursuit la mise à disposition gratuite des données publiques, conformément au principe général de réutilisation libre, facile et gratuite fixé par les circulaires du Premier ministre du 26 mai 2011 et du 13 septembre 2013 relatives à l'ouverture des données publiques, en mettant l'accent sur les données à fort impact sociétal (santé, éducation, etc.) et/ou à fort potentiel d'innovation économique et sociale.

Elle collabore étroitement avec les services chargés de la modernisation de l'action publique, notamment ceux responsables de l'innovation au service des usagers et de la transformation numérique de l'Etat.

9. L'ANTS

L'ANTS est un établissement public administratif sous tutelle du ministère de l'Intérieur. Il a été créé par le décret du 22 février 2007. Il a pour mission de répondre aux besoins des administrations de l'État en matière de titres sécurisés. Ces titres sont des documents délivrés par l'État, faisant l'objet d'une procédure d'édition et de contrôle sécurisée.

10. L'Association Nationale de Télémédecine (ANTEL)

L'ANTEL, Créée en 2006, L'ANTEL se présente comme la seule société savante associant tous les acteurs de la télémédecine, médecins, universitaires, chercheurs, professionnels de santé, industriels, sociologues, juristes. Elle regroupe plus de 300 membres.

Elle œuvre pour le développement de la santé numérique et en particulier de la télémédecine. Elle a plus précisément pour objet d'approcher par une démarche scientifique les nouvelles organisations des soins et pratiques professionnelles structurées par la télémédecine.

Son expertise dans ces domaines en fait un interlocuteur privilégié auprès des autorités de santé, des institutions, des ordres et des industriels.

Sur les autres acteurs professionnels :

- SNITEM (Syndicat National de l'Industrie des Technologies Médicales) – http://www.snitem.fr/
- LESISS (Fédération Les Entreprises des systèmes d'information sanitaires et sociaux) - http://www.lesiss.org/
- GIXEL (Groupement professionnel des industries de composants et de systèmes électroniques)
- CATEL (Réseau Français de compétences en télésanté) - http://www.portailtelesante.org
- SYNTEC Numérique (Chambre professionnelle des SSII, des Editeurs de Logiciels et des sociétés de Conseil en Technologies) - http://www.syntec-numerique.fr/
- FEIMA (Fédération des Editeurs d'Information Médicale et paramédicale Ambulatoire) - http://www.feima.fr/
- UNR Santé (Union Nationale des Réseaux de Santé) - http://www.unrsante.fr/

II. Problématiques

1. Des données de santé « sensibles » et peu accessibles

La démarche engagée par le Gouvernement pour la création du Système National des Données de Santé (SNDS)[3] aurait pu laisser augurer de réelles avancées pour un « open data » de la santé en France, en particulier pour la recherche.

L'accès aux données de santé contenues dans le fichier SNDS - notamment celles du SNIRAM (Système National d'Information Inter-Régimes de l'Assurance Maladie)– est susceptible d'être accepté, dès lors que la demande vise l'amélioration de la qualité de soins, la gestion de l'assurance maladie, ou la transmission aux prestataires de soins des informations relatives à leur activité[4].

Cette base de données met à disposition de ses destinataires notamment des informations hospitalières issues du Programme de médicalisation des Systèmes d'information (PSMI), celles relatives aux décès, et aux soins ambulatoires, les données de remboursement personnelles transmises par les complémentaires santé, ainsi que les données du MDPH (Maison Départementales des Personnes Handicapées).

Pour autant, comme l'a souligné la Cour des Comptes dans son rapport, la procédure mise en place pour le pilotage et l'accès à ces données est complexe et pourrait s'assimiler davantage à un parcours du combattant qu'à une simple démarche

[3] article 193 de la loi de modernisation de notre système de santé du 26 janvier 2016
[4] Loi n°98-1194 du 23-12-1998, CSS art. L161-28-1 et Arr. du 19-7-2013.

administrative[5] (voir Partie I.XXX), à en juger par le nombre d'autorités devant être consultées préalablement à la décision de la Caisse Nationale Maladie des Travailleurs Salariés (CNAMTS) en charge de « la gestion technique » du SDS, notamment l'Institut National des Données de Santé (INDS) nouvellement créé et dont l'avis demeure consultatif.

L'intention des pouvoirs publics de développer des systèmes d'information partagés dans les secteurs de la santé et du médico-social s'était déjà accompagnée de la création de l'ANTEL en 2006 pour la télémédecine, puis en 2009 de l'Agence des Systèmes d'Information Partagés de santé (ASIP Santé) comme agence référente de la « e-santé » en France.

L'« hyperproduction » juridique et politique autour de cette question s'est également enrichie par les contributions de nombreuses institutions (Cour des Comptes, Conseil d'Etat, CNIL..) et celles d'organisations professionnelles représentatives (SNITEM, LESISS, GIXEL, CATEL, SYNTEC,FEIMA, UNR Santé..).

Ce « millefeuille administratif » de la « e-santé » en France, la capillarité d'organismes, le foisonnement juridique qui en découle ne contribuent pas à rendre lisible et accessible le cadre juridique et les conditions d'accès aux données de santé pour les non initiés, encore moins pour le patient lui-même.

2. Des conditions d'accès complexes pour la recherche

Cette complexité peut s'avérer dissuasive pour nombre d'opérateurs, notamment pour les chercheurs, alors même que la loi vise « l'amélioration de la qualité des soins » pour l'accès au SNITAM, et « la recherche, les études, l'évaluation, l'innovation » comme finalités du SNDS.[6]

La volatilité des financements, l'évolution constante et rapide des techniques, comme des usages peuvent rapidement rendre obsolète une demande engagée à un instant T et en instance de décision pour un accès au fichier.

Parallèlement, le Gouvernement s'est engagé depuis plusieurs années dans la promotion de l'innovation dans le domaine de la « e-santé » à travers la création de pôles de compétitivité (Cap Digital, Medicen..) encourageant la recherche et la création de start-up dans ce domaine, sans compter les travaux de nombreux centres universitaires et d'entreprises de santé innovantes et reconnues dans le monde, notamment dans le secteur de la biologie, de la génétique… Autant d'acteurs qui souhaiteraient accéder à ces données.

Si l'accès aux données de santé en France est devenu le nouveau Graal de l'innovation française en « e-santé », cet engouement politique et économique pourrait se trouver temporisé par la complexité et la durée des procédures.

Qu'il s'agisse d'une étape intermédiaire ou d'un encadrement rigoureux de l'exploitation de nos données médicales pour éviter des abus ou des applications détournées, nous nous situons au début d'une nouvelle ère.

---

[5] Rapport de la Cour des Comptes publié le 3 Mai 2016 – « Les données personnelles de santé gérées par l'Assurance Maladie »

[6] article L 1461 -1- III du Code de la Santé Publique

Dans un monde désormais ouvert et global, les précautions prises par le législateur et les administrations peuvent se trouver rapidement contournées ou détournées.

A. Peu d'accès des complémentaires santé

1. L'accès aux données de santé anonymisées : un enjeu essentiel pour une gestion efficace du risque par les complémentaires

La question de l'accès aux données de santé est un sujet majeur pour les complémentaires santé. Actuellement, elles ne disposent pas d'informations sur la nature des dépenses qu'elles remboursent à leurs assurés.
En 2015, la Mutualité Française s'est exprimée durant l'examen du projet de la loi relatif à la modernisation de santé a été discutée, en faveur d'un accès aux données anonymisées permettant aux complémentaires non seulement d'optimiser la gestion de l'offre de soins, mais de créer des services innovants pour leurs adhérents.

