Le Droit de l'Internet des Objets

Table ronde 13 février 2015

Sous la direction de Jean Frayssinet et Philippe Mouron

Léonor CHOUX
Lauren ESTRUCH
Sandrina GONCALVES

LID2MS
Faculté de Droit et de Science Politique
Aix*Marseille Université
IREDIC

INTRODUCTION

Les objets connectés dans le domaine de la « santé connectée» ont connu un succès très important en 2014. Ce succès devrait continuellement s'accroître grâce à l'essor considérable de l'Internet des objets. En décembre 2014, Marisol Touraine, Ministre de la Santé, s'est adjoint une experte dans ce domaine ayant pour objectif de s'intéresser à la problématique de la démocratisation de ce type d'objet dans les parcours de soins. Bien qu'ils puissent parfois être sources d'inquiétudes en raison de leur caractère « intrusif », ces objets intéressent une grande partie des français. Ainsi, parmi les 300 exposants du domaine de la santé connectée et de la biotechnologie au Consumer Electronics Show qui a eu lieu à Las Vegas au mois de janvier dernier, cinq start-up françaises et américaines ont présenté leurs objets connectés.

Le marché de l'Internet des objets est important. Il est prévu qu'à l'horizon 2018, un individu disposera d'environ 8 objets connectés. Par ailleurs, notre corps pourra être lui-même « connecté » par le biais d'implants par exemple.[1]

D'après une récente étude[2], les objets qui font partie du top 5 des objets connectés sont les suivants : le tensiomètre connecté, la balance connectée, la montre connectée, la boite de médicaments connectée et le bracelet connecté. Ce sont donc bien des objets destinés au bien-être et à la santé.
Selon une autre étude très récente publiée le 19 janvier 2015[3] sur la perception des objets connectés au service de la santé des français, la majorité des patients est convaincue que la « *santé connectée* » peut contribuer d'une part à l'amélioration de « *la qualité des soins* » et d'autre part, peut constituer « *une opportunité en vue d'améliorer la prévention* ». Ce constat vient confirmer une précédente étude publiée par Médiamétrie en décembre 2014[4], selon laquelle : 61% des français sont aujourd'hui familiers du concept d'objet connecté, et 75% des « multi-connectés » ont déjà entendu parler des objets connectés.

S'agissant plus particulièrement de la « santé connectée », sous-thème de l'Internet des objets qui nous intéresse, les chiffres relatifs à l'évolution du secteur de la santé connectée sont percutants. Ainsi la CNIL prévoit qu'à l'horizon de 2017, un utilisateur sur deux de tablettes ou smartphones, aura installé une application mobile destinée à la santé ou au bien-être.
A cet égard, il convient de souligner que la CNIL tente de définir un label afin que les éditeurs d'applications mobiles e-santé informent davantage les utilisateurs de l'utilisation faite de leurs données personnelles. L'objectif est ici pour l'utilisateur d'avoir une maîtrise effective de ses données.

---

[1] SILGUY (S.), « Les objets connectés, un risque pour la protection de nos données personnelles », *RLDC*, n°119, 1er octobre 2014, pp. 66-69
[2] Etude CCM Benchmark « Les français et la santé connectée » publiée en Mars 2014
[3] Etude Baromètre 360 d'Orange Healthcare et MNH réalisée par Odexa publiée le 19 janvier 2015
[4] Etude Médiamétrie sur les objets connectés publiée le 10 décembre 2014

Aujourd'hui, les objets de santé connectée font l'objet d'une forte démocratisation, alors qu'auparavant, certains pensaient qu'ils ne concerneraient qu'une cible particulière de sportifs ou encore d'individus hyper-connectés. D'après certaines études, le public visé est plutôt un homme de 35 ans, parisien et CSP+[5]. Selon encore une autre étude de Médiamétrie, 60% des équipés sont des hommes, 36% des 16-24 ans.

Préalablement, il convient de définir ce que l'on doit entendre par le terme « santé connectée ». Il s'agit de « *services relatifs à la santé disponibles en permanence via un appareil mobile connecté à un réseau (objet connecté, smartphones, tablettes)* ». La santé connectée constitue l'évolution de la « e-santé » qui par définition est un *« phénomène désignant toutes les utilisations possibles des technologies de l'information et de la communication* »[6] avec un appareil mobile. Le concept de « santé connectée » peut en réalité se décomposer sous différents paliers. Ainsi, « le web 2.0 » se caractérisait par le partage de savoirs médicaux au sein de communautés, puis le « web 3.O » permet dorénavant de *« qualifier les savoirs médicaux acquis par capteurs et objets communicants* ».[7] Ainsi, la santé connectée est liée aux différents dispositifs sur les objets connectés, les dispositifs embarqués, ou les smartphones/tablettes.[8]

Le concept de « santé connectée » renvoie nécessairement aux termes « données de santé » dès lors que celles-ci vont avoir vocation à être récoltées, utilisées et parfois partagées. C'est pourquoi, il convient également de les définir. Il s'agit d'une notion qui fait l'objet d'une interprétation large, que l'on retrouve dans une délibération de la CNIL n°97-008 du 4 février 1997 portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel, et qui rappelle que « *la connaissance de l'état de santé d'une personne constitue une information qui relève de l'intimité de sa vie privée et qui est protégée par le secret médical ; en conséquence, le traitement de cette information nécessite, conformément à l'article 6 de la convention n° 108 du conseil de l'Europe (...), l'adoption de garanties appropriées* ».
De sorte que ces données « *(...) ne peuvent être utilisées que dans l'intérêt direct du patient et, dans les conditions déterminées par la loi, pour les besoins de la santé publique et que, dès lors leur exploitation à des fins commerciales doit être proscrite. En conséquence, ces données ne peuvent être traitées que dans le respect des droits des personnes et des règles déontologiques en vigueur* ».
Ainsi, « *hors les cas prévus par la loi, les professionnels de santé ne peuvent transmettre à des tiers, les données de santé à caractère personnel relatives à leurs patients, sans qu'au préalable ces données aient été rendues anonymes (...)* » ; et « *même rendues anonymes à l'égard des patients, [elles] ne peuvent être utilisées à des fins de promotion ou de*

[5] Les Français et l'internet santé, Etude TNS Sofres pour LauMa communication et Patients & Web, avril 2013
[6] DESMARAIS (P.), « Quel régime juridique pour la m-health ? », Lexis Nexis, *CCE*, n°3, mars 2003, p.15
[7] Conférence « La m-santé en 2014 » par MENNECIER (D.), *Commission XX, Académie nationale de médecine, 18 juin 2014*
[8] Conférence Santé connectée par CHARRONDIERE (H.), « Santé connectée, e-santé, télémédecine et numérique en santé », *Lesechosetudes*, 18 septembre 2014

prospection commerciale, dès lors qu'elles sont associées à l'identification du professionnel de santé ».

On trouve également des éléments de définition dans une jurisprudence de la CJUE du 6 novembre 2003 dans l'affaire Lindqvist où le terme est défini de la façon suivante : *« information concernant tous les aspects tant physiques que psychiques de la santé d'une personne »*. Plus récemment, selon la proposition du règlement des données personnelles du 25 janvier 2014, il s'agit de *« toute information relative à la santé physique ou mentale d'une personne ou à la prestation de services de santé à cette personne »*. Selon le G29[9], ces informations ont un lien *« clair et étroit avec l'état de santé d'une personne physique qu'il s'agisse d'une pathologie avérée ou susceptible d'être révélée par les informations collectées »*. Il s'agit de données donc « sensibles » et le traitement de ces données est soumis à des conditions particulières. Les données de santé sont nombreuses : rythme cardiaque, tension artérielle, taux de glycémie...[10]Aujourd'hui, la notion pourrait être amenée à évoluer du fait de la convergence manifeste entre données de santé et de bien-être à l'ère des objets connectés.

Il est possible d'opérer une classification dans les objets connectés de santé. Ainsi, certains peuvent dans un premier temps se répartir selon que leur finalité permet de meilleures conditions de vie, ou encore de véritables progrès médicaux. Ils se décomposent de manière très variable, allant de la fourchette connectée pour apprendre à manger plus lentement, qu'au matelas connecté ou des boules quiès (*Hush*) permettant de trouver le sommeil le plus optimal possible ou enfin au coussin connecté pour rester concentrer au travail tout en étant bien installé (*Darma*). Le podomètre connecté permet quant à lui au patient de mesurer sa pression artérielle et sa fréquence cardiaque. Le pilulier connecté permet de s'assurer de la prise de médicament à l'heure. Les applications mobiles sur lesquelles les patients visualisent leur résultat permettent au patient de surveiller son sommeil et ses apports ou dépenses nutritionnelles.

Les chercheurs se concentrent ainsi principalement sur ces objets de santé pour améliorer le quotidien des personnes affaiblies comme par exemple avec la cuillère connectée pour les Parkinsoniens (elle se stabilise), *Clarity* le capteur d'air portable spécial asthmatiques ou encore le *backup memory project* pour aider les malades d'Alzheimer à reconnaitre leur proches. Les objets connectés ont donc de multiples qualités déjà démontrées dans le domaine médical notamment parce qu'ils permettent une meilleure individualisation des traitements et une réelle spécificité.
Mais au-delà de ces objets externes à notre corps, cela peut aller au-delà encore avec des objets plus intrusifs qui récoltent des données personnelles corporelles comme le taux de sucre dans le sang pour les diabétiques qui se régulent seul, ou la montre connectée pour le rythme cardiaque qui peut emmagasiner une quantité incroyable d'informations.

[9] Groupe de travail qui rassemble les représentants de chaque autorité indépendante de protection nationale de l'Union Européenne. « G29 » en référence à l'article 29 de la directive du 24 octobre 1995 sur la protection des données personnelles et leur libre circulation.
[10] ANONYME, « Connecté, le patient devient acteur de sa santé », 17 juin 2014, *www.visionmarketing.com*

Tout cela est évidemment une avancée considérable pour le bien être des malades ou les non malades désireux de suivre leur santé. Ils permettent ainsi de mieux connaitre la maladie afin de mieux la combattre. Avec l'individualisation des données, les traitements sont beaucoup plus adaptés à chaque personnalité, même si cela était déjà en partie possible grâce au séquençage ADN.
S'il apparaît évident que pour les objets connectés aux données internes de notre corps, le consentement de la personne concernée soit récolté, qu'en est-il des objets externes qui collectent des données liées à notre environnement ? Peut-on les considérer comme des données personnelles ? C'est à ce type de question que nous tenterons d'apporter des éléments de réponse au sein de ce rapport.

Sur un plan historique, la santé connectée est issue de deux révolutions. D'une part, l'essor d'Internet a permis de démocratiser le savoir, et d'autre part la démocratisation des usages tablettes et smartphones qui permettent aujourd'hui aux individus d'être ultra-connectés. En outre, le développement des technologies de l'information a permis d'accroître l'autonomisation du patient et la démocratisation du savoir médical. Enfin, c'est le développement de l'Internet des objets, appelé également « informatique ubiquitaire » désignant les différentes solutions techniques (RFID, TCP/IP, Bluetooth) qui, couplées permettent d'identifier des objets, de capter, stocker, traiter et transférer des données [11]qui a permis à la santé connectée de connaître cet essor.

L'idée que l'Internet allait révolutionner l'organisation et l'accès aux soins est née en Australie en 1999 par une étude gouvernementale sous la direction de John Mitchell et le terme « e-health [12]» est donc apparu lors du 7ème Congrès International de télémédecine de Londres de 1999. La définition retenue est donc celle-ci : *« l'usage combiné de l'Internet et des technologies de l'information à des fins cliniques, éducationnelles et administratives, à la fois localement et à distance.*[13] *»*
C'est également à cette époque que le terme « télémédecine » apparaît et il se présente de la manière suivante : « *c'est la fourniture à distance de services de soins de santé par l'intermédiaire des technologies d'information et de communication dans des situations où le professionnel de la santé et le patient ne se trouvent pas physiquement au même endroit. Elle nécessite la transmission en toute sécurité de données et d'information médicales par le texte, le son, l'image ou d'autres moyens rendus nécessaires pour assurer la prévention et le diagnostic ainsi que le traitement et le suivi des patients.* »[14]

[11] FORREST (D.), « Qui a peur de l'Internet des objets ? », RLDI, novembre 2009, n°54, p.45-46
[12] MITCHELL (J.), « Increasing the cost-effectiveness of telemedicine by embrasing e-health », *J. Telemed. Telecare*, 2000, N°6, suppl1, pp.16-19.
[13] SIMON (P.), « Responsabilité des professionnels de santé dans la pratique de la télémédecine clinique », *Revue Générale de Droit médical, Les Etudes hospitalières*, Bordeaux, juin 2014, p.92.
[14] Communication de la Commission au Parlement Européen, au Conseil, au Comité économique et social européen et au Comité des régions sur la télémédecine, 4 novembre 2008, *http://europa.eu/legislation_summaries/pubic_health/european_health_strategy/sp0003_fr.htm*

En 2004 déjà, la Commission Européenne prédisait que l'intégration de l'Internet dans les soins de santé serait chose courante dans les années 2014 et que cela deviendrait la nouvelle industrie de la santé publique.

