Conseil national de la Consommation *Le 07 Juillet 2017*

Rapport du Conseil national de la consommation sur les objets connectés en santé

En France, le marché des objets connectés est estimé à 150 millions d'euros en 2013[1]. Il comprend principalement les branches de la santé, du bien-être et de la domotique avec respectivement 60 millions pour les deux premiers secteurs et 90 pour le second.

Les objets connectés sont devenus une partie intégrante de la télésanté, qui elle-même au côté des systèmes d'information de santé et de la télémédecine forment ce qui est aujourd'hui communément appelé « la santé connectée ». La télésanté, parfois appelée « m-santé » regroupe à la fois des objets connectés mais aussi des applications santé ou bien-être utilisables sur smartphones, montres ou encore tablettes numériques.

Mesure de l'activité physique, suivi de la glycémie, mesure de l'observance, prise de tension en continu ou encore avertissement de la présence d'un objet blessant dans la chaussure d'un diabétique, la connexion simplifie l'auto mesure et modifie la manière dont les données vont pour voir être analysées. Cela garantit un meilleur suivi de l'état de santé et permet de partager les résultats avec les professionnels de santé ou son entourage. Concrètement, un ensemble d'appareils connectés récupère des données qui, grâce à la connexion Bluetooth, va directement dans les téléphones, les tablettes ou ordinateurs. Ces données sont ensuite stockées dans un *cloud* en principe sécurisé et sont accessibles à tout moment pour le consommateur/patient ou aux professionnels de santé. Ces technologies modifient notre rapport au corps, à notre santé et viennent interroger l'équilibre et le fonctionnement actuel de la relation usager/professionnel de santé. Les informations enregistrées par ces objets peuvent également être récupérées par des entreprises opérant dans le secteur de la recherche en santé.

En France, le marché des objets connectés est encore peu développé et principalement orienté vers la prévention et l'accompagnement des patients. Cependant, il s'agit d'un secteur prometteur et en pleine expansion, dont il convient donc d'accompagner le développement[2].

---

[1] Selon une étude Xerfi

[2] Le marché de la m-santé représenterait $ 26 Mds en 2017, cet essor étant notamment manifeste s'agissant de la création des applications mobiles de santé (6 000 en 2010, 20 000 en 2012 et 168 000 en 2015). A l'intérieur de ce vaste secteur, près de 11.000 applications seraient dédiées, en France, à la santé/médecine, soit une part relativement modeste. La majorité des applications relèvent plutôt de la sphère du bien-être et ont un intérêt médical marginal. Obéissant à un « effet de mode » elles sont rapidement délaissées après leur téléchargement. Il en est de même s'agissant des objets connectés appartenant à la sphère du bien-être. A l'inverse, les 20 applications les plus populaires (sport, remise en forme, et santé combinés) comptabilisent 231 millions de téléchargements dans le monde.

D'après une étude réalisée par le SNITEM les applis les plus populaires de l'App Store sont pour la catégorie « médecine », les applis délivrant de l'information aux professionnels et aux patients, ainsi que sur la santé de la femme (grossesse…). S'agissant des applications enregistrées dans la catégorie « forme et santé », les applications de fitness et de minceur sont les plus téléchargées.

Le consommateur d'objets connectés en santé est susceptible d'être confronté à trois grandes problématiques :

- Le réglementaire : quel est le statut de ces objets, quelle règlementation leur est applicable, qui en assure le contrôle et vers qui se retourner en cas de litige ? De par leur fabrication et leur mode de fonctionnement, les objets connectés sont à la fois des produits (comportant eux-mêmes une partie physique et une partie logicielle) et des prestations de service (traitement et retransmission de données). Par ailleurs, si la plupart sont des produits de consommation courante, certains d'entre eux peuvent relever de réglementations particulières comme celle applicable aux dispositifs médicaux. Le consommateur est donc amené à évoluer dans un paysage règlementaire complexe en la matière.

- La fiabilité : 'l'objet connecté que j'achète est-il fiable, conforme aux allégations qu'il affiche et va-t-il le rester dans le temps ? Il est important de déterminer dans quelle mesure l'objet connecté doit être conçu et/ou règlementé de manière à garantir l'utilisateur contre les défauts de conformité ou de sécurité tant des objets que des prestations associées.

- La protection des données : les données recueillies par l'objet connecté sont-elles protégées ? Comment sont-elles stockées ? Le respect de ma vie privée est-il garanti et plus largement la sécurité informatique de cet objet est-elle garantie de sorte qu'il ne puisse être piraté ? Quelle utilisation par un tiers ? quel droit à l'oubli ? …

Fort de ces interrogations et à la demande de Madame Martine Pinville, Secrétaire d'Etat en charge de la consommation, le CNC a constitué un groupe de travail chargé de procéder à une analyse du marché de ces nouveaux objets. Le mandat rendu le 4 février 2016 précise que les travaux devront s'articuler autour des trois axes prioritaires répondant aux interrogations des consommateurs rappelées ci-avant : quel est le statut des objets connectés en santé, comment garantir leur conformité et la loyauté de leurs allégations, et comment assurer la protection des données personnelles qu'ils recueillent.

La présidence du groupe de travail a été confiée à Madame Raphaëlle BOVE, chef du bureau des produits, prestations de santé et des services à la personne à la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF). Le collège des professionnels a désigné comme rapporteur, M. Jacques SAINCTAVIT (MEDEF) et Mme Julie Macaire (FIEEC). Le collège des consommateurs a désigné M. Vincent PERROT (CLCV).

Les travaux du groupe se sont tenus à la suite ou de manière concomitante à d'autres groupes de travail créés sur le même sujet. L'Ordre des médecins, la Commission nationale de l'informatique et des libertés (CNIL) ou encore la Haute Autorité de santé (HAS) avaient déjà tous élaboré des livres blancs ou référentiels sur cette problématique. Une grande partie de ces travaux, abordant chacun d'un point de vue différent ce sujet, a été exposée au groupe du travail ce qui a permis une acquisition plus rapide des diverses thématiques notamment juridique et technique.

De nombreuses réflexions sont également engagées au niveau communautaire sur ce sujet. Une consultation publique a ainsi été lancée en 2014 afin d'identifier les freins au bon développement de ce secteur. De leur côté et avec le soutien de la Commission, les industriels ont élaboré un code de conduite en cours de validation par le G29, qui détermine les critères principaux devant être respectés au moment de la conception de ces objets afin de protéger les consommateurs et ainsi préserver leur confiance en ces nouvelles technologies. Un guide de bonnes pratiques concernant la collecte de données par les objets connectés a également été élaboré sous l'égide de la Commission et devrait prochainement être diffusé à l'ensemble des Etats-membres pour une mise en œuvre qui se fera sur la base du volontariat.

S'agissant plus particulièrement de la France, le groupe de travail mis en place par le CNC a pu également se nourrir des réflexions ayant eu lieu au sein du groupe travail dit « GT28 » mis en place dès

le mois de septembre 2015[3], dans le cadre du conseil stratégique de filière des industries et technologies de santé (CSF) dont le rapport est paru à la fin de l'année 2016.

Ce groupe de travail principalement piloté par le ministère chargé de la Santé avait également pour finalité d'élaborer des recommandations permettant d'assurer la protection des consommateurs, usagers et professionnels de santé, dans leur utilisation des objets connectés et applications mobiles de santé, mais aussi de proposer des modalités de promotion des solutions technologiques à « bénéfice avéré ».

Comme exposé ci-avant, le groupe de travail du CNC s'est quant à lui focalisé sur la seule problématique de la protection des consommateurs, dans le but d'élaborer des recommandations propices à faciliter le développement de ces objets dans un climat de confiance, étant entendu que ces produits font naitre de grands espoirs notamment pour les patients, dans le suivi de certaines pathologies chroniques.

Le groupe s'est réuni à 8 reprises entre avril 2016 et janvier 2017 et les discussions ont permis d'aboutir à un accord des deux collèges qui fera l'objet d'un avis du CNC.