De plus l'analyse des données de "santé anonymisées" donne la possibilité de :

- Mieux comprendre et améliorer notre système de santé,
- Réduire les inégalités d'accès aux soins,
- Revisiter le parcours de soin du patient,
- Identifier les pratiques les plus efficaces pour les patients.

2. La prise en charge conditionnée par le comportement des assurés

Lors de la présentation de la stratégie nationale e-santé pour 2020, Marisol Touraine a posé des limites en déclarant que « les assureurs n'auront pas accès aux données des patients ». Elle s'est également dite défavorable aux prises en charge conditionnées par le comportement des assurés.
Dans cette déclaration, la ministre vise « l'offre assurantielle comportementale ». Cette pratique créé un nouveau type de sélection du risque, reposant sur une approche assurantielle inédite en France qui prétend prendre en compte les comportements dits « bénéfiques » de la personne sur sa santé. Les données liées aux comportements sont portées à la connaissance des organismes assurantiels, qui proposent des contreparties lorsque celles-ci sont conformes aux standards de comportements. Cela revient à une marchandisation de la santé des assurés.

Le pôle santé/Prévoyance Macif a récemment considéré qu'une telle démarche ne correspond pas aux valeurs portées par le groupe. Cette pratique risque d'engendrer de nouvelles distinctions : ceux qui naissent avec un bon « capital santé » et ceux qui ne l'ont pas, ceux qui adoptent des comportements préventifs et les « autres ». Un tel écueil a pour effet de creuser les inégalités de santé de ceux qui ont des difficultés à se conformer aux standards de prévention. Cette méthode ne tient pas compte des nombreux déterminants de santé, de ces paramètres contraignant l'individu : situation de précarité, qualité du logement … *Les questions liées à l'environnement, telles que la* qualité de l'air et celle des aliments jouent un rôle déterminant sur notre santé. Les facteurs relatifs aux conditions de travail comme la pénibilité et les risques au travail ont aussi des effets directs sur l'état de santé de l'individu.

B. Peu de lisibilité pour les usagers bien qu'ils contrôlent l'accès à leurs données

Il ressort d'une étude récente (Ipsos/association Lir – 8 Juin 2016[7]) que quatre Français sur cinq (78%) seraient prêts à partager et à rendre accessibles l'ensemble des données concernant leur santé (dossier médical, résultats d'analyse, radios, ordonnances...) aux professionnels de santé qui les suivent.
En effet, la plupart des sondés déplorent l'absence de communication et de partage des informations médicales les concernant entre professionnels de santé qu'ils soient dans la sphère privée ou publique.

L'instauration par la loi de modernisation de notre système de santé et la mise en œuvre par décret[8] du dossier médical partagé (DMP) généralisé d'ici deux ans répond en grande partie aux attentes exprimées par les Français en facilitant par ce dispositif, un continuum d'informations médicales et leur partage par les professionnels qui les suivent.

Inspiré du Dossier Médical Personnel qui a permis de créer 500.000 dossiers à ce jour, il s'agira d'un dossier numérique collectant toutes les données médicales d'un patient, pour « favoriser la prévention, la coordination, la qualité et la continuité des soins ». L'objectif du Dossier Médical Partagé est de mettre à disposition des professionnels de santé, avec l'accord préalable du patient, des informations médicales (telles que les antécédents médicaux, l'état des vaccinations, les comptes rendus de biologie médicale, des examens d'imagerie médicale, les traitements prescrits) en provenance d'autres professionnels de santé: généralistes, spécialistes, personnel infirmier ou hospitalier.

Le décret définit les conditions d'accès en lecture et d'alimentation du dossier par les différents acteurs de la prise en charge des patients, ainsi que les conditions dans lesquelles certaines informations peuvent être rendues inaccessibles.

Cette évolution vers un partage et une continuité des informations médicales, est révélatrice du souhait des Français d'améliorer l'efficacité des soins et leur prise en charge.

Néanmoins, l'essor de sites Internet tels que *Doctissimo* ou le succès rencontré par des émissions, des présentateurs « experts » et des magazines grand public consacrés à la santé, montrent à quel point les Français veulent non seulement être mieux soignés, mais souhaitent également comprendre comment et pourquoi. Ils sont passés en quelques années de patients passifs à des consommateurs avertis, informés et pro-actifs.

Pour autant le patient n'est pas un « sachant».

Dans la plupart des cas, faute de pouvoir comprendre, interpréter, exploiter ses données de santé pour un diagnostic, un dépistage, un suivi thérapeutique, le patient est totalement dépendant et doit s'en remettre au corps médical entendu dans une acceptation large (médecin généraliste/spécialiste, biologiste médical, radiologue, dentiste, pharmacien,...).

[7] Sondage Ipsos réalisé par Internet du 27 au 31 mai auprès de 2.000 personnes constituant un échantillon national représentatif de la population française de 18 ans et plus.
[8] Décret n° 2016-914 du 4 juillet 2016 relatif au dossier médical partagé

Bien qu'il soit détenteur/dépositaire de l'accès à ses données de santé, celles-ci relèvent tout naturellement de l'expertise des cliniciens et praticiens, sans lesquels ce patient ne pourrait améliorer sa santé, voire prendre des risques réels, s'il dérogeait à cette règle.

Mais que lui reste-t-il pour « prendre le contrôle de sa santé », la mesurer ?

L'émergence des objets connectés a créé les conditions de cette quête d'indépendance et de connaissance, à moindre risque et à moindre prix.

Prolongeant les espaces de liberté que les patients s'étaient déjà octroyés dans des forums d'échange et de partage d'informations, avec les objets connectés le consommateur de santé s'affranchit, prend le contrôle de ses données de bien-être, intégrant un univers normé par lequel il peut tendre vers la perfection et l'invincibilité…hors du champ médical classique.

Le « quantified-self » est né, « *relevant d'une démarche non pas de mesure, mais de quantification continue, en temps réel, – contribuant à la production sociale de normes de comportements, de performance et de santé, éminemment évolutives… et permettant la visualisation et, éventuellement, la mise en comparaison de leurs progrès respectifs par les utilisateurs reliés directement à l'Internet à travers les capteurs qui les « quantifient »* ».[9]

3. Territorialité et finalité de la collecte des données de bien-être

Si l'accès aux données de santé sur le territoire français est entouré d'une nébuleuse juridique foisonnante et dissuasive, une fois franchie la frontière ténue des données de bien-être, le cadre juridique de ces dernières peut varier selon la territorialité et la qualification de l'auteur ou de l'entreprise en charge de collecter les données.

Si l'établissement principal de l'entreprise est situé dans l'Union européenne, la collecte de ces données sera encadrée par la directive européenne de 199510 crée dans le contexte de l'émergence des autoroutes de l'information en 1994, face à la menace de voir nos données massivement collectées par le biais de ce qui deviendra Internet. L'Union Européenne a dans ce contexte construit un cadre strict pour protéger nos données personnelles, par la reconnaissance de la protection de la vie privée et l'exclusion de leur exploitation à des fins commerciales.

Or, si les données de bien-être sont collectées par un opérateur dont le siège est situé hors UE, c'est la loi de son pays d'établissement qui s'appliquera.

