Objets connectés de Santé : un avenir certain, une sécurité indispensable !

Par Vincent TRELY – Président de l'APSSIS (Association pour la Promotion de la Sécurité des SI de Santé)

Auto mesure, quantified self, high tech qui soigne ou plus simplement objets connectés de santé constituent de nombreuses appellations qui reflètent la difficulté à cerner ce nouveau phénomène. De la simple application santé / bien-être (environ 100 000 applications médicales dont 13000 francophones sont téléchargeables gratuitement ou pour quelques euros et 15% le sont à destination des professionnels de santé) à la balance qui surveille votre poids et la qualité de l'air, au pacemaker connecté, la marche est grande et les enjeux ne sont pas les mêmes. Qu'un jogger qui possède un bracelet connecté reçoive des publicités intempestives pour des boissons dynamisantes (même si la grande majorité des industriels français s'est engagée à ne pas vendre à des fins commerciales les données recueillies) ou qu'il se fasse pirater ses données sur « runstatic » n'émouvra personne mais si le hacker touche au glucomètre d'un patient diabétique, c'est la panique. Tout le monde criera au scandale et au manque de sécurisation de ces objets. Car c'est là le problème. Un objet connecté est ouvert sur le monde et donc faillible. Lors du Congrès national de sécurité des SI, Philippe Loudenot, FSSI des Ministères es Affaires Sociales et de la Santé, en a d'ailleurs fait la démonstration en simulant l'explosion d'un pacemaker communicant, assez facilement. On rappellera que 7 millions de français ont été victime de cybercriminalité en 2013 (source Norton Symantec) et ce chiffre devrait ne pas diminuer avec l'apparition de ces nouveaux objets connectés. Les voitures, les systèmes de vidéo-surveillance sont déjà la cible de hackers, pourquoi pas demain nos tensiomètres ou nos pompes à insuline ?

Sommes-nous prêts ? Ne sommes-nous pas des apprentis sorciers ? La technologie ne va-t-elle pas trop vite ?

5.67 millions de français possèdent déjà un objet connecté lié à la santé et selon les estimations, ce chiffre doublera d'ici 2017. 50% des français qui possèdent un objet connecté déclarent vouloir surveiller et améliorer leur santé par eux-mêmes (étude Ifop – Atelier BNP Paribas 2013). Pour environ 80% des français, les nouvelles technologies (internet, applications et outils

connectés) pourraient améliorer le suivi des séniors à leur domicile (Baromètre BVA Orange Healthcare MNH en partenariat avec le Figaro santé). On pourrait évoquer l'étude d'IDS Santé qui a démontré que l'utilisation d'un coach sportif par les participants avait favorisé leur activité physique, réduit leur IMC et que la connectivité (échange et partage de données entre participants) était un fort levier de motivation. Les « pros – objets connectés » avanceront avec raison les avantages liés à la prévention. Contrôler sa tension, repérer soi-même ses grains de beauté suspects, maitriser son alimentation, aider à la surveillance des maladies chroniques… le tout permettant d'anticiper d'éventuels problèmes et, le cas échéant, d'être pris en charge plus rapidement. Le patient est responsabilisé, impliqué mais cela ne risque-t-il pas de se retourner contre lui ? D'un point de vue humain tout d'abord, avec un risque anxiogène (prises de mesures intempestives, stress lié à la non compréhension des données, hypocondrie) et d'un point de vue sociétal par ailleurs, avec l'apparition actuelle des premiers bonus / malus de santé que l'on trouvera dans de multiples secteurs : « tu savais que ton cholestérol était trop élevé et tu n'as rien fait ! Donc tu es responsable de tout ou partie des conséquences ». Christophe Deshayes dit, dans son petit Traité du Bonheur 2.0 **:** ***«*** *si responsabiliser l'individu sur la gestion de son propre capital santé est un progrès, que ce soit pour lui-même ou pour les finances de la collectivité, cela ne va pas sans poser des questions cruciales. Que ferons-nous par exemple de ceux qui ne feront pas ces efforts soit parce qu'ils ne le veulent pas soit parce qu'ils ne le peuvent pas ? »*