1) Objets connectés en santé : quel statut et quelle règlementation applicable ?

Les objets connectés en santé sont particulièrement protéiformes (tensiomètre, brosse à dent, pilulier, fourchette, balance, …) et oscillent dans leur destination d'usage entre la sphère du bien-être et la sphère médicale.

Suivant la destination qui lui est assignée, un même objet pourra être considéré comme un bien de consommation courante ou alors qualifié, ou qualifiable de dispositif médical, catégorie particulière de produits de santé encore mal connu du grand public.

Les auditions menées par le groupe de travail, notamment de l'Agence nationale de sécurité du médicament et des autres produits de santé (ANSM), de la DGCCRF, de l'Association française de normalisation (AFNOR) ou encore du Laboratoire national de métrologie et d'essais (LNE), ont mis en exergue le caractère complexe et éclaté des différents cadres règlementaires et législatifs applicables aux objets connectés en santé.

Les objets connectés partagent tous les caractéristiques communes suivantes, il s'agit d'équipements :
- dotés de capteurs (micro, caméra, GPS, etc.),
- capables de communiquer avec leur environnement proche ou lointain (*cloud*),
- disposant de ressources relativement limitées en termes d'autonomie, d'énergie et de réseau,
- dont les moyens d'interaction avec l'utilisateur sont rudimentaires, voire inexistants.

S'agissant des objets connectés de la sphère « santé » (incluant le bien-être), ils peuvent être regroupés en trois grandes catégories : les dispositifs médicaux déjà existants auxquels ont été ajoutés uns connectivité (tensiomètre, glucomètre…), les objets grand public de mesurage ou autres auxquels ont été ajoutés une connectivité (, balance…) et les réelles innovations.

1.1- Statut des objets connectés en santé : dispositifs médicaux ou non

Les dispositifs médicaux (DM) sont une catégorie de produits de santé au sens de l'article L.5311-1 du code de la santé publique, au même titre que les médicaments ou encore que les produits cosmétiques. Ils obéissent à une règlementation communautaire harmonisée, mise en œuvre par les directives 93/42/CEE et 90/385/CEE transposées en droit national dans le code de la santé publique aux articles L.5211-1 et suivants et R.5211-1 et suivants. Ces directives seront prochainement remplacées par un

[3] Cf. Annexe 1 – Présentation des travaux du GT28 au groupe de travail

nouveau règlement communautaire qui sera mis en œuvre dès sa parution en 2017 avec une période de transition de 3 ans.

Le dispositif médical répond à une définition stricte. Aux termes de l'article L.5211-1 « *On entend par dispositif médical tout instrument, appareil, équipement, matière, produit, à l'exception des produits d'origine humaine, ou autre article utilisé seul ou en association, y compris les accessoires et logiciels nécessaires au bon fonctionnement de celui-ci,* ***destiné par le fabricant*** *à être utilisé chez l'homme à des fins médicales et dont l'action principale voulue n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens. Constitue également un dispositif médical le logiciel destiné par le fabricant à être utilisé spécifiquement à des fins diagnostiques ou thérapeutiques. (…)* ».

Les fabricants et distributeurs de dispositifs médicaux sont soumis à un certain nombre d'obligations règlementaires. Ainsi, le fabricant est responsable de la mise sur le marché de son dispositif dont il doit démontrer la conformité aux exigences dites essentielles, attestée par la présence d'un marquage CE. Ces exigences générales sont destinées à garantir la sécurité et la santé de l'utilisateur –consommateur, malade, professionnel - et des tiers. Ces dernières sont assorties d'une démonstration de performance et d'une justification des bénéfices par rapport aux risques liés à l'utilisation. Pour cela, le fabricant peut s'appuyer sur un certain nombre de normes harmonisées au niveau européen. Enfin, dès l'instant où ce dernier applique une de ces normes, une présomption de conformité au regard des exigences essentielles couvertes par la norme, lui est octroyée.

Les DM sont classés suivant le niveau de risque lié à leur utilisation en 4 catégories : I, IIa, IIb et III. Pour les DM de risques faibles en classe I, le fabricant peut s'auto-certifier. Pour les autres classes, il doit obtenir son marquage CE en faisant contrôler son produit par un organisme notifié se trouvant dans l'Union européenne. En France, le LNE-GMED (organisme de certification dans le domaine médical et santé) est le seul organisme notifié. Il intervient notamment dans la certification des tensiomètres connectés.

Les fabricants et distributeurs de dispositifs médicaux doivent se déclarer en France, auprès de l'autorité sanitaire compétente pour ces produits, en l'espèce l'Agence nationale de sécurité du médicament et des autres produits de santé (ANSM). Néanmoins, il convient de rappeler que les DM à l'inverse des médicaments, ne nécessitent pas d'autorisation de l'autorité compétente avant d'être mis sur le marché.

Les fabricants et distributeurs sont enfin astreints à surveiller le comportement des produits qu'ils mettent en vente sur le marché et à faire remonter dans le cadre du système de matériovigilance (également piloté par l'ANSM), tout effet indésirable grave dont ils auraient été informés. Contrairement ici encore aux médicaments, il n'existe aucun monopole de délivrance ou de vente des DM, à l'exception des produits d'optique correctrice, des audioprothèses et de certaines prothèses ainsi qu'orthèses, lesquels peuvent être vendus via tous les canaux de distribution.

Le nom respect de ces obligations est le plus souvent qualifiable de délit et sanctionné au niveau pénal par de lourdes peines notamment d'amendes mais aussi d'emprisonnement. Nombre de ces infractions se doublent également de manquements administratifs pouvant être sanctionnés financièrement par l'ANSM.

En France, la surveillance du marché des DM est assurée de manière conjointe par l'ANSM et la DGCCRF. Aux termes d'un protocole de coopération revu et signé pour la dernière fois en janvier 2015, ces deux autorités ont convenu que l'ANSM cible en priorité ses contrôles sur les DM les plus à risque et notamment les DM implantables. La DGCCRF quant à elle, se charge plus spécifiquement du contrôle des DM vendus en direct au grand public, et généralement de risque moindre.

S'agissant des contrôles de qualité et de sécurité des produits, ces deux autorités exercent leur mission de surveillance au moyen d'un certain nombre d'informations rendues obligatoires lors de la mise sur le marché. Ainsi, il existe une liste complète de l'ensemble des dispositifs médicaux des classe II a, II b et III mis en service pour la première fois sur le territoire français. S'y ajoute un enregistrement de l'ensemble des fabricants et distributeur français des dispositifs médicaux. Cette surveillance s'appuie également sur un recueil de l'ensemble des incidents de vigilance (environ 15.000 incidents[4] par an recensés en France). Les professionnels représentent également une source d'informations pour les autorités.

Sur la base de ces éléments mais également de l'analyse des plaintes pouvant leur être parvenues ou des grandes tendances de consommation, l'ANSM et la DGCCRF diligentent des campagnes de contrôle sur le secteur des DM. Les contrôles peuvent être réalisés sur un type de produits en particulier ou sur un mode de distribution. Au moment du lancement du groupe de travail, aucune campagne de contrôle n'avait été lancée en matière d'objets connectés en santé. La DGCCRF pour sa part, ne recensait aucune plainte ou signalement dans ce secteur.

S'agissant plus particulièrement du contrôle des allégations et des publicités portées par les dispositifs médicaux, la DGCCRF reste compétente d'une manière générale pour intervenir au titre de la tromperie ou des pratiques commerciales trompeuses définies dans le code de la consommation. Cependant, concernant les règles strictes applicables à la publicité pour les DM (article R.5213-1 et suivants du code de la santé publique) – obligation de mentionner qu'il s'agit d'un DM, de mettre le nom du fabricant, interdiction d'indiquer qu'un état de santé normal peut être affecté par une non-utilisation du DM, interdiction de suggérer qu'un état de santé normal peut être amélioré par l'utilisation d'un DM, interdiction de s'adresser exclusivement ou principalement aux enfants, interdiction de se référer à une recommandation de scientifiques ou de professionnels de santé…- seule le directeur général de l'ANSM est habilité à intervenir.