A. Les données sont collectées massivement en Europe par des entreprises Outre-Atlantique

[9] *« Le corps, nouvel objet connecté - du quantified self à la M-Santé : les nouveaux territoires de la mise en données du monde »* - Cahiers IP N°2 - CNIL

[10] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Près de 90% des objets connectés sont commercialisés par des entreprises établies Outre-Atlantique. Bien qu'elles disposent de filiales européennes ou françaises, ces entreprises sont, pour la plupart, américaines et régies par la loi américaine.

En l'occurrence, cet élément incontestable d'extranéité amène plusieurs réflexions sur la sécurité qui entoure la collecte de ces données, leur conservation, et la finalité de leur(s) exploitation(s) après cession à des tiers par l'auteur de la saisie des données.

Il ressort de la Directive e-commerce de 2000, que la loi applicable à un opérateur collectant des données dans l'Union Européenne, se voit appliquer la loi du lieu d'établissement de son siège social.

En l'occurrence, si la filiale d'une entreprise dont le siège est établi aux Etats-Unis collecte des données de bien-être par le biais d'objets vendus dans l'Union européenne à des citoyens européens, c'est la loi américaine qui s'appliquera.

De réelles différences culturelles séparent les Etats-Unis et l'Europe dans ce domaine. L'Europe protège la vie privée. Les Etats-Unis protègent le consommateur.

B. Des accords UE-US sur les transferts de données personnelles créent de nombreuses incertitudes sur la sphère de sécurité accordée par les Etats-Unis

En l'occurrence, sur le fondement de la directive de 1995, la Commission européenne a pu entamer de longues discussions avec les Etats-Unis pour envisager une législation plus appropriée dans le cadre de transfert de données européennes. Nommés « Safe Harbor agreement », puis devenu très récemment « Privacy Shield » (voir encadré), ces accords auraient eu, bien au-delà du nombre encore faible d'entreprises américaines ayant souscrit à ces engagements, une certaine influence.

Selon le Financial Times, les discussions entreprises dans ce cadre, la pression de l'opinion, notamment après les révélations d'Edward Snowden, auront contribué au dépôt de plus de trois cents propositions de lois dans les Etats américains et près d'une douzaine au niveau fédéral dans le souci d'assurer une protection aux données personnelles.
La presse se fait l'écho d'une opinion inquiète et tiraillée entre sécurité du territoire américain face aux menaces terroristes et protection de la vie privée.[11]

Après Snowden, le plus marquant sera l'affaire Max Schrems, du nom d'un jeune étudiant autrichien en droit aux Etats-Unis, qui après les révélations d'un représentant de Facebook dans sa classe[12], a engagé plusieurs poursuites devant

[11] *« These events – and the doubts they inspired – have contributed to a cloud of personal "data insecurity" that now looms over many Americans' daily decisions and activities » - Pew interest – 20.05.2015*

[12] « Quelqu'un de Facebook est venu nous expliquer comment les lois européennes sur la vie privée fonctionnaient. J'étais le seul Européen. Et il disait : "Vous pouvez faire ce que vous voulez, rien ne vous arrivera jamais". "*Tant que personne ne vous dit non, vous p*ouvez continuer à utiliser l*eurs données".* »
Le Monde – 6 octobre 2015

la Cour de Justice de l'Union européenne, accusant notamment Facebook, mais aussi Apple, Skype, Microsoft et Yahoo!, de collaborer avec l'agence de renseignement américaine. C'est à l'issue de sa plainte que le « Safe Harbor » sera invalidé par la CJUE[13]. Comme le rappelle Viviane Reding, l'invalidation par la CJUE du *Safe Harbor* tenait à ses lacunes en termes de protection des données personnelles face à l'impératif de défense nationale et de sécurité invoquées par les agences américaines afin d'y avoir un accès quasi-illimité, élément toujours présent au sein du *Privacy Shield*.

Ce dernier court donc le risque d'être invalidé comme son prédécesseur dès sa mise en place : « *You can call it by another name and give it fresh colours, but the problem has not been solved*. »

Autre cadre de négociation entre l'UE et les Etats-Unis; le TAFTA (Transatlantic Free Trade agreement). Bien que des garanties semblent apportées pour considérer que les données personnelles ne seront traitées que sous l'angle commercial, les menaces d'appropriation telles que décrites par Max Schrems ressurgissent.

« On nous assure que les données personnelles seront exclues, que cela concernera uniquement les données commerciales, mais nous, nous considérons que 90% des données commerciales sont personnelles puisqu'elles servent notamment à cibler la publicité » déclare Isabelle Falque-Pierrotin, présidente de la CNIL.

Le nouvel accord est par conséquent susceptible d'être à nouveau invalidé par les juges européens. Pour finir, il a été élaboré dans le cadre de la directive européenne de 1995 sur la protection des données. Or, cette directive va être remplacée en mai 2018 par un règlement adopté en 2015. L'insécurité juridique, ennemie des entreprises, plane donc toujours.

[13] CJUE affaire C-362/14- 6 octobre 2015 «L'accès à grande échelle des agences de renseignement aux données que des entreprises certifiées au titre de la sphère de sécurité transfèrent aux États-Unis soulève de graves questions sur la continuité de la sauvegarde des droits des citoyens européens en matière de protection des données lorsque des données les concernant sont transférées aux États-Unis»

Le « Privacy Shield »

L'Union européenne (UE) et les États-Unis entretiennent d'importants liens commerciaux. Les transferts de données à caractère personnel constituent une partie importante des relations transatlantiques, en particulier dans le contexte de l'économie numérique mondiale actuelle. De nombreuses transactions impliquent la collecte et l'utilisation de données à caractère personnel, par exemple vos noms, numéros de téléphone, domicile etc…. Par exemple, vos données peuvent être collectées dans l'Union par une succursale ou un partenaire commercial d'une société américaine qui reçoit les informations et les utilise ensuite aux États-Unis.

Pour transférer des données à caractère personnel depuis l'Union européenne vers les États-Unis, différents outils sont disponibles, tels que des clauses contractuelles, des règles d'entreprise contraignantes et le bouclier de protection des données.
Le « Privacy shield », « bouclier de protection des données UE-États-Unis » en français, est entré en vigueur depuis le 1er août 2016. Il autorise le transfert des données personnelles de l'Union européenne à une société aux États-Unis, pour autant que cette société procède au traitement des données à caractère personnel en respectant un ensemble de règles et garanties en matière de protection des données exigés par le droit de l'Union. Au-delà de cette obligation formelle, les entreprises destinataires des données doivent être préalablement inscrites sur le registre tenu par l'administration américaine.

Le 13 avril 2016, les autorités européennes de protection des données (la CNIL pour la France) ont émis un avis sur cet accord, où elles expriment de sérieuses préoccupations. Puis le Parlement européen a fait de même dans une résolution votée le 26 mai: les députés européens réclamait de rouvrir les négociations pour apporter plus de garanties. Les Etats membres, réunis au sein d'un groupe de travail, ont quant à eux validé le texte, malgré l'abstention de quatre pays, l'Autriche, la Hongrie, la Slovénie et la Bulgarie.

Enfin, un autre cadre UE-US serait également prévu et en cours de négociation dont l'objet est la lutte contre la criminalité organisée et le terrorisme, ouvrant à nouveau les vannes d'accès à nos données.

C. La collecte de données « sensibles » peu encadrée par la réglementation américaine

Au-delà du quatrième amendement de la Constitution[14], le *Privacy Act* (loi sur la protection de la vie privée) est le principal cadre juridique protégeant les données à caractère personnel détenues par le secteur public aux Etats-Unis. Il protège les fichiers détenus par les agences gouvernementales américaines et leur demande d'appliquer des pratiques d'information justes.