On peut relier les objets connectés de santé à l'e-santé qui comporte par exemple la télésurveillance sociale à domicile, les capteurs de sécurité pour les personnes âgées (la domotique), et les applications médicales (*quantified-self*).
D'après une partie de la doctrine, les objets connectés pourraient être assimilés à la télémédecine qui est par ailleurs déjà réglementée en droit européen par la directive 98/34/CE du Parlement européen et du Conseil du 8 juin 2000 où le droit communautaire assimile l'exercice de la télémédecine clinique à un service de la société de l'information.
Mais il n'existe pas de cadre législatif clair de la télémédecine.

En droit comparé, il semblerait qu'il n'y ait pas d'homogénéité s'agissant de l'intérêt porté au thème de la santé connectée. En effet, dans certains Etats, aucune loi ne semble susceptible d'encadrer la santé connectée, tandis que d'autres ont commencé à s'intéresser aux problématiques de régulation. Néanmoins dans le domaine de la santé, il convient de souligner par exemple, que les Etats-Unis obligent par une loi, les responsables de traitement de données à mettre en place des mesures pour la protection des données médicales contre les usages qui ne seraient pas autorisés. Depuis 1996, la loi « *Health Insurance portability and accountabillity acte* » sur le traitement des données dans le secteur médical a vocation à s'appliquer. Autre exemple : l'Allemagne a pris l'initiative de l'autorégulation, en développant l'idée d'un « label de qualité » aux applications de santé disponibles pour le grand public au regard d'un code de conduite.[15]
Certaines initiatives personnelles sont de ce fait admirables pour la protection des données de santé mais un réel besoin d'harmonisation se fait de plus en plus ressentir, notamment par le fait que ces nouveaux objets connectés de santé ne connaissent aucune frontière géographique. Le 24 octobre 1995, la directive 95/46/CE du Parlement européen et du Conseil, 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 est votée et restera le cadre législatif européen en la matière. S'ajoute à cela, la loi nationale française Informatique et Liberté de 1978 qui protège les droits personnels des individus mais avec toutes les évolutions technologiques de ces dernières années, il devient urgent d'encadrer les objets connectés notamment ceux liés à la santé. De ce fait, le projet de règlement européen adopté le 12 mars 2012 par le G29 prévoit pour 2015 ou 2016 l'élaboration d'un véritable règlement qui interviendra afin de bien cadrer les Etats membres et d'éviter les mauvaises interprétations. Les données personnelles des européens seront de ce fait beaucoup plus protégées dans l'enceinte de l'Union Européenne et cela renforcera la crédibilité des instances de protection européennes face au géant américain et sa grande liberté en la matière.

[15] CNIL, « Le corps, nouvel objectif du *quantified self* à la m-santé : les nouveaux territoires de la mise en données du monde », cahier IP, n°2, *www.cnil.fr*

L'intérêt de ce sujet consiste dans le fait qu'il s'agit d'un sujet véritablement d'actualité tant sur un plan interne qu'international à égard de son attrait. Il présente également des enjeux pour les pouvoirs publics dès lors qu'il interroge la santé publique. C'est pourquoi, des « hôpitaux connectés » se sont développés. En outre, les médecins suivent le phénomène de près. Ainsi, le Conseil National de l'Ordre des médecins s'y est également intéressé et a publié en février dernier son livre vert relatif à la « santé connectée ». Par ailleurs, il présente des enjeux en termes d'économie puisque la santé numérique devrait générer à l'horizon 2015, 6 milliards de dollars de chiffre d'affaire.[16] Enfin, il présente des enjeux juridiques : le sujet pose de nombreuses problématiques notamment s'agissant de la collecte, de l'utilisation, du traitement ou de la transmission des données personnelles, ainsi que sur l'exploitation des objets connectés de santé par les tiers qui peut vite se transformer en abus.

Dans le cadre de ce rapport, nous avons toutefois choisi d'apporter des limites à ce sujet. Ainsi, nous limiterons nos analyses techniques, économiques et sociologiques, dès lors que celles-ci font l'objet d'un traitement par d'autres groupes. Toutefois, nous évoquerons néanmoins certains aspects qui nous semblent indispensables à l'appréhension et à la compréhension de notre sujet.

La problématique que nous avons choisie dans le cadre de cette étude est donc la suivante : « Le caractère sensible des données de santé véhiculées par l'Internet des objets justifie-t-il un encadrement spécifique quant à leur utilisation ? ».

Les données de santé semblent devoir faire l'objet d'un encadrement nécessaire en raison de l'essor de l'utilisation des objets connectés de santé **(Partie 1)**, dès lors que cet encadrement apparaît manifestement insuffisant en raison de l'utilisation parfois abusive de ce type d'objet spécifique **(Partie 2).**

[16] DESMARAIS (P.), « Quel régime juridique pour la m-health ? », Lexis Nexis, *CCE*, n°3, mars 2003, p.15

I/ Un encadrement nécessaire à l'utilisation des objets connectés de santé

Les données de santé sont des données sensibles et cette spécificité entraine un encadrement législatif qui doit être strict, notamment quant à leur transmission et leur conservation puisqu'elles sont souvent amenées à être exploitées. Cette exploitation a un objectif médical et personnalisé, d'où le développement du *Quantified Self* favorisé par la multiplication des objets connectés mais pas seulement(A). Cette exploitation des données corporelles intéresse également d'autres acteurs et le caractère ubiquitaire de ces données est alors avéré, justifiant ainsi l'encadrement nécessaire(B).

A- Une protection nécessaire à la transmission des données de santé

Les données de santé eu égard à leur caractère sensible doivent faire l'objet d'un encadrement strict s'agissant de leur collecte et de leur transmission.

1- Le caractère sensible des données de santé

La collecte des données de santé fait l'objet d'une double protection : d'une part au niveau international, notamment au niveau européen, d'autre part au niveau interne.

- ***La protection des données de santé au niveau européen***

Ainsi au niveau européen, les données de santé sont qualifiées de « données sensibles » à l'article 8, paragraphe 1 de la directive relative à la protection des données, ainsi que par l'article 6 de la convention n°108.[17] Toutefois, il convient de souligner que le caractère sensible de ces données a fait l'objet de nombreuses discussions dès lors que pour une partie de la doctrine, ce caractère pouvait présenter un aspect controversé. Nombreux sont ceux qui se sont interrogés sur l'opportunité de qualifier ces données de « sensibles ». Néanmoins les textes européens ont permis de leur attribuer cette qualification. Les opposants à cette qualification alléguaient de façon pertinente que la sensibilité des données était un critère qui pouvait apparaître « manifestement insuffisant ». En effet, selon ces derniers, une donnée qui peut sembler « anodine » peut avoir vocation à être qualifiée de sensible dès lors que des regroupements ou un stockage est réalisé.[18] Ce point de vue apparaît pertinent, et peut être confirmé aujourd'hui avec le développement de l'Internet des objets, et en particulier des objets connectés de santé qui collectent également des informations relatives au « bien-être de l'individu ». Or, aujourd'hui la qualification de ces données relatives au « bien-être » pose problème dès lors que fréquemment, elles semblent s'apparenter à des données de santé. Ainsi, ces données font l'objet de discussions dans la doctrine actuelle dès lors qu'elles

[17] ANONYME, *Manuel de droit européen en matière de protection des données,* Office des publications de l'Union Européenne, Luxembourg, 2014, p.94

[18] MARLIAC NEGRIER (C.), *La protection des données nominatives informatiques en matière de recherche médicale, Tome* 2, PUAM, p. 454

peuvent révéler des éléments intimes relevant de la vie privée. Par conséquent, les données « sensibles » peuvent faire l'objet de différentes approches. [19]

L'article 6 de la convention du 28 janvier 1981 interdit le traitement de ces données. Il dispose que *« les données à caractère personnel révélant l'origine raciale, les opinions politiques […] ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle ne peuvent être traitées automatiquement à moins que le droit interne ne prévoit des garanties appropriées ».*

Par ailleurs, le droit de l'Union Européenne incite les Etats membres à interdire le traitement des données à caractère personnel ainsi que le traitement des données relatives à l'état de santé d'un individu. Toutefois, le droit de l'Union Européenne permet au droit interne de déterminer la protection qui lui semble la plus adaptée pour l'utilisation de données sensibles. Néanmoins, l'article 8 de la directive relative à la protection des données évoque un système particulier pour le traitement de catégories de données qui révèlent les données relatives à la santé.[20]

- ***La protection des données de santé au niveau interne***

Au niveau interne, la sensibilité des données de santé fait également l'objet d'un encadrement spécifique. Le texte qui protège ces données est la loi Informatique et Libertés de 1978. En effet, il est prévu au sein de cette loi que les informations relatives à l'état de santé physique ou psychique d'un individu revêtent un caractère sensible. L'article 8 dispose : *« Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement […] ou qui sont relatives à la santé […] ».*

Ainsi, la collecte, le traitement, l'utilisation, la communication, le stockage ou la destruction de ces données sont strictement conditionnés[21]. Par exemple, dès lors qu'une application va recourir à une connexion pour échanger des données à caractère personnel, la loi de 1978 a vocation à s'appliquer. La collecte et le traitement de ces données est en principe interdit, à défaut d'avoir obtenu le consentement exprès du patient. Ainsi, le principe d'interdiction peut parfois faire l'objet d'exceptions. Celles-ci ont rendu possible le développement des objets connectés qui recueillent un nombre très important de données particulièrement « sensibles ».[22]

Des dispositions particulières sont également prévues au sein du code de la santé publique. Ainsi, en cas d'hébergement des données par un sous-traitant, un agrément administratif du Ministère de la santé est nécessaire[23]. Ce principe est posé à l'article L1111-8 du code de la santé publique qui dispose que *« les professionnels de santé ou les établissements de santé ou la personne concernée peuvent déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins, auprès de personnes physiques ou morales agréées à cet effet. Cet hébergement de données,*

---

[19] MARLIAC NEGRIER (C.), *La protection des données nominatives informatiques en matière de recherche médicale,* op cit, p.646

[20] ANONYME, *Manuel de droit européen en matière de protection des données*, op cit, p.189

[21] SFEZ (B.), Données de santé : des obligations de sécurité spécifiques pour les professionnels de la santé, Village-justice.com, publié le jeudi 23 novembre 2014

[22] DREYFUS (N.), Santé connectée : la CNIL s'inquiète », Village-justice.com, publié le lundi 21 juillet 2014

[23] PANSIZE (F-J.), CHARBONNEU (C.), « La dématérialisation des données médicales et les enjeux de leur hébergement », *Gazette du Palais, n° spécial, 2002,* p.23

quel qu'en soit le support, papier ou informatique, ne peut avoir lieu qu'avec le consentement exprès de la personne concernée ».

Il semble peser ainsi sur le professionnel ou bien l'établissement de santé une obligation de garantir que le prestataire peut mettre en œuvre [24] des mesures de sécurité suffisantes. Une partie de la doctrine allègue toutefois que cette obligation pèserait plutôt sur l'hébergeur.

Par ailleurs, la problématique de la convergence entre les données de santé et les données de bien être se pose également en droit interne dès lors que ces obligations pourraient également s'imposer au fabriquant d'un objet connecté qui héberge, analyse, et renvoie des données de bien être au consommateur à défaut de clarification sur la nature de ces données[25].

Le législateur a prévu expressément la conclusion d'un contrat : le patient détient un rôle prépondérant dans le contrat d'hébergement. L'hébergement de données ne peut avoir lieu qu'avec le consentement exprès de la personne concernée. Ainsi, l'accord du patient est requis, il doit être informé également sur les conséquences et les risques liés à la dématérialisation notamment les risques quant à la confidentialité des informations. Au-delà des textes, la jurisprudence a confirmé le caractère « sensible » des données dans un arrêt rendu par le Conseil d'Etat le 18 novembre 1992, CE Ligue internationale contre le racisme et l'antisémitisme, où il a été énoncé que *« les données de santé doivent faire l'objet d'une protection spécifique ».*

Il apparaît ainsi que ces données font l'objet d'un strict encadrement et d'une importante protection. Aujourd'hui ces données de médicales sont au cœur de la « santé connectée » marquée par un partage de ces informations quasiment complet et qui met en évidence l'impact de la collecte de ces données sur la relation entre le professionnel de santé et son patient. Cette relation qui impactée par l'Internet des objets connaît une importante évolution qui semble aujourd'hui plutôt positive.

2- L'impact de la collecte des données sur la relation entre le professionnel de santé et son patient

Le concept de « santé connectée» marque une rupture qui n'est pas simplement « technologique »[26]. En effet, l'Internet des objets a modifié la relation entre d'une part le médecin et d'autre part, le patient. Les objets connectés ont permis de renforcer la dimension collaborative de la consultation. C'est pourquoi certains n'hésitent plus à utiliser le terme de « consultation 2.0 ». Concrètement, cette nouvelle relation entre le patient et le médecin beaucoup plus interactive se caractérise par un partage des informations et d'autre part un processus fort d'autonomisation du patient. Ainsi, le patient et le professionnel sont aujourd'hui tous les deux connectés, entre eux mais également aux autres individus. Il apparaît ainsi que la relation entre le professionnel de santé et son patient a connu une évolution, pouvant initialement être qualifiée de « paternaliste » à une relation plutôt de

[24] MARLIAC NEGRIER (C.), *La protection des données nominatives informatiques en matière de recherche médicale, Tome* 2, PUAM, p.646

[25] LAVARDET (C.), « Les enjeux juridiques de l'Internet des objets », *JCP G, Semaine a,* n°23, 9 juin 2014, p.1154-1155

[26] Livre blanc de la santé connectée, pour entrer dans la médecine 2.0, Whitings, p.12

partenariat entre les deux individus.[27] Les médecins et les patients font preuve d'une curiosité de plus en plus importante à l'égard des objets connectés. L'appréhension des objets de santé connectée par le corps médical et les patients est toutefois progressive, même si l'attrait est aujourd'hui déjà très fort.