Le contrôle et la régulation de ce marché s'avère complexe pour les autorités de surveillance du fait du nombre très important de nouveaux objets et applications mis en vente[5] et de l'émergence de nouveaux acteurs économiques ne connaissant pas particulièrement le secteur de la santé et de fait son cadre règlementaire.

Les entreprises qui proposent des applis sont en effet majoritairement des PME-TPE. 40 % de l'offre du top 500 des objets en santé mobile et connectée provient de professionnels de santé, de patients ou de leur entourage. Les grands groupes industriels ne représentent que 12 % du nombre. Or, quasiment la moitié des entreprises qui commercialisent des applications sont issues du monde informatique alors que les industries de santé « traditionnelles » représentent entre 10 et 15% du marché. Tous acteurs confondus, on observe que la moitié des entreprises produisant des applications ont sorti leurs premiers produits il y a moins de 3 ans ce qui explique l'immaturité du marché.

Le marché des objets connectés en santé est donc extrêmement versatile et difficilement contrôlable. Son rythme d'évolution interroge la manière dont jusqu'alors les autorités pouvaient assurer la surveillance de ce marché. De plus, le caractère transfrontalier du marché (sur le top 500 des applications, seulement 30 % sont émises depuis la France) rend quasi impossible le contrôle des éditeurs localisés à l'étranger.

[4] Selon l'ANSM, très peu de signalements sont faits concernant des DM connectés. Par ailleurs la plupart de ces signalements concernant des problèmes de fonctionnalité liés à l'appareil et non de connectivité.
[5] A titre d'exemple un algorithme automatisé de veille à finalité santé et bien-être présente un turnover quotidien de 1%. En trois mois son marché s'est donc renouvelé.

Il n'en demeure pas moins qu'à l'issue des auditions réalisées, le groupe de travail s'est dit convaincu de la pertinence de la règlementation applicable aux dispositifs médicaux. Jusqu'alors, celle-ci a permis d'assurer la conformité et la sécurité des objets connectés DM mis le marché. S'agissant des problématiques spécifiques de protection des données et de cybersécurité qui n'étaient pas prises en compte par la directive 93/42/CEE, le groupe a également acté que celles-ci seraient gérées dans le cadre du futur règlement lequel renvoie vers le nouveau règlement applicable à la protection des données personnelles adopté le 14 avril 2016, et qui sera applicable en 2018.

A défaut d'être DM, l'objet connecté est considéré comme un objet de consommation courante auquel ne s'applique en conséquence aucune règlementation particulière. Les fabricants et distributeurs de ces objets doivent cependant répondre aux exigences minimales de la directive 2001/95/CE relative à la sécurité générale des produits laquelle impose aux fabricants et distributeurs de mettre en vente des produits sûrs pour les consommateurs. Dans certains cas, les objets en cause doivent également répondre aux obligations applicables en matière de produits électriques ou émettant des ondes électromagnétiques.

De manière assez schématique, il est donc apparu au groupe de travail qu'en fonction de leur statut, DM ou non DM, les objets connectés en santé assuraient des niveaux non-équivalents de sécurité et de protection pour le consommateur, le statut de DM assurant des garanties supérieures. Ce constat pourrait être légitimé par le fait que les DM sont utilisés à des fins médicales, alors que les objets non-DM se limiteraient à la sphère du bien-être où par nature les attentes et donc les risques seraient moindres. Il est cependant apparu au groupe que cette catégorisation était assez réductrice et non-conforme à la réalité du marché dans lequel existe une importante zone dite « grise » d'objets ou d'applications non DM pouvant cependant avoir de réels bénéfices pour la santé des consommateurs et pour lesquels le niveau d'exigence en termes de fiabilité notamment des données recueillies et de l'analyse qui en est faite, devrait être aussi important que pour les objets classés en DM.

1.2- Objets connectés en santé : la zone grise

Deux écueils ont pu être identifiés concernant la problématique du statut des objets connectés en santé vis-à-vis de la protection des consommateurs : le fait d'une part que le fabricant décide lui-même de la qualification de son produit en DM ou non selon la finalité revendiquée, et d'autre part, que les consommateurs mais également des professionnels de santé méconnaissent l'environnement règlementaire entourant ces produits et notamment les spécificités des dispositifs médicaux par rapport aux produits de consommation courante ou aux produits électriques standards.

Concernant les objets connectés et les applications dites non DM, on peut distinguer, d'une part, les solutions de bien-être, coaching, maintien en bonne santé, et d'autre part, les solutions de santé. Cette seconde catégorie constitue une « zone grise » de solutions qui ont un bénéfice pour la santé mais que leurs fabricants ne destinent pas pour autant à une utilisation à des fins diagnostique et/ou thérapeutique.

Cette zone grise nécessite une vigilance particulière des autorités afin notamment de lever les ambiguïtés entourant certaines revendications d'usage ou allégations. En la matière, quatre cas de figure courant se retrouvent :

- Le fabricant met en avant de réelles allégations médicales fondées, sans pour autant présenter son produit comme un DM par méconnaissance de la règlementation. Dans ce cas, les autorités lui demandent de certifier son produit et de respecter les obligations propres aux dispositifs médicaux ;
- Le fabricant met en avant de réelles allégations médicales fondées, sans pour autant présenter son produit comme un DM alors qu'il connait la règlementation. Dans ce cas, les autorités lui demandent

de certifier son produit et généralement sanctionnent l'opérateur pour mise sur le marché d'un DM sans certification ;
- Le fabricant met en avant des allégations médicales ou de santé non justifiées aux fins de mieux positionner son produit d'un point de vue marketing. Dans ce cas, les autorités interviennent pour faire enlever les allégations trompeuses ;
- Le fabricant met sur le marché son objet ou son application sous le statut de DM également pour privilégier un certain positionnement marketing de son produit (positionnement médical « dur ») alors que le produit n'a en réalité aucune finalité médicale. Dans ce cas il s'agit d'un marquage en qualité de DM indu et les autorités interviennent pour repositionner le produit en demandant également une révision des allégations revendiquées.

Dans les ciblages qu'elles opèrent, les autorités de surveillance privilégient le contrôle des objets et applications les plus à risque, à savoir ceux se présentant comme ayant des capacités de monitoring, de traitement ou de diagnostic de maladies. Lorsque les DM doivent faire l'objet d'une certification par un organisme notifié, ces organismes opèrent alors un contrôle préalable et obligatoire sur la qualification du produit afin d'en vérifier le statut. Néanmoins un tel contrôle n'est pas effectué pour les DM de classe I auto-certifiés. Dans ce dernier cas, les fabricants d'objets et applications peuvent, pour qualifier leur produit, s'aider des lignes directrices édictées par la Commission européenne à cette fin (MEDDEV). Pour les cas les plus litigieux, c'est au comité chargé des produits « borderline » qu'il appartient de se prononcer.

Ces constats n'ont pas conduit le groupe de travail à solliciter la modification des règlementations en vigueur, le groupe considérant que celle-ci était suffisante. Cependant, il a semblé nécessaire d'analyser plus avant les mesures prises ou pouvant être mises en œuvre pour mieux réguler la « zone grise ».

Si l'ANSM et la DGCCRF tentent au travers de leurs contrôles d'assurer ce travail, force est de constater comme relevé à plusieurs reprises par la présidente du groupe, que ce travail est rendu particulièrement fastidieux et de fait peu efficace, en raison de l'absence de lignes directrices concernant les allégations pouvant être ou non portées sur les objets et applications non-DM. Certaines règlementations comme celle relative aux compléments alimentaires, listent de manière précise et positive les allégations de santé pouvant être portées par tel ou tel produit. Or, en cette matière il n'existe aucune consigne claire mais juste de l'analyse au cas par cas, quand bien même un cadre strict existerait en matière de publicité pour les dispositifs médicaux ou pour certains produits émettant des ondes, comme rappelé par l'Autorité de régulation professionnelle de la publicité (ARPP) auditionnée.