Néanmoins, le *Privacy Act* ne protège pas les individus qui ne sont pas, soit des citoyens américains, soit des résidents permanents. Cette absence de protection constitue l'une des principales préoccupations pour toute négociation transatlantique.

On doit relever également l'absence d'autorités de contrôle chargées de la protection des données indépendantes aux Etats-Unis qui constitue certainement d'un point de vue européen un affaiblissement du système, surtout en cette période de développement technologique rapide. Bien que de nombreux principes de protection de données tels que reconnus dans le droit européen soient présents dans le droit américain, il n'existe aucune base solide dans le droit américain pour les principes essentiels que sont le principe de minimisation et de la limitation de la finalité.[15]

Un accord transatlantique sur l'échange et la protection des données personnelles tel qu'annoncé par le Contrôleur européen de la protection des données est certes à l'étude, mais quand pourra-t-on imaginer un accord assorti d'un système contraignant et harmonisé de part et d'autre de l'Atlantique ?

En conséquence, qu'il s'agisse des accords régissant les transferts de données entre l'Union européenne et les Etats-Unis, des accords sur la lutte contre le terrorisme, des accords « Safe Harbor » et « Privacy Shield », la loi américaine prédomine dans les échanges, accordant une grande liberté d'usage et de cession des données personnelles collectées dans l'Union européenne, assortie d'un contrôle judiciaire très limité, sans se préoccuper de la finalité et de ses conséquences.

[14] Dans l'affaire *Schmerber c. Californie*, en 1966, la Cour suprême a déclaré que « [l]*a fonction primordiale du quatrième amendement est de protéger la vie privée et la dignité contre l'intrusion injustifiée de l'Etat*».

[15] « *Protection of personal data and security measures: towards a transatlantic perspective* » Rocco Bellanova et Paul De Hert – *Cultures & Conflits*, n° 74, été 2009, p. 63-80

Les objets connectés

Un objet connecté désigne tout objet composé de capteurs qui envoient des informations vers une application mobile ou un service web. Certains objets connectés ont un usage purement personnel (évaluer sa forme, progresser dans un sport, maigrir...), d'autres s'intègrent dans une stratégie de prise en charge globale du patient (bien prendre son traitement, contrôler sa tension, sa fréquence cardiaque, mesurer sa glycémie…)

Le marché des objets connectés en chiffres :

D'après une étude menée par Gartner et l'Idate en 2020 on peut estimer que le nombre d'objets connectés en circulation à travers le monde s'élèvera entre 50 et 80 milliards. En clair chaque personne détiendra environ 6 objets connectés. Plus d'un produit connecté sur deux concerne aujourd'hui la santé, avec deux tendances : le bien-être et l'appui médical.

La santé et l'énergie devraient être les 2 secteurs les plus impactés par l'internet des objets d'ici 10 ans. Ils ne devraient d'ailleurs pas seulement être touchés par la vague IoT (*Internet of Things*) mais en grande partie réinventés et révolutionnés tant sur l'aspect pratique que théorique. Si, aujourd'hui, les consommateurs ne voient essentiellement que la partie grand public des objets connectés, ceux-ci devraient sentir les effets de cette révolution dans les prochaines années.

- La multiplication des bracelets et montres connectés : la grande tendance en matière de santé connectée est la multiplication des bracelets et montres.
- Certains renseignent sur le niveau d'activité physique (nombre de pas et de kilomètres parcourus, calories brûlées, etc.) et indiquent si l'on atteint ou non ses objectifs et comment y parvenir.
- D'autres bracelets, plus classiques, enregistrent les battements de votre coeur, ou la qualité de votre sommeil, et bien d'autres paramètres vitaux encore.

La balance connectée : un objet plébiscité

6% des français possèdent aujourd'hui une balance intelligente qui permet de suivre son poids et son IMC (indice de masse corporelle). Grâce à ce type de balance, vous pouvez suivre votre courbe de poids, vous fixer des objectifs à atteindre compte-tenu de votre poids idéal et mesurer les progrès accomplis. Certaines marques proposent en plus un coaching en ligne pour vous aider davantage.

La fourchette minceur

Cette fourchette a été développée pour aider à diminuer la vitesse à laquelle on mange et ainsi limiter les apports caloriques (réglée sur une bouchée toutes les 10 secondes). Elle a été créée à l'origine dans le cadre d'un programme médical à destination des personnes souffrant d'obésité.





Des objets connectés toujours plus médicaux

Les objets connectés vont aussi révolutionner l'univers des malades en les aidant dans leur vie quotidienne et dans l'observance de leur traitement.

Le vainqueur du prix de l'objet connecté de l'année 2015

La société française iHealth a remporté le prix "Objet connecté de l'année" en santé avec son dispositif de mini-glucomètre connecté. Le dispositif se branche directement sur la prise casque d'un smartphone ou d'une tablette et affiche la mesure instantanément sur l'application dédiée, afin de faciliter le suivi des objectifs glycémiques du patient.

Le projet ambitieux de Google : surveiller, prévenir, et défier la mortalité

La firme de Mountain View vient de déposer un brevet qui rendrait les salles de bains intelligentes et renforcerait la démarche de prévention pour ainsi éviter certaines maladies. Dans cette salle de bain futuriste, des capteurs présents dans le tapis, la baignoire ou sur le siège des toilettes auraient la faculté de suivre et mesurer la santé de l'utilisateur avec une assiduité et une acuité que beaucoup de médecins pourraient lui envier. Chaque objet aurait un rôle précis pour évaluer presque en direct les conditions de santé suivantes : l'appareil cardio-vasculaire, le système nerveux, le tonus musculaire. Un check-up qui devra, avec le consentement du patient, parvenir électroniquement au généraliste, qui sera lui seul à même de l'interpréter correctement et d'évaluer avec justesse les données collectées. Si un capteur détecte une anomalie, un message d'alerte sera directement envoyé au médecin traitant de l'utilisateur.

D. Effets pervers et effets secondaires

1. Vigilance des autorités de contrôle et prise de conscience du consommateur face aux usages et aux pratiques des éditeurs d'objets connectés

Plus encore que les Américains, les Français manifestent leur défiance à l'égard des objets connectés. Dans le cadre de l'étude (Ipsos/association Lir – 8 Juin 2016) 44%, seulement, accepterait, lorsqu'il s'agit de partager *« avec des professionnels de santé »* leurs données collectées par des objets connectés comme des trackers d'activité ou des outils de suivi de l'alimentation.

Selon une étude de GFK, certains obstacles évoqués à l'achat comprennent:

- Le doute sur la fiabilité des mesures (50% des personnes réfractaires interrogées).
- L'impression d'une l'intrusion dans le quotidien (29%).
- La méfiance quant à l'utilisation des données. (24%).
- La peur de ne pas savoir se servir de l'objet (22%).
- La peur d'une dépendance, comme celle concernant les smartphones (10%).

Si le marché a doublé en volume sur un an dans l'Hexagone, GFK estime qu'il n'a pas atteint son potentiel. En acquérant plus de *"notoriété"* et en développant plus de *"pédagogie"*, il pourra se *"réveiller"*. Une étude d'Endeavour Partner réalisée

aux États-Unis en 2014 montre ainsi, qu'un tiers des objets connectés se retrouvent rangés dans un tiroir au bout de six mois.

