

LE CORPS, NOUVEL OBJET CONNECTÉ

DU *QUANTIFIED SELF* À LA M-SANTÉ : LES NOUVEAUX
TERRITOIRES DE LA MISE EN DONNÉES DU MONDE

De nouvelles pratiques individuelles

Écosystème et Jeux d'acteurs

Quels axes de régulation ? Les voies à explorer



ÉDITO

Décidemment, la numérisation de nos activités humaines n'a pas de limites : elle concerne désormais notre corps et ce que nous en faisons. C'est ce que l'on appelle le « *quantified self* » ou quantification de soi. Sous cette expression quelque peu sibylline, sont visées des pratiques variées mais qui ont toutes pour point commun pour leurs adeptes, de mesurer et de comparer avec d'autres des variables relatives à notre mode de vie : nutrition, exercice physique, sommeil, mais aussi pourquoi pas son humeur, etc. Reposant de plus en plus sur l'utilisation de capteurs corporels connectés - bracelets, podomètres, balances, tensiomètres, etc. - et d'applications sur mobiles, ces pratiques volontaires d'auto-quantification se caractérisent par des modes de capture des données de plus en plus automatisés, et par le partage et la circulation de volumes considérables de données personnelles. Ce phénomène se développe à l'initiative des individus eux-mêmes et aussi, en raison des modèles économiques des acteurs investissant ce marché. Pratique marginale et effet de mode pour certains, signe précurseur de la révolution de l'Internet des Objets qui s'annonce ou amorce d'une transformation sociétale profonde pour d'autres : autant de points de vue différents sur la question, autant de raisons d'analyser plus en profondeur ces nouveaux usages du numérique.

C'est l'objet de ce deuxième cahier IP et, dans le prolongement des travaux menés dans le cadre du [chantier « vie privée 2020 »](#) d'étudier l'impact potentiel de ces nouvelles pratiques sur la vie privée et les libertés individuelles.

Plusieurs travaux ont ainsi été conduits : entretiens avec des experts du sujet (chercheurs, institutionnels, médecins, acteurs économiques, etc.) ; état des lieux à l'international sur les régulations à l'œuvre dans le domaine des applications mobiles de santé et des capteurs connectés ; étude du marché et du modèle économique des acteurs ; lancement de tests de capteurs et d'applications dans le cadre du laboratoire de la CNIL, etc.

Le sujet est complexe à appréhender en raison de l'hétérogénéité des pratiques de *quantified self*, de la diversité des outils et applications concernés, de leurs caractéristiques et de leurs fonctionnalités. C'est pourquoi même si ces cahiers IP sont essentiellement consacrés à l'étude des outils et applications grand public, vendues dans le commerce sans recours spécifique a priori à un professionnel de santé, les usages potentiellement médicaux de ces applications doivent aussi être pris en compte, la frontière avec des applications relevant du monde médical pouvant alors s'avérer délicate.

Au-delà, même si ces pratiques peuvent sous un premier abord apparaître ludiques voire « gadget » et portant peu à conséquences, le sujet, sur un plan plus prospectif, est porteur d'enjeux lourds non seulement en termes de santé publique mais aussi sur les plans juridiques, économiques, etc. Il pose également des questions éthiques délicates car il s'agit avant tout de données attachées au corps humain...

En définitive, ce deuxième numéro des cahiers a pour objectif de contribuer à la réflexion sur le sujet en esquissant des axes exploratoires en vue d'une éventuelle régulation à venir. 