Cette analyse au cas par cas, ne permet pas de dégager de « doctrine » pour faciliter et de ce fait massifier les contrôles d'allégations. Elle ne permet pas en outre, de fixer de règles claires pour les fabricants et distributeurs dans leur stratégie marketing[6]. Jusqu'à l'entrée en vigueur de la loi n°2011-2012 du 29 décembre 2011, une commission spéciale était chargée au sein de l'ANSM, de se prononcer sur les revendications des objets, appareils et méthodes présentés comme bénéfiques pour la santé. Cette commission en quelques sortes permettait d'élaborer quelques grands principes. Cependant depuis 2011 cet organe a été supprimé. .

La DGCCRF, par la voix de la présidente du groupe, a proposé, qu'il soit recommandé d'instaurer la mise en place de telles « guidelines » encadrant les allégations de santé portées par les objets et applications non-DM afin de mieux réguler cette zone grise. La DGCCRF a également proposé qu'il soit recommandé d'élargir sa compétence au contrôle des dispositions propres à la publicité des dispositifs médicaux (articles R.5213-1 et suivants du code de la santé publique) afin d'élargir son champ d'intervention et de venir en complément des actions menées a posteriori par l'ANSM. Ces deux recommandations n'ont pas été retenues en l'état par le groupe de travail, ne serait-ce que parce que la DGCCRF manque déjà de personnel pour les contrôles sous sa compétence actuellement. .

[6] Une telle difficulté d'analyse a également été relevée par l'AFNOR ou encore le LNE-GMED au cours de leurs auditions.

Afin de mieux orienter et protéger le consommateur dans cette « zone grise », il est apparu nécessaire au contraire, de renforcer la culture des consommateurs concernant ces objets, mais également celle des professionnels de santé qui les conseillent. Les réseaux sociaux pourraient être un bon moyen de permettre cette connaissance.

Les auditions réalisées par le groupe de travail ont mis en exergue le fait que la très grande majorité des membres des deux collèges ignorait ce qu'était un dispositif médical, ses caractéristiques et les obligations entourant sa mise sur le marché. Une difficulté est également apparue concernant les risques de confusion pour le consommateur entre les différents marquages CE existants (confusion entre marquage CE produit électrique et un marquage CE pour un DM). **Le groupe a donc estimé qu'il était primordial d'informer les consommateurs au sujet de ces produits afin de les aider à mieux orienter leur choix en leur faisant notamment comprendre que les garanties apportées par un objet connecté non-DM n'étaient pas forcément les mêmes qu'un objet connecté DM, quand bien même ces deux objets seraient quasi-identiques. .** S'agissant des confusions entre les différents marquages, cette difficulté sera résolue suite à l'entrée en vigueur du nouveau règlement DM qui prévoit la création d'un marquage « CE médical ».

Dans un second temps, le groupe a considéré qu'il était primordial afin de garantir l'équilibre de la relation patient/professionnel de santé, que le professionnel de santé soit en mesure de répondre aux questions de son patient, et de l'orienter vers l'achat de l'objet ou de l'application la plus adéquate pour répondre à ses attentes médicales. Or, ici encore, les auditions réalisées par le groupe lui ont permis de comprendre que ces objets étaient fort peu connus des professionnels de santé eux-mêmes, à l'exception de rares spécialistes. **Le groupe a donc estimé qu'il serait particulièrement important de remédier à cette situation.**

2. Comment assurer la sécurité et la conformité des objets connectés en santé, ainsi que la protection des données qu'ils recueillent ?

2.1- Protection des données et cybersécurité :

D'un point de vue informatique, les objets connectés en santé posent deux problèmes distincts, celui d'une part de la protection des données qu'ils recueillent, et d'autre part celle de leur sécurité intrinsèque vis-à-vis des autres systèmes informatiques.

Le marché des objets connectés ouvre d'innombrables perspectives lesquelles vont réclamer de s'adapter au fur et à mesure des usages et des innovations. Il est indéniable que libérer, réguler et travailler la donnée, pour faire de l'analyse prédictive à des fins d'anticipation des pathologies constitue un véritable progrès et fait naitre beaucoup d'espoirs pour la recherche.

La donnée ne peut pas échapper à cette transformation des modèles car elle fait partie intégrante du processus. Il convient donc de l'accompagner plutôt avec confiance qu'avec crainte grâce à des modes de régulation et en relativisant le mythe de la santé connectée qui serait un « aspirateur » de données personnelles n'est pas fondé. En effet, selon la CNIL seules 15 % des applications demanderaient des informations à caractère personnel. Par ailleurs, 90 % des applications de santé seraient effacées après le cinquième usage. Ces réalités ne dispensent cependant pas d'une certaine vigilance.

Cette vigilance semble d'autant plus importante que les constats opérés s'agissant du respect de la vie privée et de la protection des données, par divers opérateurs, ne sont pas particulièrement positifs, même s'ils sont en voie d'amélioration. Une interrogation légitime s'impose sur l'utilisation potentielle de ces informations par certains professionnels, notamment par le secteur assurantiel.

Sur cette problématique, le groupe s'est tout d'abord interrogé sur la qualification des données recueillies par ces objets : données, données personnelles ou données de santé ? Sur ce point, l'audition de la CNIL a été très éclairante.

Une donnée à caractère personnel est une donnée rattachée à un individu permettant d'identifier la personne à qui appartient cette donnée. La particularité de la loi informatique et liberté et du règlement européen sur la protection des données personnelles est que toutes les données qui peuvent être rattachées à un individu sont qualifiées de données personnelles, qu'elles identifient la personne directement (nom, prénom, adresse…) mais également indirectement. Au final, il existe très peu de traitements de données qui ne sont pas des données à caractère personnel. En matière d'objets connectés en santé, la collecte de données vraiment anonymes est pour ainsi dire impossible.

Les risques de ré-identification sont notamment considérablement accrus dans le domaine de la santé par le Big Data et l'Open Data qui facilitent le recoupement des données. Les capacités d'inférence sont actuellement de plus en plus considérables et l'idée généralement admise qui voulait qu'enlever le nom et le prénom garantisse l'anonymat n'est plus du tout vraie aujourd'hui. Aussi, la CNIL œuvre pour l'utilisation du terme « pseudonymiser ». Dans ce cas, l'identité de la personne est remplacée par un numéro aléatoire ou par des éléments qui restent identifiants mais de manière totalement indirecte. Le système est très utilisé dans le domaine de la santé, notamment en matière de recherches médicales, le nom du patient est remplacé par un numéro aléatoire qui n'est connu que de l'investigateur en santé, du système informatique et du patient.

La définition d'une « donnée de santé » repose quant à elle majoritairement sur quelques jurisprudences européennes et sur une définition très large inscrite dans le nouveau règlement européen sur la protection des données personnelles. Au sens de ce règlement, une donnée de santé est une donnée qui fournit des indications sur l'état physique ou psychique des personnes mais aussi, et c'est là que réside la nouveauté, sur toutes données ayant trait à la dispense de soins ou d'accompagnement à titre médical. Cette nouveauté instaure un panel très vaste sachant que des jurisprudences aux Pays Bas ont reconnu que même une information sur la bonne santé d'une personne doit être considérée comme une donnée de santé.

Il existe donc un glissement de la définition d'une donnée de santé au sens médical (pathologie, suivi d'une maladie) vers des aspects d'accompagnement et de bien-être. L'élargissement de cette acception a des conséquences importantes car les données de santé sont considérées comme des données sensibles qui imposent des formalités et des mesures de sécurité renforcées. En France notamment, la loi impose le stockage de ces données chez des hébergeurs agréés.