Ces constatations sont confirmées par le Conseil National de l'Ordre des Médecins. En effet, selon le CNOM, les applications mobiles de santé ainsi que les objets connectés ont vocation à devenir des outils « complémentaires » à la prise en charge du patient. Les objets connectés permettent d'apporter un soutien aux médecins et de renforcer la relation entre le patient et son médecin.[28] Il s'agit ainsi d'une relation beaucoup plus équilibrée, ce qui peut en partie expliquer l'attrait aujourd'hui constaté pour les objets connectés de santé.

Un exemple d'actualité permet d'illustrer ce propos. Ainsi, la marque Terraillon a annoncé en Janvier 2015 qu'elle allait prochainement proposer un « système » de coaching avec des balances connectées. L'idée est qu'un médecin partenaire pourra accéder de façon sécurisée aux données du avec lequel il pourra échanger de manière régulière afin d'assurer le suivi de ce dernier.

- ***Le médecin connecté***

Le médecin est ainsi devenu un « médecin connecté ». Par définition, un médecin peut être dit connecté dès lors qu'il répond aux e-mails de ses patients, qu'il participe à des plateformes collaboratives, qu'il utilise des applications mobiles de santé ou bien des objets connectés de santé pour améliorer l'interaction et renforcer la dimension collaborative avec son patient. Le médecin connecté est aussi le médecin qui recommande des applications mobiles de santé ou des objets connectés de santé à son patient. Il va, dans sa pratique notamment, utiliser dans son cabinet plusieurs objets connectés qui vont permettre d'envoyer vers sa tablette par exemple les données relevées pendant la consultation. Les avantages de cette connexion sont entre autres, le gain de temps et le renforcement effectif de la collaboration avec le patient. La médecine digitale peut être définie comme l'intégration des nouvelles technologies dans la prise en charge du patient associée au médecin connecté qui utilise ces outils en vue d'améliorer ses pratiques.[29] Il semblerait que la « santé connectée » soit aujourd'hui bien accueillie tant par les médecins que par les patients. En effet, les objets connectés permettent au suivi médical qui était auparavant réservé aux professionnels de santé de devenir désormais accessible à tous. En effet, alors que le secteur médical apparaissait comme « conservateur », il semblerait que les médecins soient plutôt réceptifs au développement des objets de santé connectée. Les chiffres issus d'une étude sur ce thème menée par *MediQual Research* semblent percutants et confirment ce constat. Ainsi, selon cette étude, 80% des médecins sont favorables à la santé connectée estimant qu'elle est une opportunité pour la qualité des soins, 1/5 souhaiteraient conseiller des applications mobiles dédiés à la santé ou au bien être mais 76% déplorent un manque d'information.

---

[27] ANONYME, « Connecté, le patient devient acteur de sa santé », 17 juin 2014, *www.visionmarketing.com*

[28] Contribution du CONSEIL NATIONAL DE L'ORDRE DES MÉDECINS À LA CONSULTATION PUBLIQUE DE LA COMMISSION EUROPÉENNE, « Le livre vert et la santé mobile », publié le 1er juillet 2014, *www.conseil-national.medecin.fr*

[29] Interview de Pierre Henri FREYSSINGEAS, « Santé 2.0 : Médecine Digitale et médecin connecté », *actuentreprise.com*

Une précédente étude, le 2e baromètre dans le cadre de l'observatoire *Vidal* publié en mai 2013, évaluait à 8% la part de médecins utilisateurs de smartphones en France qui auraient déjà recommandé une application de santé à leurs patients. Toujours selon cette étude dont les chiffres ont été évoqués lors de la conférence santé connectée du 18 septembre 2014[30], 56% des médecins utilisent des applications de santé. Les types d'applications téléchargées sont les bases de données médicamenteuses, les interactions médicamenteuses ou bien les actualités de santé.
Cette même étude révèle que 60 % des médecins sont équipés d'une tablette. Le développement des applications mobiles de santé s'est fait en 3 étapes : dans un premier temps, les applications mobiles ont connu leur apogée au début des années 2000, puis elles ont fait l'objet d'une commercialisation progressive qui a pris de l'ampleur à l'ère des smartphones, enfin la troisième phase est celle d'aujourd'hui et constitue une phase d'intégration et d'appropriation des applications de santé par les professionnels de santé.[31]
Selon une autre étude très récente[32], 3 médecins sur 4 estiment que les patients devraient être acteurs de leur santé en intervenant davantage dans leur traitement et le suivi de leur maladie (72%), 62% des médecins ont déjà prescrit un objet connecté médical, et 49% un objet connecté de santé grand public. Parmi ces objets grand public, on trouve les balances connectées ou les applications sportives.

- ***Le patient connecté***

D'autre part, le patient est lui aussi devenu « connecté ». Ce patient « connecté » est le patient qui devient acteur de sa santé en partie grâce aux objets connectés. Le terme « *empowerment* » est ici souvent évoqué pour décrire cette situation. « *L'empowerment* » se caractérise par une modification de l'organisation entre le patient et son médecin. En effet, avant le développement des objets connectés, il apparaît que confronté à un symptôme quelconque, le patient contactait son médecin. Or aujourd'hui avec les objets connectés, il appartient au patient « *de juger de sa situation* » afin de savoir si contacter un médecin est nécessaire et opportun.[33] « *L'empowerment* » permet alors dans une certaine mesure de responsabiliser davantage le patient. Ainsi, le patient est acteur de son suivi mais également du partage des informations avec le professionnel de santé et d'autres patients.

70 % des patients se disent prêts à s'équiper d'un objet connecté.[34] S'agissant du patient connecté, la notion clé est en l'espèce celle de « *Quantified Self* », qui peut en français se traduire par « l'auto-mesure » ou le « soi-quantifié ». Ce mouvement est apparu dans la Silicon Valley en 2007. Toutefois, il convient de souligner qu'il n'est pas réellement nouveau, mais qu'il a tout de même pris un nouveau tournant avec l'Internet des objets et les objets connectés. En effet, avant même l'apparition des objets connectés, certains médecins

[30] Conférence Santé connectée par CHARRONDIERE (H.), « Santé connectée, e-santé, télémédecine et numérique en santé », *Lesechosetudes*, 18 septembre 2014
[31] La lettre innovation et prospective de la CNIL, n°05/juillet 2013
[32] Etude Baromètre Santé 360 d'Orange Healthcare et MNH réalisée par Odexa, 19 janvier 2015
[33] Le livre blanc de la santé connectée, pour entrer dans la médecine 2.0, Whitings, novembre 2014, novembre 2014, p.7
[34] Etude Baromètre 360 d'Orange Healthcare et MNH réalisée par Odexa, 19 janvier 2015

pouvaient demander à leur patient de tenir un « cahier de bord » afin de mentionner un certain nombre d'auto-mesures. Cette pratique s'est toutefois énormément développée avec les objets connectés et l'enjeu apparaît différent dès lors que le *quantified self* peut avoir une finalité médicale, mais pas seulement, pour certains il est véritablement à l'origine d'un dépassement de soi.
Deux méthodes doivent être distinguées : soit l'information est envoyée du capteur vers l'application, soit l'utilisateur renseigne ses données au sein d'une application. Ce mouvement de *quantified self* se caractérise réellement par un aspect communautaire, source d'encouragement entre les utilisateurs.[35] Les utilisateurs se fixent des objectifs et l'aspect communautaire est très marqué et ce, notamment au travers du partage des données sur des réseaux sociaux.
Le *Quantified self* est défini par la CNIL comme l'ensemble des activités ayant pour but la comparaison de variables de mode de vie (alimentation, sport, sommeil). Ce concept repose sur l'existence de capteurs connectés et la finalité poursuivie par ce concept est le partage et la circulation de données à caractère personnel. Il convient de souligner que les patients semblent faire de plus en plus attention à leur corps et leur santé. Par ailleurs, un certain nombre de smartphones sur le marché sont équipés de capteurs permettant de récolter des données dites de santé.

La problématique juridique qui va se poser est relative à la collecte et au traitement de données à caractère personnel. En effet, certains objets connectés en matière de santé vont traiter ce type de données pour les besoins de leur fonctionnement. Ainsi, le *quantified self* aboutit à de nouvelles formes de partage de données personnelles d'un nouveau genre, tant au niveau des modalités que du type de données concernées. Aujourd'hui certains mettent en évidence « l'extériorisation de l'intimité » qui s'est développée avec le partage intensif des données sur le réseau social Facebook ».[36] La CNIL se montre très méfiante et prudente à l'égard de ce concept. En effet certaines informations récoltées peuvent avoir vocation à être stocker dans des *clouds*. Par ailleurs, il y a bien évidemment aussi le risque de détournement des capteurs connectés. A l'heure où la cybercriminalité est en hausse, il semble que ces inquiétudes soient pertinentes. Malgré les éventuels risques, les objets de santé connectée séduisent néanmoins de plus en plus de français satisfaits de l'évolution de la relation qui les lie à leur médecin.

Aujourd'hui, le carnet de santé « connecté » est l'un des objets de santé qui permet d'illustrer le mieux concrètement le renforcement de la collaboration entre le patient et le médecin, et donc l'impact de l'Internet des objets sur une situation effective. Toutefois, c'est également l'un des objets qui soulève la problématique du « consentement » à la collecte et à la transmission des données. Le carnet de santé « connecté » n'est pas réellement un objet nouveau puisqu'il convient de souligner qu'il existe un précédent : le Dossier Médical Personnalisé (DMP).

[35] MEURIS (F.) « Les dangers du soi quantifié », CCE, 1er juillet 2014
[36] CNIL, « Le corps, nouvel objet connecté du *quantified self* à la m-santé : les nouveaux territoires de la mise en données du monde », cahier IP N°02, p.14

Le DMP a été une première forme de médecine digitale, il s'agit d'un carnet de santé numérique construit à partir de la carte vitale du patient. Avant la création du dossier, il existe une obligation d'information sur le fonctionnement et il faut nécessairement donner son consentement. Une fois celui-ci recueilli, le DMP peut être créé. S'agissant de la confidentialité des données, il est possible d'exiger que les documents ne soient accessibles qu'au médecin traitant. En outre, il est précisé que le principe d'ubiquité n'a pas vocation à s'appliquer : la médecine du travail, les mutuelles, les assurances, les banques ou employeurs ne peuvent en principe y avoir accès.
Le carnet de santé « connecté » apparaît comme l'évolution logique du carnet de santé numérique. Deux concepts ont été développés, l'un aux Etats-Unis par Apple : *Healthbook* est un dossier « e-santé » intégré à *IOS 8* qui permet aux utilisateurs de suivre leur état de santé via des applications tierces dédiées sur l'Iphone. Un autre carnet de santé connecté a été développé en France. Il s'agit *d'Humanlife* qui a remporté le prix du trophée des objets connectés. Ces carnets de santé connectés au sein d'une application mobile dédiée à la santé soulèvent de nombreuses problématiques, notamment s'agissant des données récupérées puis transmises au tableau de bord et au carnet de santé connecté. Nombreux sont ceux qui s'interrogent sur l'avenir de ces données une fois leur transfert opéré. Les développeurs de l'application *HumanLife* en France garantissent l'absence de réutilisation et évoque une « *relation de confiance avec leurs utilisateurs* ».
Dans le prolongement du carnet « de santé connecté », le « carnet de vaccination 2.0 » ou connecté a fait l'objet de l'actualité très récemment dès lors qu'il a été vainqueur des trophées de la santé mobile qui ont eu lieu fin janvier 2015. L'idée de cet objet apparaît très pertinente, dès lors que selon le professeur Jean-Louis Koek du Val-de-Grâce, près de 95% de personnes qui se rendent aux urgences n'emportent pas leur carnet de santé. L'objectif de ce carnet de vaccination qui peut être consulté par le biais de l'application smartphone *IOS, Android* ou bien depuis une tablette, un ordinateur est d'éviter aux patients d'oublier de se faire vacciner ou de le faire plusieurs fois. Le carnet de santé connecté pose également la problématique du consentement.

En raison du caractère sensible des données de santé, il apparaît nécessaire que le patient donne son consentement à la collecte et à la transmission de ces données. Le patient doit pouvoir s'exprimer à propos de la transmission de ses données. Aujourd'hui avec le développement très important des objets connectés, la problématique du consentement réapparaît. Nombreux sont ceux qui ont revendiqué un régime juridique spécifique aux données de santé. En effet, eu égard à leur nature, les problématiques et les enjeux semblent différents. Ainsi, il semblerait que le cadre juridique déjà existant doit aujourd'hui s'adapter aux évolutions liées à l'internet des objets. Le consentement exprès de l'individu est nécessaire en cas d'hébergement de données de santé. Par ailleurs, le consentement est requis pour l'accès au DMP pour le personnel de santé. Pour le médecin coordinateur, il faut un accord. Enfin, pour les réseaux de santé, il faut un document d'information signé.