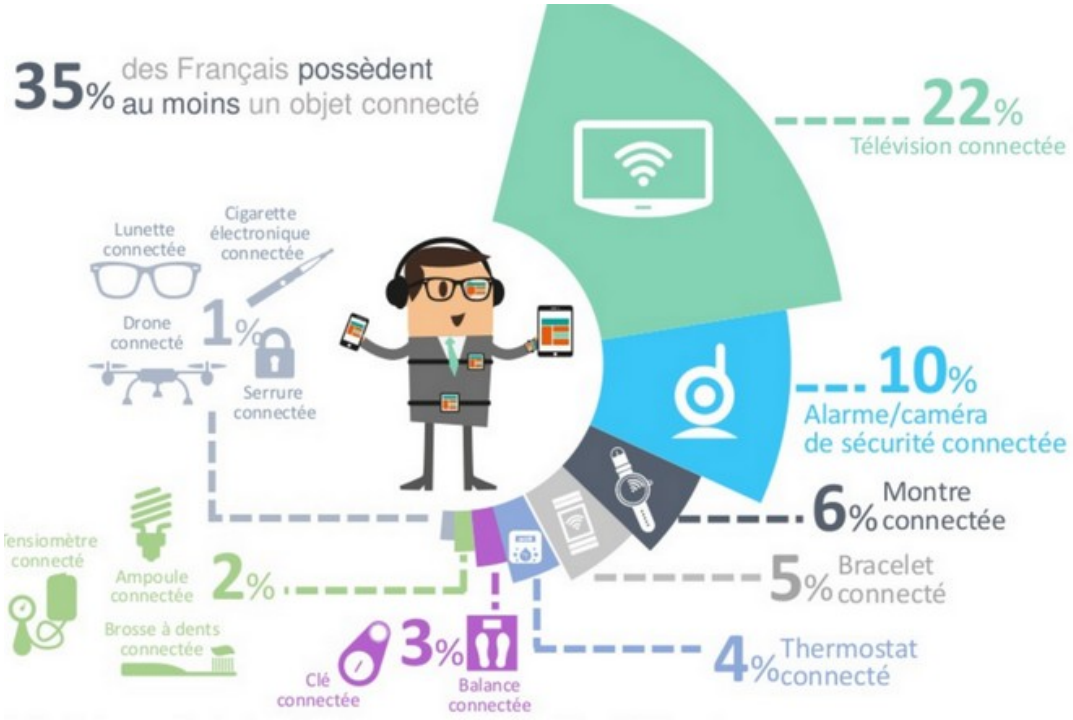
Le propre d'un objet connecté est d'échanger des informations sur les réseaux de manière quasi permanente et instantanée, par l'intermédiaire d'une application web ou mobile. Si l'utilisateur considère qu'il pourrait améliorer un suivi thérapeutique avec son médecin par ce biais, il se doute pas ou peu que ces données vont être diffusées auprès d'un plus grand nombre d'utilisateurs.

En mai 2014, la CNIL et 26 de ses homologues rassemblés au sein du Global Privacy Enforcement Network (GPEN – réseau d'organismes agissant au sein de l'OCDE pour la protection de la vie privée) ont mené un audit en ligne simultané de plus de 1.200 applications mobiles, qui témoigne d'une carence manifeste dans l'information faite aux utilisateurs du traitement des données personnelles qui les concernent.

De nombreux fabricants d'objets connectés ou d'applications mobiles n'ont pas de politique de gestion des données personnelles, ou restent volontairement flous sur le type d'informations collectées, leur partage avec des sociétés tierces et les traitements envisagés.

Lorsqu'une autorisation de la part des utilisateurs s'avère nécessaire, ces derniers peuvent être fortement incités à partager des informations relatives à leur mode de vie, leur santé, leurs déplacements, leurs habitudes de conduite, moyennant l'obtention d'avantages commerciaux (miles, bons de réduction, réduction du montant de cotisation d'assurance etc.).

Eu égard à la masse d'informations collectées et aux capacités d'analyse de données, les dérives et les risques de profilage des utilisateurs sont particulièrement élevés.



Le téléphone mobile est également devenu un objet connecté grâce à la « M-health » pour des applications payantes et gratuites. Le modèle économique de nouveaux entrants du « quantified-self » est d'offrir l'accès à ce type de service pour récolter en contrepartie des données d'usage destinées à des partenaires ou à des sociétés tierces.

Ces pratiques pourraient se résumer par l'adage: « si vous ne payez pas pour le service, c'est que vous êtes le produit ».[16]

2. Risque de perte de contrôle des données et d'appropriation à des fins malveillantes ou/ et criminelles

Plusieurs études ont révélé d'importantes failles de sécurité dans les objets connectés, rendant ainsi possible le détournement d'une multitude de données personnelles au profit de tiers non autorisés, l'utilisation malveillante des données interceptées, voire la prise de contrôle de l'objet connecté lui-même.

Ainsi, la fiabilité des objets connectés est en cause, en particulier les conséquences attachées à la défaillance de leurs capteurs.

Certains développeurs n'en ont pas conscience et omettent de se conformer aux exigences essentielles de sécurité applicables et de se déclarer (en France) auprès de l'Agence Nationale de sécurité du médicament et des produits de santé (ANSM). En effet, l'utilisateur d'objets connectés et d'applications mobiles peut craindre de perdre la maitrise de ses données une fois celles-ci collectées et faire l'objet d'un profilage préjudiciable.

Ainsi, un « peacemaker » dont les codes ont été volés peut être commandé à distance pour tuer le porteur de ce dispositif médical. Scénario d'un épisode de la série télévisée « Homeland », il n'en demeure pas moins une hypothèse, dès lors que les données de l'usager ont été détournées et que les capteurs ne sont pas suffisamment sécurisés.

Récemment, la faillibilité des objets connectés a été à nouveau invoquée, après une violente attaque informatique aux Etats-Unis. « *Les logiciels embarqués dans ces objets [connectés] peuvent contenir des vulnérabilités, ou présenter des défauts de configuration permettant d'en prendre le contrôle. Si ces objets sont connectés directement sur Internet, ils peuvent représenter des cibles faciles pour des attaquants qui pourront les utiliser […] comme vecteur d'attaque* ».[17]

Enfin, l'usurpation et le vol d'identité via l'appropriation de données biométriques (mesures du vivant) captées à travers des données de bien-être relèvent-elles d'une simple prospective ou du scénario excessif d'un thriller? Comme le souligne la CNIL, les objets connectés sont amenés à devenir toujours plus intrusifs, plus implantés et à développer toujours plus leur capacité à « capter » le corps.

3. Des données utiles pour développer le « transhumanisme »

[16] Le Corps nouvel objet connecté – CNIL
[17] LE MONDE | 25.10.2016 - Par Martin Untersinger

De « l'homme de mille ans » à « la mort de la mort », la mouvance transhumaniste se rapproche du rêve prométhéen de défier les dieux, la vie et… la mort.

Le nouveau messianisme financé par Google dans la Sillicon Valley, mais également en Chine et d'autres pays d'Asie, fait émerger la perspective d' «augmenter l'humain » et sa durée de vie, d'éradiquer les maladies héréditaires ou encore de sélectionner, dès le stade de l'embryon, des caractéristiques jugées désirables ou pas.

Appelé également « la révolution NBIC » - soit la convergence des Nanotechnologies, de la Biologie, de l'Informatique et des sciences Cognitives, ce mouvement scientifique et philosophique prône l'amélioration illimitée des facultés physiques et intellectuelles des humains.