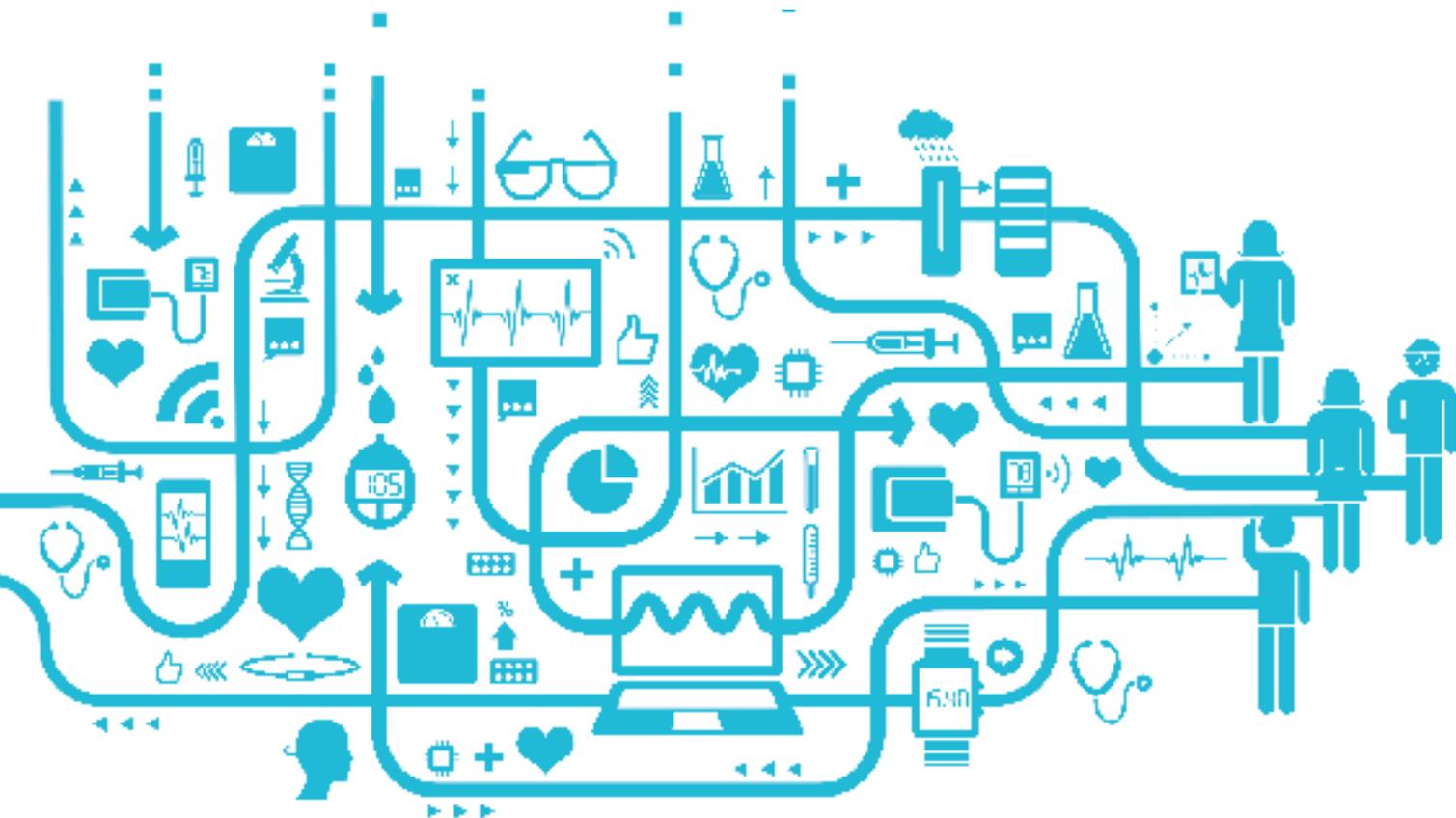
Isabelle FALQUE-PIERROTIN,
Présidente de la CNIL