En résumé, la majorité des données recueillies par ces objets ou applications sont personnelles (et généralement de santé), et relèvent donc de la loi informatique et liberté laquelle confère des droits aux consommateurs et impose des devoirs aux personnes morales publiques ou privées qui vont traiter ces données.

S'agissant des droits des usagers, le droit de suppression, d'opposition et la gestion du consentement sont inscrits dans la loi informatique et liberté depuis 1978 et s'intègrent dans le cadre général des droits des personnes qui doivent être informées en cas de traitement de leurs données. Les données de santé, qui sont des informations très sensibles, sont soumises au principe général d'interdiction de traitement sauf en cas de dérogation. La personne doit donner son accord en signant un formulaire de consentement pour que ses données soient utilisées notamment à des fins de recherche. Ce formulaire prévoit la durée de conservation mais informe également la personne sur ses autres droits : accéder à ses données, les rectifier et les supprimer à tout moment. Dans certaines situations, la suppression est possible sans mentionner de motif, dans d'autres comme pour les données de santé, un motif légitime doit être apporté. Le droit à l'oubli mis en œuvre dans la loi de modernisation de notre système du santé du 26 janvier 2016, n'est en fait que la réaffirmation du droit de suppression et d'opposition prévu depuis longtemps par la loi informatique et liberté du 6 janvier 1978 qui s'applique également aux moteurs de recherche, aux réseaux sociaux.

S'agissant des obligations imposées aux personnes retraitant les données, la première de ces obligations est que la finalité de la collecte des données personnelles doit être clairement et préalablement définie et que seules les informations pertinentes et nécessaires par rapport à la finalité du traitement doivent

être utilisées, et donc demandées. De plus, les informations personnelles ne peuvent pas être indéfiniment conservées. Les données doivent donc être collectées et traitées dans un périmètre strictement justifié par le traitement employé.

Les données de santé ne sont pas uniquement encadrées par la loi informatique et liberté mais aussi par le Code de la santé publique qui prévoit les obligations suivantes pour les professionnels de santé, les établissements de soins et les hébergeurs de données (article L.1111-8 du code de la santé publique):

- obligation de confidentialité des données médicales ;
- droit d'être informé ;
- droit d'accéder aux données ;
- obligation d'assurer la sécurité du stockage des données médicales. Cette obligation encadre plus particulièrement l'action des hébergeurs de données de santé (HDS) qui, pour stocker des données de santé, doivent obtenir un agrément délivré par le ministère de la santé après avis de l'Agence des systèmes d'information partagés de santé (ASIP) et de la CNIL.

Or, dans le cadre de l'enquête qu'il a mené sur un panel d'objets connectés en santé, laquelle fait écho à des constats effectués dans d'autres Etats-membres[7], l'Institut national de la consommation (INC) a relevé que si la fiabilité médicale des objets analysés était bonne, d'importantes failles avaient été détectées d'un point de vue informatique. Des observations, il ressort que peu de fabricants utilisent un langage véritablement sécurisé. Un éparpillement des données des applications vers des serveurs d'audience et des serveurs liés à la publicité a été également constaté. Les fabricants indiquent parfois sur leur site que les données récoltées sont envoyés sur des serveurs tiers mais le type de données transmises n'est pas précisé, de même que la finalité de ces serveurs ou leur localisation. Les données personnelles peuvent ainsi partir à l'étranger.

De manière générale, l'INC relève que l'utilisateur n'a aucune prise sur le devenir de ses données qui constitue pourtant un sujet de consommation majeur. Le partage des données est prévu quasiment par l'ensemble des fabricants. Cependant, il est à déplorer que l'alerte sur la nécessité d'être vigilant sur ce partage par mail ou via les réseaux sociaux ne soit pas présente de manière systématique. Dans la plupart des cas, l'accord du consommateur est requis pour sa géolocalisation. A noter que dans certains cas, l'intérêt de cette géolocalisation est sujet à caution.

La politique appliquée par les fabricants est celle de « l'opt out ». Le consommateur doit donc penser à refuser la transmission de ses données à des tiers et contacter le fabricant à cet effet, ce qui est souvent complexe. Des difficultés d'accès à l'information ont également été relevées en matière d'identification et de protection des données personnelles. Avant de pouvoir télécharger une application, le consommateur doit être en mesure de trouver la fiche d'information sur cette dernière. Or, lorsque que ces fiches existent, certaines sont en anglais et les éditeurs ne sont pas, de manière générale, clairement identifiés.

Fort de ces constats, le groupe de travail a par la suite approfondi le volet règlementaire de ce sujet au travers de la présentation, par la CNIL, du Règlement européen sur la protection des données personnelles adopté le 27/04/2016 qui rentrera en application dans l'ensemble des pays de l'Union Européenne le 25/05/2018.

Il prévoit un niveau de sanction adapté à l'écosystème des grands opérateurs de données au niveau mondial. Actuellement, la CNIL peut sanctionner les opérateurs à hauteur de trois cent mille euros, le

[7] Une étude a en effet été conduite sur les applis recommandées par le NHS (*National Health Service*) au Royaume Uni[7], et sur les 79 applis certifiées fiables sur le plan médical, il a été montré que 89% d'entre elles transmettaient des données à des services tiers, aucune ne disposait d'un système de chiffrement (« cryptage ») des données enregistrées sur le smartphone, 66% envoyaient des informations identifiantes non chiffrées sur le net, et 20% n'avaient aucune politique de protection des données. En faisant la preuve des trous de sécurité des applis recommandées ne permettant pas de garantir la confidentialité des données sensibles collectées, cet article a eu l'effet d'un pavé dans la mare et a conduit à la fermeture du site NHS Health Apps Library[7] du NHS Choices.

règlement permettra aux CNIL européennes de requérir jusqu'à 20 millions d'euros ou quatre pour cent du chiffre d'affaires annuel mondial des entreprises.

Le règlement prévoit des nouveaux droits des personnes : le droit à l'oubli, le droit à la portabilité qui facilite le changement de prestataire (très utile en matière d'objets connectés qui s'inscrivent dans un écosystème plutôt captif), la possibilité d'introduire des recours collectifs et le principe général de transparence applicable au responsable du traitement. Mais aussi, des nouvelles responsabilités pour les entreprises :

- formalités allégées pour le responsable de traitement qui devra non plus a priori mais a postériori produire la documentation qui atteste de sa conformité ;
- désignation d'un délégué à la protection des données, les Data protection officer (DPO), pour toute entreprise qui traite de manière massive ou récurrente ou qui réalise du profilage sur des données personnelles ;
- réalisation d'une étude d'impact sur la vie privée des gens : privacy impact assessment (PIA).

Le PIA constitue le moyen de se mettre en conformité avec le règlement européen et de le démontrer. Il s'applique aux responsables de traitements dans le cadre de la conception des traitements de données à caractère personnel et aux fournisseurs dans le cadre de la conception de leurs produits. Le rapport de PIA devra être accessible aux autorités de protection des données. Le PIA traitera concurremment du respect des principes fondamentaux (« non négociables », fixés par la loi) et de la gestion des risques sur la vie privée (mesures techniques et organisationnelles pour protéger les données et la vie privée des personnes concernées). La gestion des risques sur la vie privée mesurera les conséquences pour l'utilisateur en cas d'impact sur les données. Trois catégories de risques ont été identifiées :

- l'accès illégitime aux données **:** l'atteinte à la confidentialité peut se traduire par des vols de données qui conduisent à leur publication (internet, réseaux sociaux…) ou exposer l'utilisateur à des risques de « tracking », « profiling », « big data », revente de fichiers, usurpation d'identité…;
- la modification non désirée **:** l'intégrité des données peut être menacée par des attaques ou par leur exploitation frauduleuse (détournement du traitement, usurpation d'identité) ;
- la disparition des données *:* disparition de la disponibilité des données (effacement du dossier médical) ou perte d'informations sur des données médicales qui peut conduire à l'interruption des soins.