Qu'en sera-t-il des objets connectés de santé ? Comment s'assurer du consentement donné de l'utilisateur à la collecte des données et surtout à leur réutilisation ? En effet, c'est principalement la réutilisation des données qui aujourd'hui suscite un certain nombre de

craintes. C'est pourquoi, la CNIL notamment n'hésite pas à intervenir en amont, afin d'apporter des conseils à l'utilisateur et de les informer de leurs droits.

3- Les impératifs de sécurité et de confidentialité des données

Malgré l'essor continu que les objets connectés de santé connaissent actuellement, ces derniers ne font pas l'unanimité. Nombreux sont ceux qui s'interrogent et qui s'inquiètent. La CNIL se montre notamment très méfiante à l'égard du *quantified self*.

- ***Les préconisations de la CNIL pour une meilleure maîtrise des données personnelles de santé et de bien être***

Ainsi, la CNIL dans son rapport annuel a souligné que cette pratique induisait la circulation massive de données personnelles qui touchent en particulier à l'intimité et qui sont en général destinées au partage. La dématérialisation des données de santé doit ainsi faire face à des difficultés tenant à la sécurité et à la confidentialité de ce type de données. Ainsi, il convient de rappeler que les patients disposent d'un droit au respect de leur vie privée et d'un droit au secret des informations les concernant, prévu par la loi du 4 mars 2002 relative aux droits des malades. En outre, une protection est accordée à la confidentialité des données à caractère personnel par le code de la santé publique. [37] Toutefois, il est opportun de s'interroger sur le fait qu'il est possible de toujours garantir l'effectivité de ces droits avec l'essor des objets connectés. En attendant qu'un cadre juridique précis vienne délimiter les responsabilités, la CNIL qui se montre déjà méfiante, n'hésite pas à émettre de nombreuses préconisations. Comme nous le verrons plus tard au sein de ce rapport, des réflexions existent déjà sur la mise en jeu de la responsabilité des acteurs. Toutefois, il apparaît également que le patient doit également être actif.

Ainsi, le patient devenu « connecté » doit être en mesure de veiller à la confidentialité et à la sécurité des données le concernant, en faisant preuve de vigilance. La CNIL dans son cahier intitulé « le corps objet connecté » s'est intéressé à la problématique du contrôle et de la valorisation des données par l'individu. Cette maitrise pourrait être source *d'empowerment*.[38] C'est pourquoi, la CNIL a émis un certain nombre de conseils à l'égard de l'utilisateur adepte du *quantified self*. Le développement du mouvement de *quantified self* interroge et inquiète dès lors qu'il s'agit de données sensibles. La CNIL est donc intervenue afin d'émettre quelques conseils pour une meilleure garantie de la sécurité et de la confidentialité des données de santé. La Cnil a relevé un certain nombre de difficultés auxquelles l'utilisateur pourrait être confronté.[39]

[37] BALLET (P.), et BENEAT (A.), « Dématérialisation des données de santé : quels référentiels ? », Gazette du Palais, 22 janvier 2011, n°22, p.22

[38] « Le corps, nouvel objectif du *quantified self* à la m-santé : les nouveaux territoires de la mise en données du monde », cahier IP, n°2, *www.cnil.fr*

[39] MEURIS (F.), « Les dangers du soi quantifié », *CCE*, N°7, juillet 2014 p.2

Parmi ces préconisations, la CNIL incite les utilisateurs à utiliser un pseudonyme, puis elle conseille également de ne pas partager les informations issues du *quantified self* sur les réseaux sociaux de type Twitter ou Facebook. Elle invite les utilisateurs à ne partager leurs informations qu'à l'égard d'un cercle de confiance. Enfin, la CNIL conseille aux éditeurs d'effacer leurs données dès lors qu'ils n'utilisent plus un objet connecté ou une application.[40]
En outre, bien que certaines donnés ne soient pas classées sensibles, elles doivent toutefois faire l'objet de surveillance. Il s'agit d'autres types de données telles que celles relatives au bien-être d'un individu par exemple. Ainsi, une brosse à dents « connectée » permet de savoir où se situe un individu. Ce type d'information qui peut faire l'objet de détournement suscite la crainte.[41]Aujourd'hui, il semblerait que ces craintes soient corroborées par des chiffres qui permettent de les mettre en évidence. Ainsi, selon une étude très récente[42] : une personne sur deux (46 % des patients, 49% des médecins et 50% des français), exprime la crainte que la « *santé connectée représente une menace pour le secret médical.* » Une meilleure information du patient (pour laquelle la CNIL œuvre déjà) et des professionnels de santé qui utilisent les objets connectés de santé pourrait être une solution ou bien l'effectivité de la garantie sur la confidentialité des données par les hébergeurs pourrait également être une autre piste…
Il convient de souligner que la CNIL n'est pas la seule à s'inquiéter à l'égard des objets connectés de santé. En effet, le Conseil National de l'Ordre des Médecins a pu également émettre un certain nombre de réserves à l'égard des objets connectés.[43] Le CNOM a ainsi mis en garde contre « l'impact psychologique, la dépendance et l'encouragement à l'usage immodéré des applis mobiles et objets connectés ».

- ***Une difficile mise en œuvre de l'effectivité des droits du patient***

Le patient acteur de sa santé est également le patient acteur de la garantie de la confidentialité et de la sécurité de ces données. Il convient de rappeler que ce patient fait l'objet d'une protection particulière, en vertu de la loi du 6 janvier 1978. En effet, il dispose de plusieurs droits dès lors que des données personnelles et nominatives font l'objet d'une récolte. Ainsi, parmi ces droits, il dispose du droit à l'information, du droit d'accès et de rectification, et du droit d'opposition. Toutefois, l'interprétation de ce de dernier soulève des interrogations. Ainsi, selon Jean Frayssinet, la CNIL aurait développé s'agissant de ce droit, une double doctrine[44]. Certains s'interrogent sur le fait de savoir s'il s'agit d'une opposition immédiate (qui consistait dans « *le refus de répondre au moment de la collecte* » ou bien d'une opposition différée où le patient s'oppose « *avant la cession d'un fichier* ».) Ces droits sont également prévus au niveau du droit de l'UE à l'article 12 de la Directive relative à la

[40] LAVERDET (C.), « Données personnelles : la sécurité des données à l'ère des objets connectés », *Expertise des systèmes d'information*, n°392, 1er juin 2014, p. 215
[41] Mullenex (D.), « les objets connectés, une législation déconnectée de l'avenir industriel », *JCP G La semaine juridique, n°40,* 29 septembre 2014, p.1764
[42] Etude Baromètre 360 d'Orange Healthcare et MNH réalisée par Odexa, 19 janvier 2015
[43]- Contribution du CONSEIL NATIONAL DE L'ORDRE DES MÉDECINS À LA CONSULTATION PUBLIQUE DE LA COMMISSION EUROPÉENNE, « Le livre vert et la santé mobile », 1er juillet 2014
[44] MARLIAC NEGRIER (C.), *La protection des données nominatives informatiques en matière de recherche médicale, Tome* 2, PUAM, p.477

protection des données (droit d'accès), et à l'article 14 de la Directive relative à la protection des données (droit d'opposition).[45]
Aujourd'hui ces interrogations sont toujours pertinentes dès lors qu'avec l'Internet des objets, les données de l'individu ont vocation à être de plus en plus souvent sollicitées et réutilisées. Dès lors, il semblerait que la garantie des droits pour le patient devrait être renforcée.

Aujourd'hui il semblerait que les craintes que peuvent susciter les objets connectés justifient un encadrement et un régime juridique qui soit propre aux données de santé.[46] En effet, les données de santé sont de plus en plus sollicitées afin de permettre notamment un meilleur ciblage de l'individu et aujourd'hui la demande de ce type de données a vocation à croître de façon continue. La sollicitation des données de santé de la part des assurances, de la recherche, de l'employeur devient de plus en plus envahissante et pourrait être à l'avenir encore plus intrusive.
C'est pourquoi, un encadrement juridique strict apparaît nécessaire s'agissant non seulement de la transmission mais également de la réutilisation des données de santé.

B- Une protection nécessaire de la réutilisation des données de santé

Les données de santé servent certes dans un premier temps à mesurer ses efforts personnels, afin de se réguler et contrôler son hygiène de vie et sa santé mais également pour comparer ses résultats avec ses proches via les réseaux sociaux suite à la collecte sur des applications mobiles.
Jusque-là, les données collectées apparaissent anodines et sans grande valeur pour l'individu mais pourtant, ces données peuvent avoir une toute autre signification selon la personne qui la collecte. Le monde des objets connectés à l'heure actuelle rime avec celui du Big Data qui entraine un potentiel énorme d'exploitation et une valeur marchande inattendue, en tout cas du point de vue du détenteur de l'objet initial[47].

1- La croisée des données anonymes

Les données de santé sont en plus normalement sensées rester anonymes lorsqu'elles sont collectées par les centres de recherches médicales ou par les statisticiens. Cette anonymisation apparaît quelque peu hypocrite car la croisée des données, notamment avec l'omniprésence avérée aujourd'hui du Big Data permet dans la plupart des cas de ré-identifier la personne concernée sans aucun problème.
C'est pourquoi, ces données qui ont souvent une caractéristique étroitement personnelle avec leur détenteur identifient l'être humain et l'individualisent. C'est là qu'un nouveau problème se pose puisque ces données ne sont pas censées être divulguées car elles sont destinées à des professionnels de santé qui n'ont normalement pas besoin de savoir de qui il s'agit. Or cette

[45] ANONYME, *Manuel de droit européen en matière de protection des données*, Office des publications de l'Union Européenne, Luxembourg, 2014, p.111
[46] MARLIAC NEGRIER (C.), *La protection des données nominatives informatiques en matière de recherche médicale, Tome* 2, PUAM, p.642
[47] WEINBAUM (N.), « Les données personnelles confrontées aux objets connectés », *CCE*, n°12, décembre 2014, p17

identification va permettre de suivre l'individu en tant que personnalité unique et distincte et l'enjeu de la traçabilité[48] va encore plus trouver de sens avec l'Internet des objets.
Au-delà de l'Internet des objets, la dématérialisation des données et l'ubiquité de celles-ci, pouvant se retrouver dans toute sorte de capteurs, entrainent une véritable identification indirecte du porteur. Chaque donnée ainsi isolée, comme la vitesse à laquelle la personne mange ou son rythme cardiaque, n'apporte pas beaucoup d'informations sur le patient mais une fois qu'elles sont recoupées avec les caractéristiques physiques et les habitudes de celui-ci, l'identification grâce à des serveurs est un jeu d'enfant.
Chaque donnée prise individuellement n'a pas grand intérêt mais plusieurs données regroupées indiquent énormément d'informations sur la personne. Une information banale acquiert une multiplicité de valeur.

Même si le cadre législatif pourtant strict en la matière indique l'importance de la confidentialité des données de santé par la loi du 4 mars 2002, et que la loi du 1er juillet 1994 modifiant celle de 1978 permet l'échange des informations de santé sous certaines conditions et pour la recherche médicale, ces comportements sont à surveiller avec la multiplication des objets connectés.
Bien que ces lois parlent bien d'une finalité médicale à cette collecte d'informations personnelles même anonymes, il est de plus en plus fréquent que les données de santé arrivent chez des professionnels des milieux mercantiles.
Pourtant la CNIL cherche depuis longtemps à interdire la commercialisation des données de santé directement ou indirectement et ceci, même si elles sont anonymes, comme pour la prospection commerciale.[49]
Le caractère ubiquitaire des données de santé donc entraine des risques quant au principe de finalité[50] pour lequel les informations ont été collectées. Le patient devrait toujours pouvoir savoir qui dispose d'informations à son sujet et dans quel but.
En effet, des acteurs économiques différents peuvent avoir complètement intérêt à récolter ces données qui ont une grande valeur sur le marché économique.
Si le principe d'ubiquité a pour mérite d'éviter l'impunité, il pose d'énormes problèmes en matière de responsabilité car toutes les informations transmises à divers destinataires doivent respecter un principe de finalité afin qu'elles ne soient pas exploitées à de mauvaises fins.

2- Le droit à l'information des acteurs non médicaux

En effet, avec le vif débat autour de la patrimonialisation des données relatives à la santé, se cachent de véritables enjeux pour les banquiers, assureurs ou encore publicitaires.
Par exemple, pour le cas du milieu des assurances[51], la transparence des rapports réciproques entre les assureurs et les assurés se traduit par une obligation d'information.