Une autre problématique touche à l'essence même de ces objets. Ce sont des objets connectés « de santé ». Prendre sa température avec son smartphone, pourquoi pas ! Le transformer en laboratoire d'analyse (taux de cholestérol et de sucre), soit ! Mais ensuite, que faire de ces données ? Se rendre chez son médecin pour l'informer de nos mesures ? Comment le médecin pourra considérer ces mesures prises hors du parcours de soin classique ? Pourra –t-il se fier au système de calcul alors qu'aujourd'hui, il n'y a aucun label, aucun contrôle sur ces outils de mesure en accès libre sur internet? Que dire à une patiente qui se rendrait chez son médecin avec les mesures prises par son échographe personnel ? Le Docteur Jacques Lucas fournit une première piste de réponse : « *Pour toute avancée, la limite n'est pas au niveau de la science ou de la technologie mais au niveau du bon usage adapté. Si ce dispositif est*

prescrit et inséré dans un projet partagé de suivi de la patiente, celle-ci utilisera le dispositif dans les indications que le médecin aura proposé. Le médecin n'est pas seulement un interprétateur d'image ou d'une donnée fournie (…) Si la patiente, séduite par l'offre commerciale, achète d'elle-même ce dispositif et demande ensuite une interprétation, ce n'est plus dans une relation médicale ». La santé n'est pas qu'une mesure, qu'une image à un moment donné. Elle englobe l'histoire du patient, ses antécédents… Il est parfois bon de le rappeler !

L'ultime question n'est pas de savoir si on est pour ou contre car c'est irréversible. Les statistiques annoncent la présence de plusieurs milliards d'objets connectés (tout confondus) dans le monde d'ici 2020. Mais celle de savoir comment encadrer ces nouvelles pratiques car comme le souligne la CNIL : « *il s'agit de données d'un nouveau genre. Ce sont des « données issues du corps », communiquées volontairement par les individus et qui peuvent paraitre anodines (nombre de pas, poids…). Pourtant, par leur accumulation et par leurs analyses combinées avec d'autres données, elles peuvent révéler un état physique ou mental anormal. Donc ces données sont tout aussi sensibles que s'il s'agissait de données médicales « traditionnelles ».* Et comment s'approprier ces outils qui ne doivent pas se substituer à l'avis médical mais venir en complément, en support. Pour le docteur Nicolas Postel-Vinay: « *ces objets peuvent apporter des informations pertinentes et exploitables, améliorant la qualité de décision* », sous-entendu donc que la décision finale de traitement ou de diagnostic revient au médecin !

On comprends bien à ce stade qu'au delà de la sécurité, de nombreuses questions de société se posent en parallèle. Plusieurs révolutions se précisent, qui impacteront nos comportements et notre rapport à la santé. Entre l'époque de la sacro-sainte blouse blanche, unique source de la connaissance et profondément respectée en tant que telle, et une nouvelle ère où le Médecin peut devenir un simple prescripteur pour citoyens éduqués, cherchant et partageant des données médicales et « s'autogérant », il faudra trouver un juste équilibre. Entre les millions d'objets et d'applications qui nous seront proposées ces prochaines années, lesquelles deviendront pour nous indispensables, au même titre que le réfrigérateur, le sèche-linge et la box Internet ? Lesquelles amélioreront vraiment notre quotidien et tout

particulièrement celui des malades ou des plus vulnérables (enfants, personnes âgées) ?