Ce panel de risques relativement simples peut entraîner des conséquences très variées de gravité parfois élevée. Aussi, le PIA prévoit une analyse de ces risques qui se fonde sur deux axes : la gravité (impact) et la vraisemblance (probabilité que cela se produise). Cette démarche va permettre au responsable de traitement de limiter les risques avec la mise en place d'une série de mesures organisationnelles, de sécurité logique et de sécurité physique. Cette étude de risques PIA permet au responsable de traitement de démontrer que tous les risques sur la vie privée ont été identifiés et ramenés à un niveau résiduel. Le rapport de PIA est accepté par le responsable de traitement (directeur d'entreprise, chef de service d'une administration…) ce qui constitue une auto homologation. La mise en conformité se fonde donc sur les démarches entreprises par le responsable de traitement et non pas, à l'instar des normes ISO, sur des audits externes. Les CNIL européennes continueront à accompagner les responsables de traitement pour les aider à valider leur PIA. Dans cette perspective, la CNIL a édité trois guides pour leur réalisation et accompagne notamment les PME-TPE dans leur réalisation.

Fort de ces explications, le groupe de travail a considéré que le cadre règlementaire en place s'agissant de la protection des données était suffisant[8], mais ici encore trop mal connu des consommateurs, ce à quoi il conviendrait de remédier.

---

8 Le droit positif en matière de données personnelles apparaît déjà étoffé mais les dispositifs sont mal connus des consommateurs, ce qui justifie d'améliorer l'information sur les droits que ces textes leur confèrent. Les principaux textes en vigueur sont notamment les suivants : la directive 95/46/CE sur la protection des données personnelles, la directive 2009/136/CE, la directive 2002/58/CE, la loi 78-17 du 06 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, et ses décrets d'application, la loi du 21 juin 2004 pour la confiance dans

Le groupe de travail a par ailleurs approfondi le sujet de la cybersécurité de ces objets qui est également un problème majeur en termes de protection des consommateurs. Les aspects de cybersécurité en matière de DM peuvent entraîner des conséquences dramatiques pour le patient telles que la prise de commande d'un pace maker ou d'une pompe à insuline à distance par un tiers. Les objets connectés non DM, bien qu'également soumis aux risques de cyberpiratage, ne constituent pas un même niveau de menace pour leurs utilisateurs. Néanmoins, ces derniers peuvent être utilisés par les pirates comme passerelle pour s'introduire dans d'autres systèmes[9].

Pour l'Agence nationale de la sécurité des systèmes d'information *(*ANSSI*)*, auditionnée au cours des travaux du groupe de travail, la première attitude à tenir en matière de sécurité informatique est d'anticiper sur des scénarios de cyber menaces qui peuvent prendre plusieurs formes dont :

- l'espionnage avec le vol de données, notamment à caractère personnel, qui vont alimenter un marché parallèle très bien organisé,
- le sabotage qui concerne plus particulièrement des secteurs vitaux comme l'énergie : les attaques informatiques dans ce secteur peuvent entraîner l'arrêt d'une centrale et priver d'alimentation en énergie tout un périmètre territorial,
- les menaces dites de « déstabilisation » telles que les [10]défigurations réalisées sur des sites institutionnels qui peuvent entamer leur crédibilité ou les dénis de service qui consistent à envoyer une masse de requêtes à des serveurs afin d'en paralyser le fonctionnement,
- le « cyber racket », qui cible particulièrement les entreprises et s'appuie sur l'utilisation de logiciels malveillants qui chiffrent toutes les données et qui nécessitent une clé pour être décodées sous réserve du versement d'une rançon.

L'ensemble de ces menaces portent sur des enjeux de souveraineté, de développement économique et de protection des citoyens. Du fait de l'absence de périmètre en matière d'objets connectés, l'ANSSI exerce des missions de veille sur des secteurs très variés tels que les objets du quotidien, les outils de communication mais aussi les objets à usage médical.

L'Agence rappelle que la prise en compte de l'aspect cybersécurité est profitable à l'ensemble des acteurs. Elle permet par exemple de préserver la confidentialité des données des patients contre les prédateurs. Elle peut également protéger les praticiens contre les risques juridiques liés à un défaut de sécurité.

La cybersécurité représente aussi une opportunité pour les industriels du secteur. L'industrie française de la sécurité est d'ailleurs un secteur performant, notamment en matière de cryptologie. Aussi, la sensibilisation des industriels français aux perspectives prometteuses qu'offre le marché de la cybersécurité (produits et services) contribue au développement de l'innovation.

Afin d'informer l'ensemble des publics (administrations, professionnels, particuliers) intéressés par les aspects de sécurité informatique, l'ANSSI dispose d'un site internet. Y figurent notamment, des guides d'hygiène de sécurité et des recommandations de bon sens sur lesquels il serait souhaitable de communiquer davantage auprès des consommateurs. Ces préconisations « de base » pourraient en outre être systématiquement reprises dans les notices des objets ou applications.

---

l'économie numérique. S'ajoute à ce dispositif, la loi du 7 octobre 2016 pour une république numérique qui comporte un volet sur les données personnelles, ainsi que le Règlement européen prècité.

[9] Il en est de même pour les pacemakers connectés dont la preuve de leur vulnérabilité semble avoir été faite, conduisant, par exemple, Dick Cheney (ancien vice-président des Etats-Unis) à remplacer le sien de façon à désactiver de façon définitive la connexion sans fil.

2.2- Normalisation, certification, labellisation : quelle voie privilégier et selon quels critères ?

Tel que rappelé précédemment, les objets connectés non-DM obéissent généralement à la seule obligation générale de sécurité ou à des règlementations sans rapport direct avec le contrôle des effets thérapeutiques ou de santé revendiqués par ces produits. Or, il est apparu primordial de garantir le bon fonctionnement et la fiabilité des données recueillies par ces objets au regard des revendications qu'ils affichent, qu'ils soient ou non DM[11], ainsi que la fiabilité de la protection des données.

Pour ce faire, le groupe de travail a étudié les divers hypothèses présentes à ce jour sur le marché ou en cours de conception tant au niveau national, que communautaire. Cette étude s'est nourrie de l'audition d'acteurs variés du monde de la normalisation et de la certification, que celle-ci soit réalisée par des organismes professionnalisés en la matière, par de petites entreprises ou encore par des groupes de patients nés de la société civile. Le groupe a par ailleurs longtemps réfléchi à l'opportunité de préconiser la mise en œuvre d'un label propre à encadrer et de ce fait sécuriser la vente d'objets connectés.

S'agissant des processus de normalisation et/ou de certification, l'AFNOR a expliqué qu'elle travaillait depuis de nombreuses années sur le numérique et qu'elle intervenait notamment sur deux labels de certification délivrés par l'ANSSI : le label « secure cloud »[12] et le label « eIDAS » concernant la mise en œuvre du règlement communautaire relatif à l'identification électronique et les services de confiance pour les transactions électroniques entré en vigueur le 1er juillet 2016.

Les travaux spécifiques de l'AFNOR sur les objets connectés, ont débuté quant à eux fin 2014, et étaient loin d'être aboutis. L'Agence a dû au préalable identifier les différents partenaires et se consacrer à la construction du groupe de travail à l'international sur la normalisation qui rassemble des présidents de commissions de différents pays. Par ailleurs, afin d'accélérer les réflexions en cours, certaines commissions ont souhaité travaillé avec l'AFNOR pour commencer à construire un cahier des charges permettant l'évaluation des objets connectés. L'AFNOR était donc, au moment de son audition, en cours d'élaboration d'une check-list qui ambitionne de rassembler l'ensemble des problématiques relatives aux objets connectés : conformité du produit, fiabilité du logiciel embarqué, gestion de la Data, transition des données par les réseaux, délivrance ou non de ces données à d'autres tiers… Ce référentiel pourrait servir de première base pour une certification, avant d'envisager la mise en œuvre d'une norme en la matière, qui ne devrait pas intervenir avant deux ou trois ans. La norme internationale concernera les objets connectés dans leur ensemble. Cependant, des cahiers des charges spécifiques devraient être adoptés par grandes familles, comme pour les objets connectés en santé. Ces derniers prendront en compte l'ensemble des problématiques identifiés par le groupe de travail à savoir : la sécurité, la fiabilité du recueil des données et de la transmission et l'exactitude de l'analyse des données.