---

[48] PEDROT (P.) dir., *Traçabilité et responsabilité – Le traitement des données médicales informatisées : un nouveau défi à la traçabilité*, Economica, Paris, 2003, pp. 137-153.
[49] Délibération n° 01-011 du 08 mars 2001 portant adoption d'une recommandation sur les sites de santé destinés au public, *www.cnil.fr*
[50] Principe notamment repris dans les lois n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique dite LCEN et la n° 78-17 du 6 janvier 1978 dite Informatique et Libertés

Le droit à l'information de l'assureur est d'autant plus légitime que le cocontractant est censé avoir consentit préalablement lors de la conclusion du contrat. Parfois le contractant consent implicitement mais cela n'équivaut pas à un droit de prestation pour l'assureur, il ne fait donc pas ce qu'il veut de ces données.[52]
L'assureur doit informer le souscripteur via le contrat de toutes les modalités de garanties et les conditions générales concernant les données personnelles de santé collectées par l'Internet des objets, ainsi que les conséquences que ces dernières pourront avoir sur le contrat d'assurance. Le consentement de l'assuré doit alors être recueilli dès la signature du contrat.
Ceci permet une véritable confiance entre ces collaborateurs contractants.
Quant à l'assuré, ses obligations sont définies par l'article L113-2-2 du code des assurances puisqu'il a une obligation de bonne foi, de sincérité et de loyauté envers l'assureur.
Pour l'assurance des personnes par exemple, un questionnaire de santé doit être rempli, questionnaire qui peut désormais l'être en temps réel et de manière continu par un bracelet connecté par exemple. Ce questionnaire intervient ainsi dans la phase pré contractuelle avec les assureurs qui peuvent exiger des informations sur l'état de santé afin d'apprécier le risque et tarifer en conséquence.[53]
Mais dès lors, un certain déséquilibre existe entre les cocontractants puisque l'assuré découvre un nouvel objet qui lui parait être un gadget et qui va lui permettre de se motiver à avoir une meilleure hygiène de vie certes, mais sans savoir que l'assureur va agir en fonction des résultats. Des cadeaux seront offerts pour les assurés sérieux, c'est l'exemple du podomètre *Withings*, offert par Axa aux 1000 premiers souscripteurs du contrat d'assurance santé *Modulango*. En effet, le compteur *Pulse* va par exemple mesurer le nombre de pas, les dénivelés ou la distance et la société *Axa* propose un jeu de défi visant à faire le plus de pas possibles par jour, si les 10 000 pas sont atteints par jour pendant un mois, les assurés gagneront des surprises. La société promet ainsi l'obtention de deux chèques de médecine douce d'une valeur de 50 euros chacun et 20% de remise sur le site withings.com.
Des assurés en bonne santé rendent l'assureur comblé car les risques sont minimes. L'assureur pourra utiliser cet outil dans un but autre que celui prévu dans le contrat et les risques d'exploitation abusive vont se multiplier également entrainant une nouvelle forme de discrimination.

L'argent est connu pour être un objectif motivant pour les personnes en général et cette initiative des assurances pousse les assurés à contrôler leurs excès et à trouver une motivation supplémentaire à vivre de manière saine. Les assurances y voient aussi un autre avantage : les objets connectés permettent également de lutter contre les fraudes à l'assurance. En effet, le secret médical est souvent utilisé en assurances pour frauder. L'assuré bénéficie par exemple d'une aide importante pour la survenance d'un sinistre sur sa personne, même si ce sinistre est faux.

---

[52] CCass 1ère civ, 13 novembre 2008, n° 07-18-364, Bull civ II, n°240
[53] CCass 1ère civ, 29 octobre 2002, n° 99-17-187, Bull civ I, n° 244

Le secret médical reste ainsi une garantie et une protection optimale pour empêcher les assurances de s'immiscer dans les données de santé de l'assuré.[54]
De plus, le secret partagé entre le médecin conseil de l'assurance et le médecin traitant de l'assuré est prohibé.[55]
L'assureur n'avait donc souvent pas d'autre choix que de lancer une expertise judiciaire même si l'intérêt légitime de l'assuré est constamment défendu par la juridiction française[56].
L'assureur est ensuite contraint par le secret professionnel au détriment du secret médical mais il ne sera pas le seul puisque le banquier subira les mêmes limites à la liberté d'entreprendre, tout comme les publicitaires.
Les publicitaires ne pourront trouver que des avantages à la multiplication des objets connectés de santé puisqu'ils permettront le ciblage comportemental sans qu'il y ait besoin d'agir après la délivrance de l'objet. Toutes les données collectées qui seront enregistrées sur le smartphone relié à Internet permettront à tout professionnel du marketing d'adapter le message publicitaire à chaque intéressé. Au même titre que les publicités intrusives rencontrées sur le web, la moindre information collectée sur n'importe quel capteur de santé pourra renseigner de manière efficace, gratuite et rapide, les annonceurs qui pourront augmenter leur chiffre d'affaire du fait de l'amélioration du message transmis par la publicité.

Ainsi, les données de santé prennent une toute autre valeur, plutôt mercantile qui intéressera des acteurs économiques variés, qui les exploiteront de différentes façons sans que le consentement soit de nouveau collecté.
D'autant plus, que les assureurs par exemple ne sont pas liés par le secret médical étant donné qu'ils n'appartiennent pas à ce domaine mais peuvent être liés par le secret professionnel établit par l'article 226-13 du code pénal s'ils en ont fait la promesse déontologique à l'origine de leur communication marketing.

3- Le principe de précaution obligatoire pour les objets connectés des personnes âgées

Les maisons de retraite[57] se retrouvent souvent dans l'actualité quand des drames surviennent telles que les fugues mortelles dues au froid ou aux accidents des personnes âgées fragiles de l'esprit. Ces faits relancent à chaque fois le débat traitant de la balance entre la sécurité de ces personnes et leur liberté individuelle.

Ainsi, imposer le port d'un bracelet connecté à tous les pensionnaires serait, au titre du principe de précaution, une bonne chose pour leur protection mais réduirait considérablement leur liberté. C'est pourtant ce qu'essaye de faire certains établissements, en ajoutant des caméras de surveillance dans tous les locaux ou encore, en équipant certains pensionnaires de

[54] BICHOT (P.), «Le secret médical : un outil redoutable à la disposition des assurés de mauvaise foi », *RLDC*, janvier 2005, p.13.
[55] Rapport SAURY, « Secret médical et entreprises d'assurances », publié par le Conseil National de l'Ordre des Médecins, avril 2000, *www.conseil-nationall.medecin.fr*.
[56] Cour de Cassation, 2ème civ, n° de pourvoi 04-13509 du 2 juin 2005.
[57] MAZEN (NJ.), BEVIERE-BOYER (B.), « Ethique et droit du vivant », *Revue Générale de Droit médical*, Les Etudes hospitalières, Bordeaux, juin 2014, pp.271-299.

cannes connectées permettant de les localiser même hors des bâtiments. En effet, la canne japonaise de chez Fujitsu baptisée *New Generation Cane* est un prototype à la base créé pour les aveugles afin qu'ils puissent se guider de manière autonome, mais cet accessoire peut également servir à surveiller les personnes l'utilisant.
Le problème majeur est bien qu'il y ait ici un gros risque de stigmatisation, de généralisation des évènements d'actualité sur l'ensemble des pensionnaires de ces établissements.
Dans l'intérêt des concernés, un Comité National pour la Bientraitance et les Droits des personnes âgées et handicapées a été mis en place pour prévenir les risques d'abus des droits de ces personnes du fait de la géo localisation ou la télésurveillance. [58]
Un problème de recueillement du consentement des personnes est évidemment présent car elles ne peuvent dans la plupart du temps pas donner leur avis sur ces dispositifs qui pourtant, est normalement obligatoire.[59]
L'institut qui accueille la personne âgée privilégiera toujours le bien-être et la sécurité de l'intéressé ainsi celle que des autres personnes, pensionnaires ou personnels soignants. D'où le développement des mesures restrictives de liberté pour les personnes sensibles, tels que des bracelets ou puces connectés, solutions prises pour 18% des EHPAD pour prévenir les fugues[60].
Les progrès sont démultipliés avec les objets connectés afin d'être plus doux dans l'environnement du malade ou de la personne âgée. La canne connectée par exemple permet aux personnes affaiblies d'indiquer par des pointillés lumineux au sol le chemin le plus rapide pour trouver un point de repos. Le quotidien de ces personnes affaiblies en devient facilité grâce à ces petits accessoires hight tech.
La robotique ou domotique permet de favoriser le bien-être de ces personnes qui pourront continuer à être stimulées et vivre une vie presque « normale », diminuant par la même occasion leur isolement social.

Une autre question se pose quant à la qualification de certains objets connectés qui apparaissent d'une utilité évidente mais qui n'agissent pas sur le corps directement. C'est par exemple le cas des détecteurs de fumée qui enregistrent des données liées à l'environnement de la personne. Si les bénéfices sont effectivement faciles à déterminer, il n'en reste que ces objets interviennent de manière imposée dans la vie de la personne, d'autant plus si c'est une personne fragile comme une personne âgée ou handicapée qui n'aura pas toujours envie que ces proches par exemple, aient accès à des informations telles que la température de leur habitat.
La gazinière qui s'éteint pour éviter l'incendie, ou le détecteur de l'air ambiant qui prévient les proches en cas de chaleur trop forte, sont beaucoup plus intrusifs et surveillent la personne parfois même au-delà du raisonnable. Le plus gros problème reste surtout vis-à-vis du consentement notamment pour les personnes âgées puisque les collectes de santé réalisées pour rassurer leurs proches se font parfois sans leur consentement. C'est l'exemple de *Lysbox*,

[58] Création le 7janvier 2013 suite à la volonté du gouvernement de confier ces missions de contrôle à un organisme indépendant.
[59] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé
[60] Enquête de 2013 réalisée par la Fondation Médéric Alzheimer auprès de 5690 établissements, « La lettre de l'Observatoire », n° 27, juillet 2013, *www.fondation-mederic-alzheimer.org.*

cette box créée dans le Loiret qui envoie des données sur l'air ambiant au sein de la maison d'un proche à toute la famille. Mais le cas des collectes de données de l'air ambiant chez une personne âgée par exemple envoyées à sa famille correspond-il à une situation réciproque comme lors d'un rapport médecin/ patient ? Les données collectées sont-elles des données de santé ? Oui, car elles concernent bien l'intimité du propriétaire et son environnement direct donc le consentement doit aussi être recueilli. Ainsi, comme cela a déjà été vu précédemment, c'est une condition essentielle à la collecte des données médicales.

Une réelle obligation de sécurité doit être respectée car le détournement de la finalité est souvent possible.
Un véritable principe de proportionnalité devra alors être dégagé pour mesurer la balance entre les avantages et les inconvénients en fonction de la situation pour permettre d'adapter les objets au sujet.
La mise en place de tels objets doit être réalisée dans des cas particuliers et ne doit en aucun cas être généralisée à toute une catégorie de personne. Les innovations peuvent être une bonne chose selon l'utilisation qui en sera faite.
L'importance du principe de finalité trouve toute sa force lors de l'exploitation de ces objets connectés puisque les conséquences qu'ils peuvent avoir sur les droits des individus sont parfois disproportionnées par rapport au but poursuivi.

La première partie a donc mis en exergue la nécessité de l'encadrement de ces objets qui génèrent de nombreuses données. Celles-ci ont une valeur utile pour les recherches médicales mais également une valeur marchande d'où leur ubiquité puisqu'elles se retrouvent exploitées par divers acteurs dans divers endroits au même moment. Pourtant, il est évident que les données corporelles sont des données sensibles qui doivent être protégées durant toutes les phases d'exploitation, c'est-à-dire de la collecte au traitement final. Le cadre légal en matière de protection du transfert des données dans le cadre de la carte vitale par exemple est ainsi déjà bien admis et peut être étendu aux objets connectés.
Mais est-il réellement suffisamment ? Depuis l'essor de l'internet des objets, de nouveaux délits apparaissent quant à l'utilisation abusive de ceux-ci, entrainant des conséquences juridiques inévitables.
Le droit français est dans de nombreuses matières, très en retard par rapport à la réalité, et le milieu technologique en est la preuve. C'est pourquoi, la dernière partie de ce rapport traitera des solutions envisagées par les instances étrangères, que ce soit en Europe ou hors de l'Europe.

II/ Un encadrement insuffisant dû à l'utilisation abusive des objets connectés de santé

Maintenant qu'il a été démontré de quelle manière fonctionnent les objets connectés liés à la santé, il est temps de voir de quelle manière ces mêmes objets et ces mêmes techniques peuvent également devenir des abus.

Il est certain que dès lors qu'un individu possède un objet connecté, et plus précisément un objet de santé, beaucoup d'informations sur la personne sont envoyées un peu partout dans le monde afin d'être ensuite reçues chez le médecin, dans l'ordinateur, à la banque, chez assurance etc. C'est pourquoi, les conséquences juridiques liées aux abus de l'utilisation des objets connectés doivent être prises en compte (A).
Ainsi entre le moment où les données partent de l'objet connecté pour arriver chez le destinataire, elles sont conduites via des réseaux de communication (ondes hertziennes, câble etc). Or rien n'est plus facile pour quelqu'un de malveillant et de spécialisé de voler ces données. Il apparaît toutefois que ces risques sont déjà pris en compte ailleurs (B).

A- Des conséquences juridiques liées aux abus de l'utilisation des objets connectés

L'encadrement juridique des objets connectés de santé apparaît insuffisant à de multiples égards.