Cette approche vise une humanité « éternellement » connectée et bien portante, société idéalisée et normée, digne du film *« Bienvenue à Gattaca».* Ainsi, dans sa forme ultime, le transhumanisme va jusqu'à préconiser la fusion physique entre les humains et les futurs réseaux d'ordinateurs dotés d'intelligence artificielle. Surnommés *« body hackers »* des chercheurs *cyborg* existent déjà Outre-Atlantique en se greffant des puces dans le corps, comme Kevin Warwick, le célèbre professeur de cybernétique.

Pour fonder une telle société ne faut-il pas opérer « une sélection » des individus répondant à ces idéaux, en créant une société à plusieurs vitesses ? Ainsi, la collecte de données personnelles n'est-elle pas le début de ce tri entre individus bien portants et performants, et les autres. Comme le souligne l'association « Technoprog » : *« l'un des risques, c'est qu'une oligarchie s'accapare cette technologie et que nous tombions dans une sorte de dictature ».*

Comme le prédit Juli Zeh dans son livre de science-fiction « *Corpus delicti – un procès* »[18], notre monde dans 40 ans sera doté des moyens de prévenir et de réparer, interdisant la maladie considérée comme un comportement déviant.

Nouvelle vision du monde qui amène de nombreuses interrogations, tant éthiques, que philosophiques ou religieuses, elle est paradoxalement hors du champ de la réflexion politique.

Cette doctrine repose au demeurant, sur des avancées scientifiques avérées et offrant à notre humanité un potentiel fabuleux pour la prévention et la guérison de nombreuses maladies, notamment grâce à la biologie et à ce que l'on nomme désormais, la médecine prédictive.

Le rêve d'une partie de la sphère scientifique et économique mondiale de les associer et de les croiser avec d'autres technologies, nous oblige à mieux appréhender la portée d'une telle révolution et ses enjeux éthiques, à repenser notre rapport à la santé, à faire émerger la nécessité d'un patient en mesure de contrôler sa santé, sans être contrôlé à son insu.

[18] Babel - Actes Sud – Mars 2016

III. Six propositions pour une prévention connectée et contrôlée

1. Affirmer les valeurs et la performance européenne pour une Europe qui garantisse et contrôle l'usage de nos données personnelles

L'Union européenne a, depuis l'élaboration du règlement de 1995 sur le traitement des données à caractère personnel pu actualiser et adapter ce dispositif à l'arrivée de nouvelles technologies avec le « Groupe de l'article 29 » pour apprécier leur conformité avec les valeurs de protection de la sphère privée.

Pour autant, la globalisation, la constante et multiple connexion de chaque citoyen via Internet et son Smartphone ont de toute évidence permis de contourner les précautions prises dans les années 90.

Si les Etats membres, notamment la France, tendent à encadre et à renforcer les dispositifs de collecte de données de santé, ces systèmes n'avantagent pas toujours les chercheurs.

Une nouvelle réflexion s'impose pour rendre compatibles une Europe de l'innovation et celle de la protection du citoyen et de sa sphère privée.

Le cadre de cette réflexion devrait permettre l'émergence de plusieurs propositions telles que :

- **créer un bouclier et une préférence communautaires pour la recherche européenne pour l'accès aux données de santé par une réglementation et un programme de soutien adaptés, comme un programme visant une espace européenne de la prédictibilité et de la prévention, et de la contextualisation des données,**

- **créer les conditions d'un dialogue, d'une réflexion et de propositions européennes sur la question du transhumanisme,**

- **renforcer les obligations qui pèsent sur les fabricants et importateurs d'objets connectés dont la finalité affecte des données sensibles, qu'il s'agisse de données de santé ou de données de bien-être,**

- **légiférer sur la création de tiers de confiance qui contrôleraient l'utilisation, la finalité et la cessibilité de données sensibles européennes aux Etats-Unis.**

2. Défendre la singularité et la performance de la recherche européenne

Les effets pervers d'une défiance collective des consommateurs et des patients sur l'utilisation détournée, voire frauduleuse de leurs données [19]à d'autres fins que celles de leur santé pourraient être préjudiciables à terme, pour la recherche européenne.
Cette méfiance pourrait entraîner un renforcement et une complexification des dispositifs nationaux d'accès aux données de santé. Alors même que des données européennes « anonymisées » et « recoupées » entre elles, sans restriction juridique, seraient collectées massivement, notamment par les Etats-Unis et la Chine, une réelle distorsion serait crée de facto pour nos chercheurs au niveau international.

Encourager la recherche et l'innovation européennes dans le domaine de la santé et de la prévention constitue une garantie d'indépendance pour faire entrer l'Europe dans une nouvelle ère, sans renier ses valeurs.

Aussi, il nous semble important de faciliter l'accès et de donner une priorité à notre recherche européenne pour l'utilisation de données de santé, en apportant à l'ensemble des citoyens le bénéfice scientifique et économique de ces avancées.

3. Contrôler l'usage de nos données au niveau européen

Dans l'Union Européenne, et plus particulièrement en France, une série de dispositions législatives et réglementaires a vocation à s'appliquer, imposant des obligations à respecter par les fabricants, éditeurs d'applications et hébergeurs, de manière à protéger les données des utilisateurs d'objets et applications connectés.

Dans le cadre de la révision du projet de règlement européen[20] – en cours d'élaboration, et qui a vocation à s'appliquer aux Etats membres – fixe un cadre de protection des données à caractère personnel avec une plus grande responsabilisation des individus. Le législateur européen entend placer celui-ci au cœur du dispositif de protection des données à caractère personnel.

Dans ce cadre, il pourrait être prévu de disposer du droit à la notification d'une violation de ses données à caractère personnel lors de l'apparition de failles de sécurité, voire du droit d'opposition à une mesure de profilage ou encore, selon des motifs limitativement énumérés, du droit à l'effacement de ses données, ainsi que l'effacement par des tiers des liens vers ces données ou de toute copie ou reproduction de celles-ci.

Ces nouveaux droits sont primordiaux en ce qu'ils permettent d'accroître la maîtrise que les utilisateurs ont sur leurs données.

4. Prise de conscience et de contrôle par le patient

L'individu n'est pas nécessairement conscient des enjeux attachés à la protection de sa vie privée et de ses données. Il ne mesure pas toujours les conséquences d'une appropriation ou un vol de ses données.

---

[19] Voir notamment les articles "Des centaines de résultats d'analyses médicales accessibles sur internet", publié sur www.rue89.com, le 10 janvier 2012

Une éducation de l'usager et a fortiori du patient, s'impose dans ce domaine.

Il nous semble déterminant d'encourager, voire de rendre obligatoires les processus de type **« privacy by design »** (prise en compte de la vie privée dès la conception du dispositif technique) et de **« privacy by default »** (paramétrage par défaut de l'application visant à assurer le maximum de protection de la vie privée) pour renforcer l'arsenal préventif, voire répressif.

Face à la multitude d'objets et applications connectés qui existent sur le marché, le développement de normes attestant des garanties offertes, notamment en matière de sécurité et de protection de données sensibles, pourrait, en outre permettre aux utilisateurs d'effectuer une sélection avisée des objets ou applications connectés.

Le degré de protection des données personnelles doit aller de pair avec l'accroissement du digital et de l'utilisation d'objets et d'applications connectés. **Dans un marché hautement concurrentiel, plus d'information du consommateur sur les objets connectés permettront de gagner la confiance du public et un avantage compétitif pour le fabricant**.