Isabelle LANDREAU, Avocat au Barreau de Paris, nous dit : « Les objets connectés dans le domaine de la santé vont révolutionner notre approche de la santé avec l'arrivée massive de données prédictives. L'individu est au cœur de cette évolution où il devient "objet" lui -même. Nous devons veiller à ce que l'humain connecté par des objets l'aidant dans sa vie physique, mentale, psychique, affective ne cesse pas d'être un sujet de droit. Pour cela, il faut veiller i) d'une part à la sécurisation des données afin d'éviter une manipulation à distance de ces données et une marchandisation par le secteur privé qui s'annonce inéluctable et d'autre part ii) au respect des données à caractère personnel. L'avenir est entre nos mains et les associations ont un rôle important à jouer pour la défense de ces droits. »

Après la technologie et le droit, les ouvertures et les formidables avantages que nous offriront les vainqueurs de la course, qu'exigera-t-on en terme de sécurité ? Rien de moins que l'usuel, que le classique DICP. Je vais volontairement donner un ordre d'importance dans cette courte liste d'exigences et cet ordre est bien entendu discutable. L'objet traitant des données médicales et effectuant des calculs devra **avant tout être parfaitement intègre**. Sans intégrité, pas de confiance. Sans confiance, pas d'usage. La cause majeure des échecs de certains projets de santé vient du manque de confiance accordé aux outils. Si 2 et 2 font 5, même une seule fois, le rejet d'un progiciel de type circuit du médicament informatisé est immédiat. Il en sera de même pour le patient « connecté ».

L'objet étant devenu indispensable, **ses fonctionnalités devront être disponibles en permanence**. Si l'on pense aux objets connectés qui seront directement liés au traitement d'une pathologie (diabète, cœur, implants de diffusion de médicaments), il sera un jour vital que leur disponibilité soit totale.

La société évolue sur le concept de confidentialité. Je pense qu'elle évolue vers une transparence relative sur laquelle je ne porte aucun jugement, mais que je constate. Le comportement des jeunes générations qui sont entrées dans une dynamique de partage de pans entiers de leurs vies « privées » avec les autres peut constituer le signe avant-coureur d'une forme de libéralisation

de la donnée personnelle et de la redéfinition de son contexte. Aujourd'hui, notre société est encore obsessionnelle sur les concepts de l'argent et de la santé en particulier. Qu'en sera-t-il demain ? Néanmoins, avant de parier sur l'avenir, il faut traiter le présent et le désir de confidentialité est bien là. L'objet connecté et tout son environnement (liaisons, serveurs, applications, flux d'échanges) doivent **assurer à l'utilisateur un haut niveau de confidentialité** concernant les données qu'il souhaite garder confidentielles, à minima.

Dans le cadre du contrôle, effectuée par les autorités compétentes, et dans celui du juridique (besoin de preuves en cas de litiges), les objets connectés devront **assurer une traçabilité de leurs propres actions et de celles réalisées par leurs administrateurs ou par leurs usagers**. Il ne peut en être autrement sauf à valider le chaos, ce qui n'est pas le propos.

Il reste ensuite 2 autres questions essentielles : où sont les données de santé produites par les objets et quelle est ou quelles sont leur(s) finalité(s) ? Certaines alimenteront consciencieusement des bases de données d'open data, utiles au prédictif et à la recherche, entre autres, d'autres alimenteront les industries du secteur, des laboratoires pharmaceutiques aux compagnies d'assurance ou pire, permettront une sorte de surveillance permanente et malsaine de masses de population.

Qui aujourd'hui valide cet ensemble de prérequis ? Quel laboratoire français officiel (public, privé ou les deux) labellise les objets connectés, afin que seuls ceux ayant subi les batteries de tests nécessaires ne puissent être mis sur le marché ? A ma connaissance, ce laboratoire n'existe pas encore mais je suis convaincu qu'il aurait de l'avenir.

Lorsqu'il m'arrive de m'exprimer devant des amphithéâtres d'étudiants, je n'oublie jamais de leur rappeler que la sécurité de l'information a un bel avenir devant elle et qu'il ne serait pas idiot de s'orienter vers cette passionnante discipline. La sécurité constitue l'un des socles du développement massif des technologies numériques, c'est sans appel...