1- Un risque important d'ingérence par des tiers

D'après le rapport d'Europol rendu en 2013[61], le premier meurtre par Internet était estimé en 2014 donc les risques d'ingérence par les tiers sont connus depuis déjà quelques temps.
Le tiers en question peut être n'importe qui : le voisin, le partenaire mais également une personne à l'autre bout du monde, voir même un terroriste ou toute autre personne dangereuse.
En effet, le risque d'ingérence consiste à ce que ce tiers via toute les données qu'il a pu recevoir de l'intéressé, vole des informations importantes, se fasse passer pour lui, fasse des choses illicite en son nom, s'amuse à pirater tous les systèmes ou bien dans les cas plus extrêmes peut même directement s'en prendre à l'individu.

Ce qu'il faut bien comprendre c'est que le fonctionnement de ces objets de l'internet repose sur le traitement des données. Ainsi ces objets soulèvent des problématiques d'ordre juridique, telles que la conciliation de leur utilisation avec le respect de la vie privée, le respect de la règlementation du traitement des données personnelles, mais ils posent également des problèmes par rapport à la sécurité et la confidentialité des données liées à leur exploitation, ainsi que la propriété de ces données et le « droit au silence » de ces objets.

De plus, toujours concernant le cadre juridique, la gestion des données récoltées risque également de poser problème. En effet, les organismes juridiques se penchent de plus en plus

[61] Rapport EUROPOL 2013, *www.europol.europa.eu*

sur la question. Ainsi, c'est à travers sa « *Lettre innovation et prospective* » n° 4 parue en Mars 2013 que la Commission Nationale de l'Informatique et des Libertés (CNIL) a déclaré s'intéresser de près aux nouveaux objets et services qui créent, stockent des données personnelles et tracent nos activités. [62]

Il est vrai, comme nous l'avons déjà précisé, que les objets utilisent des réseaux de communications pour fonctionner. Or ces réseaux ne disposent pas nécessairement d'antivirus ou de logiciels de protection. Ainsi, le marché des objets connectés a vocation à devenir un immense terrain de jeux pour les hackers, ou autres cybercriminels.
Il s'agit là d'une préoccupation récurrente car ces nouvelles technologies ont pour but d'être partout autour de nous. Elles vont donc « *former un écosystème omniprésent mais qui sera très vulnérable au piratage, à l'intrusion et « crash » en tous genres*. C'est un avertissement réel qui a déjà été relayé de nombreuse fois et par de nombreux experts en sécurité tel que Bruce Schneier.
En effet ces objets connectés, et principalement ceux liés à la santé, décuplent les dangers car ils envoient des données strictement personnelles mais également parce qu'ils touchent directement la santé de l'individu.

S'il est facilement imaginable que quelqu'un puise pirater le compte en banque d'une personne, autant que de se faire voler son identité, cela ne suppose pas nécessairement une fin tragique. Il est moins évident de s'imaginer que l'on pourra également à distance recueillir toute les informations nécessaires afin de blesser cette personne.
Dans un secteur un peu plus éloigné de la santé déjà traité dans certains films comme la sécurité, il est fréquent que des personnes piratent les freins d'une voiture par exemple afin de causer un accident. Aujourd'hui cela peut être possible à distance grâce aux voitures connectées.

Ceci ne relève donc plus de la fiction et concerne également aujourd'hui, le domaine de la santé.
Barnaby Jack, un célèbre hacker aujourd'hui décédé, avait déjà démontré en 2011 qu'il était possible d'injecter une dose létale à un utilisateur de pompe à insuline en exploitant les failles de l'appareil. En 2012, il a prouvé qu'il pouvait y arriver à une distance d'environ 90 mètres par le biais d'une antenne à haut-gain.
De plus, toujours en 2012, Jack présentait au *BreakPoint* de Melbourne, les résultats de travaux montrant qu'il était possible d'assassiner un porteur de stimulateur cardiaque, confirmant ainsi les travaux théoriques qu'il avait effectué en 2008.[63]
Pour rejoindre cette étude, on peut citer l'exemple du vice-président américain Dick Cheney. En effet, alors qu'il est porteur d'un stimulateur cardiaque, ce dernier a vu les fonctions sans-fil de son pacemaker désactivées afin d'éviter toutes attaques potentielles. En effet, il est normalement possible de stimuler ou d'éteindre à distance, à l'aide d'un code sécurisé le dispositif cardiaque. Ainsi, le vice-président craignant qu'on ne l'assassine à distance, a pris

[62] CNIL, « Lettre innovation et prospective », cahier IP n° 4, *www.cnil.fr*
[63] GAGNON (B.), « Internet finira par vous tuer, ou les conséquences du tout connecté tout le temps », 21 octobre 2014, *www.branchez-vous.com*

les devants en décidant de désactiver cette option. [64]

Cette idée d'attaquer à distance un appareil électronique relié au corps humain avait déjà fait l'objet d'un épisode de la série *Homeland*. En effet lors de la saison 2 de la série, des pirates informatiques assassinent le vice-président des Etats-Unis en s'infiltrant dans son pacemaker, et en déclenchant un choc électrique fatal.
Lors de la diffusion de cet épisode les critiques avaient été nombreuses sur le fait que la science-fiction avait un caractère trop présent. Toutefois, au regard des récentes avancées technologiques, les sceptiques vont peut-être devoir très prochainement reconnaître la possibilité d'un tel scénario.
Ce genre d'attaque reste pour le moment relativement rare, et cela principalement parce que ces cibles ne représentent pas pour l'instant d'intérêts financiers. En effet, les pirates informatiques préfèrent un gain financier, en volant des numéros de carte de crédit par exemple. Toutefois, la situation pourrait rapidement changer car plus ces objets connectés deviendront présents et multifonctionnels, plus il y a de chances pour que leurs fonctions premières soient détournées par des gens malintentionnés ou par des manœuvres accidentelles.

Or, la question se pose de savoir quelle serait la conséquence et la responsabilité d'un tel accident ? Quelles sont les manières de les prévenir et les éviter ?
Que faire, vers qui se retourner, en cas de panne, de non fiabilité de l'information, d'accident causé par l'objet connecté ?
C'est là qu'entre en jeu le régime de responsabilité de ces objets connectés.

2. Un régime de responsabilité partagé entre fabricant et utilisateurs

Il serait trop simple de dire que seule une personne serait responsable et ce peu importe le problème. En effet, plusieurs critères sont à prendre en compte. Tout d'abord, il faut effectivement s'assurer que l'objet en lui-même ne soit pas défaillant, mais ensuite c'est l'utilisateur lui-même qui devra s'assurer de sécuriser du mieux possible son objet. Ainsi cela nous donne un double régime de responsabilité.

- ***Le régime de responsabilité du fabricant***

Lorsqu'on parle de responsabilité du fabricant, on visualise tout de suite un problème dans la fabrication, le montage de l'objet, mais il peut également s'agir d'un problème de fonctionnement dans le cas où l'objet n'agit pas tel qu'il le devrait.
Par exemple si l'on s'éloigne un peu du secteur de la santé, qui serait responsable en cas d'accident impliquant un véhicule sans pilote tel que la *Google car* ?[65] Si la voiture cause un accident, qui sera considéré comme responsable étant donné qu'il n'y a pas de conducteur ? Il

[64] ANONYME, « Dick Cheney, menacé comme dans "Homeland" ? », 22 octobre 2013, *www.telerama.fr*
[65] Conférence, par QUEMENER (M.) et SCHMOLL (S.) « Les objets connectés », 23 septembre 2014, *www.blog.dmi.com*,

n'existe pas aujourd'hui de définition de la notion de « conducteur » dans la loi. Or la Convention de Vienne dit seulement qu'il *« est celui qui assume la direction du véhicule »*. Ainsi, on a besoin d'une véritable adaptation de la législation. On peut imaginer que la responsabilité d'un tel accident soit imputée au constructeur mais encore faut-il s'assurer que l'accident provient bien d'un problème technique et non d'une erreur d'un des passagers.
Pour se rapprocher du secteur de la santé, l'exemple du drone est de mise. En effet il a été mis en place des drones pouvant venir secourir en premier lieu des personnes ayant des problèmes cardiaques. Que faire si celui-ci ne fonctionne pas ? Que faire s'il blesse quelqu'un au passage ou bien tue par erreur le malade ? Qui dans ce cas sera considéré comme responsable ?

Dans le cadre juridique actuellement admis, seul 20% des objets connectés sont concernés par la législation. Il faut donc penser à créer des textes applicables aux usages quotidiens car le droit s'adapte difficilement à la multiplicité des technologies.
Il convient cependant de relever que certaines lois sont pérennes et permettent d'appréhender cette problématique des objets connectés. C'est le cas de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ou de la loi du 5 janvier 1988 relative à la fraude informatique
Un projet de règlement sur le traitement des données personnelles est aujourd'hui discuté au Parlement européen. Il a vocation à s'appliquer à l'ensemble des Etats membres et à régir de nombreuses notions telles que le droit à l'oubli. Ce règlement va engendrer de nombreuses questions dans un futur proche.

Mais en attendant, les fabricants se sont protégés via des clauses limitatives. En effet, en cas de défaillance, les fabricants auront prévu dans le contrat des clauses limitatives de responsabilité, qu'ils tenteront d'opposer aux garanties contractuelles et légales (notamment l'article 34 de la Loi Informatique et Liberté[66] ou sanctions pénales prévues par la loi Godfrain).
De plus, les fabricants devront prouver qu'en cas d'accident, l'utilisateur serait fautif du fait de la mauvaise utilisation de son objet. Ainsi, il peut exister une deuxième hypothèse quant à la responsabilité.

- ***Le régime de responsabilité de l'utilisateur***

Le régime de responsabilité des utilisateurs prend en compte deux éléments. Tout d'abord celui de la « bonne pratique » qui consiste à se montrer plus intelligent que les objets connectés en faisant son maximum pour protéger ses données. Pour cela, il faut mettre en place des mots de passe, des cryptages de données et au minimum, faire les mises à jour régulières de l'objet afin de s'assurer de la meilleure sécurité possible.
Malgré le fait que dès qu'un objet connecté est mis en circulation, la CNIL doit s'assurer du traitement des données, il n'empêche que l'utilisateur doit faire attention.

En effet, en plus de ces démarches pratiques, celui-ci devra également s'assurer de « traiter »

[66] Loi n° 78-17 du 6 janvier 1978 dite Informatique, Fichiers et Libertés

l'objet connecté comme il se doit. Cela se traduit par une obligation de véracité lors de la configuration de l'objet. Il est vrai qu'il n'y a que peu d'intérêt à mentir sur nos informations personnelles puisque celles-ci sont censées n'être visibles que par nous. Il n'empêche que cela pourrait entrainer un problème de fiabilité dans les données en faussant les résultats et cela pourrait par la suite avoir des conséquences importantes selon la personne qui les reçoit (médecin, assurances...). L'idée de prêt de l'objet est fortement déconseillée.
Ainsi, ces mesures réalisées en dehors d'une supervision soulèvent plusieurs séries de questions dont celle de la fiabilité des dispositifs utilisés et par voie de conséquence des données captées et analysées. Une relation nouvelle doit donc s'établir entre l'utilisateur et le fabricant d'objets connectés : « *avec les objets connectés, l'utilisateur accepte que le fabricant ait accès à ses données de manière à ce qu'il puisse l'aider s'il y a un dysfonctionnement* ». Par conséquent, l'une des manières de prendre en compte cette problématique de la fiabilité serait peut-être de recourir à des tiers de confiance.

3. Une nouvelle preuve admise par le droit

En France « *la nécessité de la preuve incombe à celui qui se plaint* ». Ainsi la présomption d'innocence dont dispose l'accusé peut être renversée en cas de présentation d'une preuve basée sur des faits. On admet plusieurs sortes de preuve, les simples et les irréfragables.
De plus en plus de lois sont mises à la disposition des forces de l'ordre afin de pouvoir accéder à toutes formes d'informations disposé à innocenter ou accuser une personne.
Par exemple, il est tout à fait concevable de voir nos historiques de recherche Google, nos envoies de mails, nos GPS examinés par la police afin d'alimenter et/ou constituer un stock de preuves afin d'essayer de prouver les actions et l'endroit où se trouvait l'accusé à tel ou tel moment.

Depuis le 28 mars 2014, la loi sur la géolocalisation a même été plus loin en offrant la possibilité pour la police judicaire d'utiliser « tout moyen technique destiné à la localisation en temps réel sur l'ensemble du territoire national, d'une personne, d'un véhicule ou de tout autre objet, sans le consentement de son propriétaire ou de son possesseur ».[67] En l'espèce, de telles mesures pourront s'appliquer que dans des cas extrêmes ou lorsqu'un certains nombres de critères seront remplis au préalable.
Bien sûr, cette loi ne concerne pas spécifiquement le droit de la santé, mais on peut facilement comprendre en quoi les objets connectés de santé pourraient jouer un rôle dans la localisation.