5. Donner à l'usager connecté des outils de contrôle et des « conseillers »

Face à une menace croissance, polymorphe et en provenance de pays aux législations contrastées en matière de protection sur les données à caractère personnel, l'usager peut difficilement faire face sans une protection et des tiers de confiance.

L'objectif est de pouvoir continuer à s'informer, à téléphoner, à faire du sport en utilisant des objets connectés, à disposer d'applications gratuites ou payantes, sans prendre le risque de voir ses données détenues et exploitées à des fins inconnues par des tiers non autorisés.

Pour anticiper et contrôler ces pratiques, au-delà du cadre législatif et réglementaire national ou européen, il apparaît désormais indispensable de créer les conditions pour les usagers de pouvoir s'en remettre à des tiers de confiance (encadré ci-joint) pour la protection de leurs données.

Par ailleurs, il serait même envisageable de recourir à des technologies aussi avancées que les « block-chain » pour que l'usager devienne seul détenteur de données encryptées et sécurisées.

Tiers de confiance numérique

« Editeurs de logiciels, prestataires de services, experts, professionnels réglementés, structures institutionnelles, les Tiers de Confiance du Numérique contribuent fortement à l'essor d'une digitalisation fiable et sécurisée, en élaborant de la doctrine, en produisant des référentiels et des labels, en assurant des formations expertes et universitaires, et en mettant à la disposition de chacune des personnes ou des organisations pour lesquelles ils

interviennent, des outils, des produits et des services destinés à les protéger des dangers inhérents à l'usage du Numérique, et à préserver leurs droits. » (Source FNTC).
La FNTC, acteur majeur en France et à l'étranger, née en février 2001, à la suite de la publication le 13 mars 2000 de la Loi "portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique", rassemble aujourd'hui plus de 130 acteurs de l'écosystème numérique.

La loi française du 21 juin 2004, transposant la directive européenne sur le commerce électronique, ne parle pas de tiers de confiance. Il n'y a plus de définition juridique stricte depuis l'abrogation de la loi du 29 décembre 1990 et qui donnait une définition de cette notion. Selon la FNTC, le Tiers de Confiance Numérique est reconnu par ses pairs, doit être membre d'un ordre, d'une association ou d'une fédération disposant d'une charte et d'un comité d'éthique.

Il est intègre, transparent et respecte une stricte confidentialité. Il garantit son interopérabilité avec les autres Tiers de Confiance Numérique. Il doit démontrer sa capacité de continuité de service au-delà de sa propre existence en garantissant la réversibilité de ses services.
Le Tiers de s'engage à respecter la règlementation, les normes ou labels en vigueur. Il contribue en permanence aux évolutions techniques. Il se soumet à des audits externes réguliers.

Le champ d'intervention des tiers de confiance s'est fortement élargi (e-finance, e-santé, vote électronique, "cachet électronique visible", big data, objets connectés, blockchain ...).

Si un professionnel ou un établissement de santé souhaite héberger ses données de patients chez un tiers, ce dernier doit être agréé par le ministre chargé de la santé, conformément aux articles L.1111-8 et R.1111-9 du Code de la santé publique. L'obtention de l'agrément est soumise à la mise en œuvre de solutions techniques, d'une organisation et de procédures de contrôle assurant la sécurité, la protection, la conservation et la restitution des données hébergées, et d'une politique de confidentialité et de sécurité. [21]

6. Une troisième voie : les données de prévention

Comme nous l'avons souligné, le patient demeure dépositaire du droit d'accès à ses données de santé, sans pour autant être en capacité de els comprendre et de les utiliser indépendamment des professionnels de santé. Il arrive même qu'il n'en ait même pas pris connaissance, faute de les comprendre.

A l'inverse, le patient davantage connecté et informé, souhaite « contrôler » sa santé.
Les données de bien-être produites par les objets connectés lui en donne dans une certaine mesure, l'illusion. En revanche, elles apportent à des tiers des informations précieuses sur le comportement, les habitudes, l'état physique et psychique de l'usager.

[21] Données de santé : des obligations de sécurité spécifiques pour les professionnels de la santé. Me Betty Sfez.

En revanche, pour permettre au patient, qu'il soit en bonne santé ou malade, de prendre davantage le contrôle en amont de son parcours de santé et de le comprendre, il nous apparaît essentiel de faire émerger une troisième catégorie de données médicales personnelles, à savoir <u>les données de prévention.</u>

Les données de prévention sont clairement définies dans la liste des données composant le futur Dossier Médical Partage (DMP) et le :

« Les données de prévention (les rappels de vaccin, facteurs de risques individuels, comptes rendus d'actes diagnostiques à visée préventive, calendrier des vaccinations et des actes de prévention …) ».

Cette définition pourrait être également étendue aux données image : radiographie, tomodensitométrie, imagerie par résonance magnétique, échographies. Il dispose d'un espace d'expression personnelle permettant au titulaire de porter des informations personnelles à la connaissance des professionnels de santé : sa position sur le don d'organes, par exemple, ou les coordonnées de la personne à prévenir en cas d'accident.

Les données de prévention en Allemagne

Cette notion est apparu il y a un certain nombre d'années en Allemagne.

Vorsorgedaten (les données de prévention) en Allemagne où en 1987 (Ärzteblatt, novembre 1987), il s'agissait des données concernant les prises de poids, la pression artérielle, les résultats de glycémie, le taux de protéine et d'alcool, ainsi qu'un point sur l'alimentation et l'état global de la personne.

A chaque visite, le médecin enregistre ces données permet tant ainsi une traçabilité, un suivi pour pouvoir anticiper d'éventuelles maladies. Ces données sont enregistrées sur la carte à puce de l'assuré (appelé en 1987 : passeport électronique de santé)

Ce dispositif qui a évolué jusqu'à la « loi e-health « pour renforcer l'implication du patient concernant ses données et ses traitements. Ainsi tous les acteurs du parcours de soins sont liés par un système d'infrastructure digitale (*Telematik-Infrastruktur*). Le patient de son côté, a pour la première fois la possibilité de fournir des données aux médecins, notamment de ses applications mobiles de fitness/ santé, appelées aussi « wearables ». Le médecin saura en tirer des conclusions utiles pour le dossier du patient.

Grâce aux évolutions et aux informations qu'apporte aujourd'hui le séquençage du génome, il est possible de connaître les prédispositions biologiques à certaines maladies de chaque individu, sa sensibilité à certains médicaments.

Nommée pour la première fois par le Prix Nobel de médecine, Jean Dausset en 1970, la médecine prédictive apporte à chacun de nous la capacité de disposer désormais d'un tableau de bord de sa santé.

Le coût d'un test génétique a considérablement baissé et a été recommandé par la HAS pour nombre d'applications, comme l'opportunité ou pas de suivre certains traitements comme l'abicavir, un anti-HIV.

Au-delà de la thérapie, imaginons que chacun puisse disposer de la capacité, dès son plus jeune âge, de connaître et de comprendre qui il est et comment mieux adapter en amont son activité, sa nutrition, ses habitudes.

Il va de soi que pour comprendre et mieux exploiter ces données de prévention, l'usager doit pouvoir se reposer sur son médecin traitant et le biologiste médical qui vont les analyser, les décrire et lui apporter une éducation personnalisée en santé et thérapeutique personnalisée, à partir de ces données, tout au long de sa vie.

Ces données de prévention pourraient in fine permettre au patient de mieux guider sa santé et de la comprendre, sans perdre le contrôle de l'exploitation

Il va de soi que ce dispositif appellerait un régime juridique adapté.