---

[11] Si certaines applis sont fiables (et en l'espèce efficaces) sur le plan médical comme c'est le cas par exemple de l'appli Moovcare qui a fait la preuve d'un allongement significatif de la survie des patients atteints d'un cancer du poumon métastatique certaines applis de santé sont beaucoup moins fiables. Ainsi, l'appli « Instant blood pressure » téléchargée plus de 100 000 fois utilise les capteurs du smartphone qui serait placé contre la paroi thoracique (objectif de la caméra occulté) pour mesurer la pression artérielle. Or, une publication scientifique récente a permis de montrer que les mesures de pression réalisées par le dispositif sous-estimaient les valeurs pour près de 77,5% des hypertendus. Il

[12] Le label « secure cloud » prend notamment en compte :

- la gestion externalisée avec des entreprises qui emploient des prestataires qui, eux-mêmes, externalisent à d'autres prestataires ou bien qui stockent dans leurs locaux ou dans des locaux appartenant à des tiers ;
- les impacts liés à la sécurité du cloud dans les cas d'externalisation des données entre différents pays qui ne sont pas soumis à la même législation ;
- la formation des personnels des entreprises pour pouvoir les accompagner sur leur montée en compétences ;
- l'anticipation des risques à partir de tests et d'analyses qui permettent de déterminer un pilotage en amont et mettre en place des actions correctives tout au long au service.

Ce label complexe à obtenir, exclu de fait les PME et TPE.

Parallèlement à la mise en place de cette normalisation, d'autres référentiels d'évaluation ont été créés et utilisés par les industriels et la société civile, sans pour autant qu'un de ces référentiels n'émerge comme référentiel de « référence » dans le secteur, et ce jusqu'à la diffusion du référentiel de la HAS.

Le groupe de travail a ainsi auditionné la société DMD Santé, laquelle s'est créée son propre référentiel de certification, après avoir entrepris une revue de l'ensemble des 4 000 applications médicales de l'App store et d'Android. Cette initiative comme celle de la société MedApp doit être saluée et encouragée, notamment en ce qu'elle stimule la réflexion des opérateurs sur le marché et a aidé au développement de son autorégulation. Le recours à des organismes de régulation privés peut donc constituer une solution, cependant le groupe de travail s'est interrogé sur la manière dont pouvait s'opérer le contrôle de ces nouveaux régulateurs et sur la fiabilité dans le temps des certifications qu'ils peuvent délivrer.

Le groupe de travail a par ailleurs auditionné un représentant de « Living lab » ainsi qu'une association de patients (en l'espèce de diabétiques[13]) afin de mieux comprendre :

- quels leviers doivent guider la conception des applications/objets ou leur amélioration pour un usage meilleur, voire optimal, particulièrement en matière de soins des pathologies chroniques, de bien-vivre et de prévention ?
- quels aspects socioculturels doivent être pris en compte dans l'évaluation des objets connectés en santé?

Le rôle du *Living lab* est de créer une passerelle entre les patients/consommateurs et le monde industriel (et des professionnels de santé) au travers de quatre grandes phases : le cadrage avec la définition du besoin ; l'implication des futurs usagers dès l'initialisation du concept ; le test du prototype par les utilisateurs et enfin l'appropriation de l'objet qui peut générer de nouveaux besoins ou des insatisfactions qui entraîneront son évolution. Les auditions des Living lab et de l'association des diabétiques de France ont permis au groupe de travail de mieux appréhender ce qu'était « la valeur d'usage » des objets connectés en santé, valeur qu'il lui a semblé important de préserver et de promouvoir afin d'assurer un développement « sensé » de ce marché.

Le groupe de travail a enfin entendu la HAS[14], laquelle est venue exposer le contenu de son référentiel de bonnes pratiques visant à promouvoir des objets et applications connectés à la fois fiables, sécurisés et de qualité. La création de ce référentiel procède en l'espèce d'une saisine du ministère de la santé et des affaires sociales. Réalisé suite à un long travail d'identification des risques liés à ces objets, le référentiel fondé sur l'analyse de la littérature internationale et sur l'expertise d'un groupe d'experts scientifiques et indépendants, composé de professionnels de santé et de sociétés savantes, d'associations d'usagers, de chercheurs, ingénieurs, d'informaticiens (…) a été soumis à la relecture de trois groupes de travail :

- le groupe de travail indépendant de l'Agence nationale de la sécurité des systèmes d'informations (ANSSI) et de la CNIL,
- le groupe de travail de structures qui pouvaient avoir des intérêts économiques sur le sujet (DMD santé et Medappcare)
- et le GT28 du CSF.

Le contenu du référentiel permet une évaluation multidimensionnelle qui vise à délivrer des informations de santé fiables et de qualité, à élaborer un produit techniquement performant et ergonomique et à garantir la confidentialité des données personnelles et la cybersécurité. Chacun des 101 critères ou bonnes pratiques retenus pour l'évaluation est systématiquement justifié (fondement scientifique, dispositions réglementaires ou légales) et illustré par des exemples explicitant le contenu attendu et les modalités d'évaluation.

[14] Annexe 2 - présentation de la HAS au groupe de travail

L'ensemble de ces bonnes pratiques n'est pas systématiquement employé pour l'évaluation d'un appareil. Leur utilisation a été modulée en fonction des exigences attendues pour chaque objet ou application connecté. Trois niveaux de bonnes pratiques ont été déterminés : « souhaitées », « recommandées » et « obligatoires ». Chaque objet et application connectés a été caractérisé en fonction du principal utilisateur cible et de la destination d'usage. Le type d'appareil détermine le périmètre de bonnes pratiques à prendre en compte par les développeurs et par les évaluateurs. Une matrice des risques entre les critères « souhaités », « recommandés » et « obligatoires » a été créée afin d'aider notamment les développeurs et les évaluateurs à différencier les objets et applications connectés relevant de la zone grise ou d'un DM. En fonction du niveau de criticité, la grille d'évaluation d'un produit comportera un nombre d'exigences en matière de bonnes pratiques plus ou moins important.

Ce processus de sélection des critères en fonction du risque est repris par les catalans et est actuellement en discussion au niveau européen où s'élabore un autre référentiel qui devrait être publié dans le courant du premier semestre 2017. Cependant, en l'état actuel des travaux européens, l'évaluation se focalise exclusivement sur le contenu relatif à la santé et n'intègre pas les dimensions de sécurité des données et de cybersécurité.

Bien que complexe à comprendre et à mettre en œuvre, le référentiel de bonnes pratiques élaboré par la HAS a été plébiscité par le groupe de travail.

Le groupe de travail s'est enfin interrogé, sur l'opportunité de promouvoir une certification ou un label en particulier, initiative qui serait soutenue par l'Etat lui-même et qui garantirait aux consommateurs une totale sécurité.