En effet, le principe même d'un objet connecté est de suivre une personne afin de pouvoir calculer des données. Or dans ces données, en plus des informations basiques que l'on cherche à connaitre telles que le nombre de pas, les calories mangées, le temps de sommeil, le tracé du chemin effectué etc. Il y a également toutes sortes de données secondaires auxquelles on ne prête pas attention mais qui, si on regarde de près, peuvent nous apporter des preuves concrètes de l'endroit où l'on se trouve. A quelle heure ? Pour combien de temps ? Ou encore,

[67] Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation

si telle ou telle personne avait une santé qui pouvait l'empêcher physiquement de faire quelque chose... Ainsi une telle source d'information est bénite ou maudite par la police, les avocats et les utilisateurs en fonction du résultat obtenu.

Un panel d'avocats canadiens l'a bien compris. Pour la première fois de l'histoire, un bracelet connecté sera utilisé comme preuve lors d'une affaire de responsabilité civile au Canada.
En effet, le bracelet *FitBit* pourrait bien aider les juges canadiens de Calgary à déterminer les conséquences d'un accident et calculer les indemnisations des victimes.[68] Les données accumulées dans ce bracelet seront présentées par l'avocat d'une plaignante pour prouver qu'elle est moins en forme que la moyenne à cause d'un accident. Les avocats veulent prouver ainsi que le comportement de la victime ainsi que son activité sont statistiquement inférieurs ou dégradés par rapport à celle d'un individu « normal ». On entend ici par normal une personne du même sexe, du même âge et de la même profession.

Jusqu'à maintenant, lors de ce type de procès, c'était un médecin-expert qui, après une visite et une observation médicale, rendait ses conclusions quant à la santé physique et mentale d'une personne.[69] Ainsi, on peut légitimement se poser la question de savoir si les objets connectés ne seraient pas les futurs médecins experts, car plus fiables et plus précis du au fait que le résultat serait obtenu grâce à des données prélevées durant des jours, des mois, voir même des années.

En l'espèce, dans le procès de Calgary, la demande de la victime a peu de chance d'aboutir car il n'existe pas de données préalables à l'accident. Ainsi les juges ne pourront avoir d'éléments de comparaison sur le comportement et l'activité de la plaignante. Or, sans cet « avant/après » il devient compliquer d'apercevoir les conséquences de l'accident survenues quatre ans auparavant.
Il n'empêche que cela ouvre la voie à de nouvelles possibilités en matière d'acceptation de preuves juridiques.
Bien évidemment, on peut de suite dire que les fabricants de ces objets connectés sont réticents à l'idée de partager publiquement l'ensemble des données de santé de leurs clients. Cependant, « *ils pourraient bien se voir contraints par la justice de les délivrer, un peu à l'image de ce que Facebook ou Twitter ont été obligés de faire dans certains cas extrêmes...*».[70]

De plus, une autre limite à cette utilisation peut être soulevée car à ce jour il est difficile de démontrer qui portait réellement l'appareil à un instant précis. Ainsi, les résultats finaux pourraient être faussés.

---

[68] GAUTIER (A.), « Un bracelet connecté utilisé comme preuve en Cour américaine », 1er décembre 2014, *www.webdesobjets.fr*
[69] ERTZSCHEID (O.), «Les objets connectés, nouvelle « boîte noire » enrôlée par la justice », 20 novembre 2014, *www.rue89.nouvelobs.com*
[70] BERTAUD DU CHAZAUD (J.), « Les données d'objets connectés : nouvelles preuves dans les procès ? », 25 novembre 2014, *www.droitdu.net*

Enfin, certains parlent déjà des objets connectés comme d'une boîte noire. Par exemple, Janic Tremblay, une journaliste canadienne disait que les « *wearable pourrait très bien devenir la boite noire des individus* ».[71] En effet, tout comme les boîtes noires dans les avions enregistrent ce qu'il se passe, les objets connectés enregistrent les moindres faits et gestes de la personne qui le porte.

La question qui se pose désormais est de savoir de quelle façon l'Europe se positionne quant à l'utilisation des objets connectés par rapport au reste du monde.

B- Des conséquences déjà prises en compte dans d'autres pays

Tous les pays n'en sont pas au même niveau concernant les objets connectés. En effet, certains sont plus en avance que d'autres, certains les approuvent, d'autres sont plus réticents et certains pays ont même déjà commencé à mettre en place des règles afin de s'assurer du bon respect de fabrication, d'utilisation, de circulation et de stockage des informations venant de ces objets connectés.

1- Une Europe des objets connectés en pleine croissance

L'internet des objets (IdO) n'est pas encore une réalité tangible, mais plutôt un champ de possibilité offert par un certain nombre de technologies qui pourraient, dans les 5 à 15 prochaines années, modifier en profondeur le mode de fonctionnement de nos sociétés.
Ainsi, en étant active, l'Europe pourrait jouer un rôle de premier plan pour mettre en place les règles de fonctionnement de l'IdO et elle pourrait en retirer des avantages économiques et sociétaux.[72] Ne pas tout mettre en œuvre pour y arriver reviendrait à manquer une occasion importante et l'Europe pourrait se retrouver contrainte d'adopter des technologies conçues au mépris de ses valeurs fondamentales, telles que la protection de la vie privée et des données personnelles.
La Commission, via son Parlement et son Conseil entend donc jouer un rôle majeur dans cet effort pour atteindre ces objectifs.
C'est pourquoi, la Commission Européenne a annoncé un nouveau financement de 100 millions d'euros à destination des jeunes entreprises et des PME de haute technologie dans différents secteurs, dont notamment celui des objets connectés.

Cependant, étant donné que l'Europe concerne plusieurs pays, cela implique plusieurs niveaux d'avancement, plusieurs systèmes juridiques, plusieurs cultures. C'est en regardant les termes du Livre Blanc « *Les nouveaux Eldorados de l'économie connectée* » portant sur les objets connectés, que l'on peut constater que le contexte juridique des objets connectés est encore instable à ce jour. En effet, il semblerait que l'Union Européenne soit en pleine

[71] ANONYME, « Les données d'un bracelet intelligent bientôt utilisées en cour », 27 novembre 2014, *www.ici.radio-canada.ca*
[72] Rapport de la COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS, « L'internet des objets – Un plan d'action pour l'Europe », 2009, *eur-lex/europa.eu*

réflexion sur le cadre juridique encadrant la collecte, le stockage et le traitement des données personnelles afin, tel qu'on l'a dit précédemment, d'éviter tout écueil dans la protection de la vie privée et des données personnelles.[73]

Pour le moment, la France est le pays le mieux connecté en Europe. En effet, le taux de pénétration de l'internet haut débit est de 70 % chez les particuliers et de 92 % dans les entreprises, soit près de 5 points au-dessus de la moyenne européenne. Ainsi, l'adoption des objets connectés par les français ne sera pas freinée par des problèmes techniques. [74]
De plus, le système français est dynamique, et dispose de compétences techniques. La France ne doit donc pas se laisser distancer et se doit de surveiller ses voisins, et même de s'en inspirer si nécessaire.

Il est évident qu'il faudra harmoniser les lois entre les territoires mais tant que cela ne sera pas mis en place, chaque pays sera libre d'avancer tel qu'il le souhaite à partir du moment où il respecte les lois de bases. Effectivement, « *au niveau de l'UE, il existe une proposition d'harmonisation règlementaire datant du 25/01/2012 et en France nous avons aussi un projet de loi numérique. Les lois du Parlement Européen, même si elles sont aménagées au niveau de chaque Etat, doivent être mises en pratique et respectées. En l'espèce les deux lois primordiale consiste en une transparence de l'information, une proportionnalité des durées de conservation, la finalité de la collecte, et enfin la pertinence des données et la territorialité.* » [75]

Quant aux objets connectés et à la santé même, pour l'instant le Conseil National de l'Ordre des Médecins met en avant huit points de vigilance quant au Livre vert de la Commission Européenne.[76] En effet, le CNOM a contribué à donner des informations telles que la nécessité de la protection des données recueillies et cela même dans des états extracommunautaires.

Pour le moment, la réglementation existante de l'Europe classe les données de santé parmi les plus sensibles, leur traitement est interdit sauf dans les cas définis dans la directive 95/46/CE.[77]
Le projet de règlement européen relatif à la protection des données personnelles, actuellement en discussion, définit pour la première fois les données concernant la santé, comme « *toute information relative à la santé physique ou mentale d'une personne, ou à la prestation de*

[73] ANONYME, « Objets connectés : opportunités et limites », juillet 2014, *www.objetconnecte.net*
[74] Rapport G9+, Livre Blanc « Les nouveaux Eldorados de l'économie connectée », décembre 2013, *www.g9plus.org*
[75] Rapport de l'école SKEMA, « Business rule breakers and the internet of everything, Le livre Blanc, la révolution du commerce par les objets connectés », 2014, *www.skema-mdce.fr*
[76] Contribution du CONSEIL NATIONAL DE L'ORDRE DES MÉDECINS À LA CONSULTATION PUBLIQUE DE LA COMMISSION EUROPÉENNE, « Le livre vert et la santé mobile », juillet 2014, *www.conseil-national.medecin.fr*
[77] Directive 95/46/CE 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

services de santé à cette personne ». Ainsi, l'hébergement de ces données doit être soumis à un agrément préalable du ministre de la Santé selon un décret du 4 janvier 2006.[78]

Ainsi, on peut voir que l'Europe essaie de lier du mieux possible le droit déjà existant aux nouvelles problématiques que soulèvent les objets connectés mais cela reste encore très obscure.
La solution serait peut-être alors de se rendre compte de l'avancement des autres pays afin de pouvoir comparer et pourquoi pas échanger les dispositions prises par chacun.

2 - Les tentatives législatives des pays hors UE

Au-delà de la tentative d'harmonisation de l'Union Européenne, d'autres pays dans le monde se sont concentrés sur la protection des données personnelles de santé. Même si les objets connectés en eux-mêmes ne disposent encore pas de régime propre, des pays comme le Canada, les Etats-Unis ou la Corée du Sud ont pris en compte la régulation de l'exploitation de ces données sensibles.

- ***Le cas canadien pour l'intelligence ambiante***

Dans un pays beaucoup plus libéral sur l'utilisation des données personnelles comme les Etats-Unis, les objets connectés seront plus encouragés que dans les pays très protecteurs de ces libertés individuelles. Au Canada par exemple, la législation prend en compte l'installation progressive de la société de surveillance et notamment par le biais des objets connectés de santé.
Le droit canadien s'est concentré sur la question des données collectées dans l'air ambiant.[79]
L'intelligence ambiante est un véritable progrès au service de la sécurité mais porte néanmoins atteinte à la protection de la vie privée.
Ainsi, dans cet article, la crainte vis-à-vis des technologies justifie le contrôle et l'encadrement législatif strict dont ces objets ont besoin. D'autant plus que les risques liés à ces technologies sont modernes dès lors qu'ils supposent la prise de décision humaine à l'origine. Ainsi, même si ce futur parait incontrôlable, l'origine elle, ne sera jamais inconnue du droit, contrairement aux risques naturels.
Les risques sociaux sont par ailleurs pris en compte sur la déshumanisation des relations médicales par exemple, puisque la surveillance à distance remplacera peu à peu la présence physique des personnes, ce qui est de plus en plus souvent le cas dans les maisons de retraite ou pour éduquer les enfants.
Le droit canadien met en garde sur la collecte de ces informations qui engendre des comparaisons entre les individus permettant une catégorisation de ceux-ci, néanmoins très valorisante sur le plan économique. Il favorise ainsi le conformisme des individus afin de limiter les risques sur la mauvaise interprétation de la collecte de leurs données.

[78] Décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique
[79] BENYEKHLEF (K.), PAQUETTE-BELANGER (E.), PORCIN (A.), « Vie privée et surveillance ambiante : le droit canadien en chantier », *Droit et Cultures*, 2013, pp.191-223

C'est pourquoi, plusieurs lois fédérales [80] et provinciales protègent les renseignements personnels et ont déjà pris en compte l'internet des objets dans le cadre précis de l'intelligence ambiante, la considérant donc comme partie intégrante des données personnelles.

- ***Le cas américain et le département HHS***

Sur le même continent, un tout autre système de régulation en matière de protection des données personnelles fait ses preuves. Les Etats-Unis ont en effet en 1996 voté la loi *Health Insurance Portability and Accountability Act* dite HIPAA sur le domaine de la santé et la transmission des données de santé dans le cadre de l'assurance maladie. Bien que la santé connectée par les objets connectés ne fasse encore l'objet d'aucune loi spécifique, les américains se sont concentrés sur la e-santé et ses aspects numériques. La loi fédérale HIPAA a une application large puisqu'elle concerne également les professionnels économiques traités précédemment, c'est-à-dire les assureurs. La loi oblige notamment les organismes, qui disposent des données de santé, à rendre publique toutes les grosses failles à la sécurité de leurs systèmes lorsque cela survient[81]. Le département de la Santé et des Services sociaux des Etats-Unis dit HHS créé en 1979 est chargé de la bonne régulation des échanges de ces données médicales et peu même utiliser un pouvoir de sanction si ses règles ne sont pas respectées[82]. Cet organisme s'assure donc de la protection de la vie privée.
Quant aux applications de santé et de bien-être qui intéresse ce rapport, les Etats-Unis ont un régulateur qui surveille et émet des recommandations : la FDA (*Food and Drug Administration*). Concernant le devoir d'information de l'utilisateur et l'éclairage de son consentement, les américains ont créé la FTC (*Federal Trade Commission*).