CONCLUSION

A l'aune de changements majeurs pour le patient, mais également pour le professionnel de santé, il apparaît déterminant d'appréhender le champ des potentiels offerts par la « e-santé » dans sa globalité, de les cartographier et de les hiérarchiser.

La « e-santé », le « M-Health », le transhumanisme doivent devenir des sujets de société et amener une doctrine européenne, partagée, tant sur les opportunités et les risques attachés à une exploration sans encadrement de nouvelles pratiques, que des attentes de l'Union européenne en matière de droit international. La Corée du Sud a de ce point de vue, apporter la preuve d'une avance et d'une maturité considérable sur ces sujets, sans mettre en danger l'usager, et sans freiner son économie.

Une approche européenne, coordonnée au niveau communautaire, devrait permettre d'inventorier les pratiques et législations dans chacun des Etats membres et chez leurs partenaires extra-européens, pour identifier les bonnes pratiques et créer les conditions d'un dialogue tant sur la question de la protection des données sensibles dans le domaine de la santé, que le cadre d'exploitation de ces données pour une recherche fondamentale ou appliquée.

ANNEXES

Club des Acteurs de la Prévention, membres du groupe de travail « e-santé » :

Monsieur Jean-François Boulat	Président Prévention, Groupe Macif
Maître Charles Casal	Avocat à la Cour, Associé chez Cheysson Marchadier & Associés
Monsieur Alain Le Meur	Biologiste médical
Maître François Marchadier	Avocat à la Cour, Associé chez Cheysson Marchadier & Associés
Monsieur Paul Piersson	DSI, Cerba Healthcare
Madame Stéphanie Pistre	Coordinatrice CADP
Madame Alice Bernard	responsable partenariats CADP
Madame Wiebke d'Amécourt	responsable évènements CADP

Sources :

- Loi de modernisation de notre système de santé, 26 janvier 2016
- Loi n°98-1194 du 23-12-1998, CSS article L161-28-1 et Arr. du 19-7-2013
- Code de la santé publique, article L 1461 -1- III et article L 6316-1
- Décret n° 2016-914 du 4 juillet 2016 relatif au dossier médical partagé
- Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
- Projet de règlement européen sur la protection des données, publié le 6 avril 2016
- Directive européenne 93/42/CE sur les dispositifs médicaux
- Rapport de la Cour des Comptes publié le 3 mai 2016, « Les données personnelles de santé gérées par l'Assurance Maladie »
- Stratégie nationale e-santé 2020 annoncée par le Ministre des Affaires Sociales et de la Santé du 4 juillet 2016
- Sondage Ipsos réalisé par Internet du 27 au 31 mai auprès de 2.000 personnes constituant un échantillon national représentatif de la population française de 18 ans et plus.
- « Le corps, nouvel objet connecté - du quantified self à la M-Santé : les nouveaux territoires de la mise en données du monde » - Cahiers IP N°2 – CNIL, 2014
- « These events – and the doubts they inspired – have contributed to a cloud of personal "data insecurity" that now looms over many Americans' daily decisions and activities » - Pew interest – 20.05.2015
- « Max Schrems, le « gardien » des données personnelles qui fait trembler les géants du Web » Pixels, Le Monde, 06/10/2015
- CJUE affaire C−362/14 - 6 octobre 2015
- Ministère du commerce : www.privacyshield.gov
- Cour suprême, affaire Schmerber c. Californie, 1966
- « Protection of personal data and security measures: towards a transatlantic perspective » Rocco Bellanova et Paul De Hert – Cultures & Conflits, n° 74, été 2009, p. 63-80
- « La sécurité des objets connectés en question après une violente attaque informatique », Martin Untersinger, Le Monde, 25/10/2016
- Babel – Actes Sud – Mars 2016
- "Des centaines de résultats d'analyses médicales accessibles sur internet", www.rue89.com, le 10/01/2012
- « Données de santé : des obligations de sécurité spécifiques pour les professionnels de la santé ». Me Betty Sfez, 21/11/2013, http://www.village-justice.com/articles/Donnees-sante-obligations-securite,15638.html#UKcL0gby9k6LZckF.99
- Site internet de la Fédération des Tiers de Confiance du Numérique https://fntc-numerique.com/fr/accueil.html
- Blockchain France, https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/
- « La Télésanté : Un atout au service de notre bien-être », Rapport Lasbordes, 2009
- « INTERVIEW Alors que la loi pour une République numérique prévoit l'ouverture des mégadonnées publiques, un projet de loi pourrait restreindre l'accès aux données publiques de santé. Explications de Jeanne Bossi Malafosse, avocate, membre du

Healthcare Data Institute. » http://www.challenges.fr/entreprise/sante-et-pharmacie/faut-il-ouvrir-les-donnees-publiques-de-sante_438527

- « Objets connectés et protection des données personnelles : le paradoxe », Olivia Luiz, CIO Online, 13/05/2015 http://www.feral-avocats.com/fr/publication/objets-connectes-et-protection-des-donnees-personnelles-le-paradoxe/
- « Eric Lombard : « L'utilisation des données personnelles n'est pas sans risque », Jacques-Olivier Martin, Le Figaro, 27/10/2016

- « Questions & réponses – Partenariat transatlantique pour le commerce et l'investissement (PTCI/TTIP – Transatlantic Trade and Investment Partnership) entre l'Union européenne et les Etats-Unis », http://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-economique-et-commerce-exterieur/accords-de-libre-echange/ue-etats-unis-le-partenariat-transatlantique-de-commerce-et-d-investissement/article/questions-reponses-partenariat-transatlantique-pour-le-commerce-et-l
- « Traité Tafta ; Bruxelles s'attend à une « pause » dans les négociations » Sud Ouest Eco, 11/11/2016, http://www.sudouest.fr/2016/11/11/traite-tafta-bruxelles-s-attend-a-une-pause-dans-les-negociations-2565425-705.php
- « Traité transatlantique : quels enjeux pour le numérique ? », Pierric Marissal, L'humanité, 29/05/2014, http://www.humanite.fr/traite-transatlantique-quels-enjeux-pour-le-numerique-538740
- « Traité transatlantique et protection des données personnelles : entre liberté et sécurité » Emmanuelle Gris, https://europe-liberte-securite-justice.org/2016/05/15/traite-transatlantique-et-protection-des-donnees-personnelles-entre-liberte-et-securite/
- « Dossier patient informatisé à visée de recherche biomédicale, Electronic health records and biomédical research » La Presse Médicale, Vol 38, n°10 octobre 2009, http://www.em-consulte.com/en/article/227341
- « Americans' attitudes about privacy, security and surveillance » Mary Madden and Lee Rainie, PewResearchCenter, 20/05/2016, http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/
- « La protection des données personnelles à la croisée des chemins », chapitre 1, Michel Gentot, Groupe d'études Société d'information et vie privée, https://www.asmp.fr/travaux/gpw/internetvieprivee/rapport3/chapitr1.pdf
- « Faire de la France un leader des données de santé », Le Monde, 12/07/2016, http://www.lemonde.fr/idees/article/2016/07/12/faire-de-la-france-un-leader-de-l-analyse-des-donnees-de-sante_4968485_3232.html

ACTEURS DE
LA PRÉVENTION

Contacts : Stéphanie Pistre
Tél. : 01.82.50.95.34
Portable : 06.20.57.33.46
Mail : *acteursdelaprevention@gmail.com*
http://les-acteurs-de-la-prevention.fr/