Or en la matière, le groupe a été amené à constater :

-qu'une telle démarche avait été initiée au Royaume-Uni par le National Health Service (NHS) et qu'elle avait échoué. Les applications et objets connectés bien que fiables d'un point de vue technique et médical, présentés d'importantes non-conformité en termes de protection des données ;

-que la certification adoptée en Espagne avec Appsaludable[15], ne parvient pas à supporter le rythme exponentiel de croissance du marché des objets et applications et le cycle de vie court de ces produits. Cette option n'apparaît donc pas adaptée à notre contexte ;

-que la CNIL a renoncé à mettre en place un label propre aux objets connectés en santé, au regard de la vitesse d'innovation dans ce secteur et de l'important turn-over des outils utilisés ;

-que le GT28 propose la mise en place d'un référentiel de labellisation facultative qui serait à titre principal proposé aux fabricants d'objets et d'applications en santé non-DM, sous la forme d'un ensemble d'exigences à satisfaire qui regrouperaient les bonnes pratiques listées dans le référentiel de la HAS, mais également l'obligation de réaliser un PIA sur un mode générique afin de recenser l'ensemble des risques. Ce PIA générique permettrait ainsi de fixer le spectre des droits fondamentaux des utilisateurs que les fabricants devraient respecter, ainsi que les mesures générales de traitement des risques sur la vie privée, adaptées au contexte des objets connectés en santé. Ce label n'aurait pas pour finalité de promouvoir des objets ou applications à bénéfice thérapeutique avéré. En effet, les méthodologies d'évaluation sont encore à parfaire sur ce sujet. Or, il paraissait important pour le GT28 de ne pas plus attendre ;

[15] Deux régions espagnoles (Catalogne et Andalousie) se sont lancées dans un processus de labellisation. L'Andalousie a mis en place une plate-forme de certification sur laquelle sont recommandées vingt-six applications non DM. Ce site, ouvert depuis trois ans, est utilisé par 17% de la population andalouse (17 millions) pour sélectionner une application. La Catalogne a instauré un processus d'évaluation quasi similaire au guide des bonnes pratiques de la HAS.

Le GT 28 propose en outre de populariser ce label auprès des consommateurs mais aussi des professionnels de santé avec la mise en place d'un portail de référencement. Ce dernier proposerait la liste des objets et applications connectés avec le résultat de leur labellisation. Ce label resterait une simple faculté pour les fabricants ;

-que d'autres travaux de labélisation ont d'ores et déjà été engagés et pourraient concerner des objets connectés en santé :

- le label AFNOR « Testé et approuvé par les seniors » : lancé à l'occasion du salon Silver Economy Expo. Le produit ou la solution feront l'objet d'une évaluation complète réalisée par un groupe de seniors et un groupe d'experts dans le cadre d'un protocole très cadré.
- le référentiel AFNOR de certification de qualité de services : un GT "Objets Connectés de Santé et de Bien-être" a été mis en place par l'AFNOR pour définir un référentiel de certification de qualité de services. (…)

-que des travaux sont par ailleurs en cours au niveau communautaire, travaux qui pourraient aboutir à la diffusion d'un référentiel commun ; que pour autant à l'heure actuelle, il n'existe aucun mécanisme de reconnaissance entre les différents systèmes de labélisation déjà mis en place dans plusieurs Etats-membres, l'Espagne et la France étant identifiés comme des pays précurseurs en la matière ;

Sur la base de ces constats, le groupe de travail n'envisage pas la création d'un nouveau label porté par l'Etat. Il lui_ semble préférable d'identifier un socle commun d'exigences qui serait rendu applicable à l'ensemble des labels déjà existant ou en cours de construction afin que le consommateur soit rassuré dans son acte d'achat.

L'avis du groupe de travail du CNC relatif aux objets connectés en santé a été adopté à la majorité des voix des représentants de chacun des deux collèges au bureau du CNC, le 07 juillet 2017.

Liste des acronymes

AFNOR	Agence française de normalisation
ANSM	Agence Nationale de Sécurité du Médicament et des Produits de Santé
ANSSI	Agence Nationale de Sécurité des systèmes informatiques
ARPP	Autorité de régulation professionnelle de la publicité
ASIP	Agence française de la santé numérique
CNIL	Commission Nationale de l'Informatique et des Libertés
CSF	Comité Stratégique de Filière
CSIS	Conseil Stratégique des Industries de Santé
DGCCRF	Direction générale de la concurrence, de la consommation et de la répression des fraudes
DM	Dispositif Médical
DPO	Data protection officer (successeur du correspondant informatique et libertés)
HAS	Haute Autorité de Santé
HDS	Hébergeur de données de santé
INC	Institut national de la consommation
Living Lab	Méthodologie où citoyens, habitants, usagers sont considérés comme des acteurs clés des processus de recherche et d'innovation
LNE	Laboratoire national de métrologie et d'essais
MEDDEV	Guide définissant des lignes directrices d'interprétation des directives communautaires
NHS	National Health Services (Agence sanitaire de l'Angleterre)
PIA	Privacy impact assessment (catalogues de bonnes pratiques destinées à traiter les risques que les traitements de données à caractère personnel (DCP) peuvent faire peser sur les libertés et la vie privée des personnes concernées)
SNITEM	Syndicat National de l'Industrie des Technologies Médicales

Liste des participants au groupe de travail

COLLEGE DES ASSOCIATIONS DE CONSOMMATEURS

M. Vincent PERROT, rapporteur	Confédération de la consommation, du logement et du cadre de vie (CLCV)
Mme Micheline BERNARD-HARLAUT	Association « Léo-Lagrange » de défense des consommateurs (ALLDC)
M. Geoffroi PENET	Confédération nationale des associations familiales catholiques (CNAFC)
M. Hugo CADET	Conseil national des associations familiales laïques (CNAFAL)
Mme Nicole DAMON	Conseil national des associations familiales laïques (CNAFAL)
M. Julien LEONARD	Conseil national des associations familiales laïques (CNAFAL)
Mme Marion PLATEEL	Confédération nationale du logement (CNL)
Mme Claudine LEMER	Familles rurales (FR)
Mme Morgane LENAIN	Union nationale des associations familiales (UNAF)
Mme Nathalie TELLIER	Union nationale des associations familiales (UNAF)

COLLEGE DES ORGANISATIONS PROFESSIONNELLES MEMBRES DU CNC

M. Jacques SAINCTAVIT, rapporteur	Mouvement des entreprises de France (MEDEF**)**
Mme Christine BARATTELLI	Mouvement des entreprises de France (MEDEF**)**
Mme Céline DELACROIX	Chambre de Commerce et d'Industrie de région Paris Ile-de-France (CCI Ile de France)
M. François BERTIN HUGAULT	Confédération générale des petites et moyennes entreprises (CGPME)
Mme Amélie JUGAN	Confédération générale des petites et moyennes entreprises (CGPME)
Mme Julie MACAIRE, Co-rapporteure	Fédération des industries électriques, électroniques et de communication (FIEEC)
M. Gilles ROUVIERE, Co-rapporteur	Fédération des industries électriques, électroniques et de communication (FIEEC)
M. Jérôme BALMES	Fédération Française des Sociétés d'Assurances (FFSA)
Mme Eléonore DAVAUX	Fédération Française des Sociétés d'Assurances (FFSA)
Mme Anne-Marie PAPEIX	Fédération Française des Sociétés d'Assurances (FFSA)
M. Philippe GAERTNER	Union nationale des associations de professions libérales (UNAPL)

AUTRES ORGANISMES PROFESSIONNELS

Mme Elisabeth HUBERT	Fédération Nationale des Etablissements d'Hospitalisation à Domicile (FNEHAD)
Mme Sabah DOUDOU	Industrie du génie numérique, énergétique et sécuritaire (IGNES/FIEEC)
Mme Florence OLLE	Syndicat national de l'industrie des technologies médicales (SNITEM)
Mme Natalie JOUEN ARZUR	Union Nationale des Entreprises de Télécommunications, de Réseaux et de Services en Télécommunications (UNETEL)

MEMBRES DE DROIT

Mme Karine BOQUET	Conseil national de l'alimentation (CNA)
Mme Patricia FOUCHER	Institut national de la consommation (INC)
Mme Marie MARTIN	Institut national de la consommation (INC)
M. Thierry MARTIN	Institut national de la consommation (INC)

ADMINISTRATION

Mme Raphaëlle BOVE	Présidente du Groupe de travail DGCCRF – Chef du bureau produits et prestations de santé et des services à la personne (5B)
M. Olivier PIAT	DGCCRF – 5B
Mme Nicole PETIT	DGCCRF – 5B
Mme LALOUELLE Françoise	DGCCRF – GIC-CNC
Mme BAZINETTE Nadine	DGCCRF – GIC-CNC

Liste des annexes –