- ***Le cas de la Corée du Sud et son acte de régulation PIPA***

De l'autre côté de la planète, l'Asie n'est pas en reste en la matière. La Corée du Sud par exemple, connue pour son avance dans les réseaux mobiles[83], accueille l'une des villes les plus connectées du monde : Songdo où le décor futuriste de cette ville laboratoire contraste avec le reste du pays.
C'est dans cette ville que l'entreprise hight tech *Cisco* a élu domicile pour tester ses innovations ainsi que l'entreprise française *Véolia*.
La régulation sud-coréenne est confirmée en 2011 lors de la prise d'effet de la *Personal Information Protection Act*[84] (PIPA) après leur loi sur la protection des données personnelles de 1994 et offre un cadre législatif attractif pour les entreprises spécialisées dans les objets connectés.

[80] Lois sur la protection des renseignements personnels de 1985 et PIPEDA qui ajoute les documents électroniques de 2000
[81] CONSEIL NATIONAL DE L'ORDRE DES MEDECINS, « Livre blanc Santé connectée, de la e-santé à la santé connectée », janvier 2015, *www.conseil-national.medecin.fr*
[82] Site du *US Department of Health & Human Services, www.hhs.gov*
[83] La Corée du Sud développe déjà la 5G
[84] Le document complet sur le document pdf : *http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf*

L'émergence des objets connectés dans le monde médical aura ainsi bien évidemment d'énormes avantages pour la recherche et les progrès scientifiques permettant la victoire contre de graves maladies mais ils sont également l'origine de multiples abus, propres aux spécificités humaines. Si certains Etats du monde en ont bien pris conscience, l'anticipation reste limitée face aux évolutions techniques qui poussent toujours plus loin dans leurs retranchements, les certitudes juridiques.

3-Le futur des objets connectés de santé

Pour conclure, les objets connectés sont déjà bien implantés dans notre quotidien et dispose d'un arsenal législatif conséquent afin de protéger les données de santé qui sont réputées sensibles. Au sein de ce rapport, il a été mis en exergue que les fournisseurs des objets connectés de santé doivent protéger leurs appareils au regard de la problématique des données personnelles précédemment évoquées. Cette problématique centrale a vocation à croitre, notamment du fait du caractère ubiquitaire de ces données. Cette problématique est également importante au regard des utilisations de ces objets qui peuvent être malveillantes.

L'appât du gain dans un premier temps motivera le monde de l'entreprise à toujours plus investir dans ces technologies très proches du consommateur[85] qui permet un ciblage comportemental précis à l'origine de stratégie marketing efficace.
L'interaction entre les marques et le consommateur seront de plus en plus direct et les individus se retrouveront de plus en plus en danger sans même qu'ils en aient conscience.

De plus, l'individualisme humain est en effet au centre même du principe de *quantified self* qui poussera les gens à se renfermer sur leurs propres statistiques collectées par ces nouveaux gadgets, et concrétise toujours un peu plus le débat autour de la patrimonialisation du corps humain.
Les films de sciences-fictions avaient par ailleurs déjà anticipé l'internet des objets et envisageaient déjà les risques possibles de cette nouvelle technologie.
D'autant plus que la multiplication du nombre de capteurs par individu obligera les fabricants à rassembler les données sur un seul système de traitement qui sera, (pourquoi pas ?), directement incorporé dans le corps même de chaque personne.
A l'orée d'une convergence entre les mondes virtuels et réels, et si le pays souhaite garder son avance en la matière, le droit français devra donc trouver de nouvelles réponses à cette technologie beaucoup plus intrusive et peut-être même essayer d'anticiper en prenant plus au sérieux l'imagination des scénaristes futuristes.
En effet, la réalité concernant l'intelligence artificielle arrivera peut-être encore plus vite que prévue grâce aux objets connectés et la recherche approfondie dite « *deep learning* », basée sur les données collectées quotidiennement permettra d'anticiper les besoins avant tout mouvement humain. [86]

[85] Rapport de l'école SKEMA, « Business rule breakers and the internet of everything, Le livre Blanc, la révolution du commerce par les objets connectés », 2014, *www.skema-mdce.fr,* p.16
[86] DOUCENDE (B.), « Les objets connectés : notre futur serein ou restreint ? », mai 2014, *www.synertic.fr,* p.8

BIBLIOGRAPHIE

OUVRAGES GENERAUX OU SPECIALISES

- ANONYME, *Manuel de droit européen en matière de protection des données*, Office des publications de l'union européenne, Luxembourg, 2014, 215 p.

- MARLIAC NEGRIER (C.), *La protection des données nominative informatique en matière de recherche médicale tome 2*, PUAM, 2001, 844 p.

- PEDROT (P.) dir., *Traçabilité et responsabilité*, Economica, Paris, 2003, 323 p.

RAPPORTS

- CNIL, « Le corps, nouvel objet connecté du *quantified self* à la m-santé : les nouveaux territoires de la mise en données du monde », cahier IP N°02, *www.cnil.fr*

-CNIL, « La lettre innovation et prospective », cahier IP n°4, *www.cnil.fr*

-CNIL, « La lettre innovation et prospective », n°5, juillet 2013, *www.cnil.fr*

- CNIL, Délibération n° 01-011 du 08 mars 2001 portant adoption d'une recommandation sur les sites de santé destinés au public, *www.cnil.fr*

- Rapport de MORIN-DESAILLY (C.) au nom de la mission commune d'information, « Nouveau rôle et nouvelle stratégie pour l'union européenne pour la gouvernance mondiale de l'Internet », n° 696, déposé le 8 juillet 2012, *www.senat.fr*

- Rapport SAURY, « Secret médical et entreprises d'assurances », publié par le Conseil National de l'Ordre des Médecins, avril 2000, *www.conseil-national.medecin.fr*

- Rapport de l'école SKEMA, « Business rule breakers and the internet of everything, Le livre Blanc, la révolution du commerce par les objets connectés », 2014, *www.skema-mdce.fr*

- Rapport EUROPOL 2013, *www.europol.europa.eu*

- Rapport de la COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS, « L'internet des objets – Un plan d'action pour l'Europe », juin 2009, *eur-lex/europa.eu*

- Rapport de la COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS, « La télémédecine », 4 novembre 2008, *europa.eu*

- Contribution du CONSEIL NATIONAL DE L'ORDRE DES MÉDECINS À LA CONSULTATION PUBLIQUE DE LA COMMISSION EUROPÉENNE, « Le livre vert et la santé mobile », juillet 2014, *www.conseil-national.medecin.fr*
- Rapport G9+, Livre Blanc « Les nouveaux Eldorados de l'économie connectée », décembre 2013, *www.g9plus.org*

- Rapport CNOM, Livre Blanc « De la e-santé à la santé connectée », février 2015, *www.conseil-national.medecin.fr*

ARTICLES JURIDIQUES

- ABRAVANEL-JOLLY (S.), « Transparence en santé et assurance », *Revue générale de droit médical*, Les Etudes Hospitalières, Bordeaux, Juin 2014, pp. 115-127

- BALLET (P.), BENEAT (A.), « Dématérialisation des données de santé : quels référentiels ? », *Gazette du Palais*, 22 janvier 2011, n°22, p.22

-BENYEKHLEF (K.), PAQUETTE-BELANGER (E.), PORCIN (A.), « Vie privée et surveillance ambiante : le droit canadien en chantier », *Droit et Cultures*, 2013, pp.191-223

- BICHOT (P.), « Le secret médical : un outil redoutable à la disposition des assurés de mauvaise foi », *RLDC*, janvier 2005, p.13

- DESMARAIS, P., (2013). Quel régime pour le m-Health ?, LexisNexis, *CCE*, n° 3, mars 2013, p. 15

- FORREST (D.), « Qui a peur de l'Internet des objets ? », *RLDI*, n°54, novembre 2009, p.3

- LAVERDET (C.), « Les enjeux juridiques de l'internet des objets », *JCP G Semaine juridique*, n°23, 9 juin 2014, pp.1154-1155

- MAZEN (N.J.), BEVIERE- BOYER (B.), « Ethique et droit du vivant », *Revue générale de droit médical*, Les Etudes Hospitalières, Bordeaux, juin 2014, pp. 271-299

- MEURIS (F.), « L'internet des objets, regard critique », *CCE*, n°9, septembre 2014, p.2

- MEURIS (F.), « Les dangers du soi quantifié », *CCE*, n°7, juillet 2014, p.12

- MITCHELL (J.), « Increasing the cost-effectiveness of telemedicine by embrassing e-health », *J.Telemed. Telecare*, 2000, n°6, pp. 16-19

- MULLENEX (D.), « Les objets connectés : une législation déconnectée de l'avenir industriel », *JCP G La semaine juridique*, n°40, 29 septembre 2014, p.1764

- PANSIZE (F.J.), CHARBONNEU (C.), « La dématérialisation des données médicales et les enjeux de leur hébergement », *Gazette du Palais*, n° spécial, 2002, p.23

- SILGUY (S.), « Les objets connectés, un risque pour la protection de nos données personnelles », *RLDC*, n°119, 1er octobre 2014, pp.66-69

- SIMON (P.), « Responsabilité des professionnels de santé dans la pratique de la télémédecine clinique », *Revue générale de droit médical*, Les Etudes Hospitalières, Bordeaux, juin 2014, pp. 91-104
-WEINBAUM (N.), « Les données personnelles confrontées aux objets connectés », *CCE*, n°12, décembre 2014, p.15

ARTICLES NON JURIDIQUES

-ANONYME, « Dick Cheney, menacé comme dans "Homeland" ? », 22 octobre 2013, *www.telerama.fr*

- ANONYME, « Connecté, le patient devient un acteur engagé de sa santé », 17 juin 2014, *www.visionmarketing.com*

-ANONYME, « Objets connectés : opportunités et limites », juillet 2014, *www.objetconnecte.net*

-ANONYME, « Les données d'un bracelet intelligent bientôt utilisées en cour », jeudi 27 novembre 2014, *www.ici.radio-canada.ca*

- BERTAUD DU CHAZAUD (J.), « Les données d'objets connectés : nouvelles preuves dans les procès ? », 25 novembre 2014, *www.droitdu.net*

- DOUCENDE (B.), « Les objets connectés : notre futur serein ou restreint ? », mai 2014, *www.synertic.fr*

- DREYFUS (N.), « Santé connectée : la CNIL s'inquiète », 21 janvier 2014, *www.villagedelajustice.com*

- ERTZSCHEID (O.), «Les objets connectés, nouvelle « boîte noire » enrôlée par la justice », 20 novembre 2014, *www.rue89.nouvelobs.com*

- GAGNON (B.), « Internet finira par vous tuer, ou les conséquences du tout connecté tout le temps », 21 octobre 2014, *www.branchez-vous.com*

- GAUTIER (A.), « Un bracelet connecté utilisé comme preuve en Cour américaine », 1er décembre 2014, *www.webdesobjets.fr*

-SFEZ (B.), « Données de santé : des obligations de sécurité spécifique pour les professionnels de santé », 23 novembre 2013, *www.village-justice.com*

CONTRIBUTIONS - ENQUETES

- Projet de loi sur la santé par TOURAINE (M.), Ministre de la santé, 15 octobre 2014

- Enquête de 2013 réalisée par la Fondation Médéric Alzheimer auprès de 5690 établissements, « La lettre de l'Observatoire », n° 27, juillet 2013, *www.fondation-mederic-alzheimer.org*, 12p.

- Etude Baromètre 360 d'Orange Healthcare et MNH réalisée par Odexa, 19 janvier 2015

CONFÉRENCES

-Conférence, par CHARRONDIERE (H.), « Santé connectée, e-santé, télémédecine et numérique en santé », *Lesechosetudes*, 18 septembre 2014

-Conférence, par MENNECIER (D.), « La m-santé en 2014 » *Commission XX, Académie nationale de médecine*, 18 juin 2014

- Conférence, par QUEMENER (M.) et SCHMOLL (S.) « Les objets connectés », *www.blog.dmi.com*, 23 septembre 2014

TEXTES LEGISLATIFS

- Décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique

- Directive 95/46/CE 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

- Loi n° 78-17 du 6 janvier 1978 dite Informatique, Fichiers et Libertés

- Loi sur la protection des renseignements personnels de 1985

- Loi sur la protection des renseignements personnels et les documents électroniques dite PIPEDA de 2000

- Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé

- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

- Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation

JURISPRUDENCE

- Cour de Cassation, 2ème civ, n° de pourvoi 04-13509, 2 juin 2005

- Cour de Cassation, 1ère civ, n° de pourvoi 07-18-364, 13 novembre 2008, Bull civ II, n°240

- Cour de Cassation, 1ère civ, n° de pourvoi 99-17-187, 29 octobre 2002, Bull civ I, n° 244

MULTIMEDIAS

- « Santé 2.0 : Médecine Digitale et médecin connecté », *actuentreprise.com*

SITES INTERNET

Le site de l'Agence des Systèmes d'Information Partagés de Santé

www.esante.gouv.fr

La Commission Nationale de l'Informatique et des Libertés

www.Cnil.fr

TABLE DES MATIERES