AVANT-PRO

En Français, on a tendance à traduire *quantified self* par « auto-mesure de soi ». L'élaboration d'un « soi » commensurable car « chiffré », renvoie bien à l'obsession contemporaine pour une objectivité qui passe par la mise en nombres. Pourtant, la quantification et la mesure sont deux idées très différentes. Comme l'expliquait Alain Desrosières¹, quantifier consiste à « exprimer et faire exister sous une forme numérique ce qui, auparavant, était exprimé par des mots et non par des nombres » alors que « l'idée de mesure implique que quelque chose existe sous une forme déjà mesurable (...) comme la hauteur de la Tour Eiffel ». La « bonne santé », la « bonne humeur », ne sont pas des choses qui se laissent facilement « mesurer » indépendamment de conventions d'équivalences préalablement définies. Le phénomène du *quantified self* relève d'une démarche non pas de mesure mais de quantification continue, en temps réel, – contribuant à la production sociale de normes de comportements, de performance et de santé, éminemment évolutives... et permettant la visualisation et, éventuellement, la mise en comparaison de leurs progrès respectifs par les utilisateurs

reliés directement à l'Internet à travers les capteurs qui les « quantifient ».

La construction dynamique et interactive de cette normativité perfectionniste conduit à une exposition croissante de la vie privée voire de l'intimité de chacun, dans l'interaction avec des acteurs économiques qui ne poursuivent pas nécessairement les mêmes objectifs que les adeptes de la quantification de soi. Ce point est d'autant plus important que les données produites peuvent être, soit directement, soit indirectement, révélatrices d'informations sensibles relatives notamment à l'état de santé actuel ou futur. Des données traditionnellement confiées au médecin de famille dans le cadre d'une relation de confiance garantie notamment par le principe du secret médical se retrouvent sur les réseaux. Il est frappant de constater le peu d'inquiétude que cela suscite parmi les adeptes du *quantified self*. Que la confiance routinière accordée au médecin de famille soit étendue aux dispositifs numériques destinées non seulement à l'enregistrement mais aussi à la publication et au partage des paramètres observés par les capteurs, atteste de l'efficacité du design de ces interfaces conviviales conçues pour susciter le sentiment de confiance et de



POS

proximité. Ainsi le confort et la facilité d'utilisation, la précision et la fiabilité des enregistrements, font passer au second plan les interrogations éventuelles quant à la trajectoire et aux utilisations des données pour des finalités qui ne seraient pas nécessairement alignées sur les intérêts de l'utilisateur.

Par ailleurs, dans la mesure où ces pratiques contribuent à redéfinir continuellement des objectifs de performance et de jouissance de manière à inscrire les individus dans des processus de perfectionnement dont l'objectif recule au fur et à mesure qu'ils progressent, le risque est évidemment, pour les adeptes, de tomber dans une forme de « normopathie » (maladie de la norme) dont les symptômes sont notamment décrits par Y. Buin²: le langage, la pensée, le comportement normés en vue de la performance et de l'efficacité y perdraient tout pouvoir de contestation dès lors que la vie elle-même deviendrait un programme, lui-même intégré à celui d'une immense machinerie acéphale.

Cette question nous interroge sur le type de capacité d'agir (*agency*, dit-on en anglais) des individus dans ces contextes de quantification de la vie même. On parle beaucoup « d'empowerment » des individus par les technologies, rendus conscients de micro-événements physiologiques qui seraient passés, sans l'intervention des dispositifs de *quantified self*, complètement inaperçus. L'hyper-focalisation sur les événements physiologiques, cardiaques, digestifs, ... de la vie, ce dédoublement et cette intensification de la mémoire du corps permettra peut-être (mais ici, non plus, rien n'est certain) à l'individu de mieux préserver ses intérêts individuels, y compris en contestant les diagnostics médicaux, mais en aucun cas ce repli de l'individu sur lui-même ne permet la délibération collective sur les normes. Or, la notion d'émancipation n'est pas séparable de la notion de collectif, d'interindividualité, d'espace public où s'élabore du projet politique irréductible à la seule concurrence des intérêts et performances individuels. Les pratiques de quantification dans le domaine de la santé favorisent la micro-gestion individuelle de la santé au détriment d'une appréhension plus collective. Elles font des individus des entrepreneurs d'eux-mêmes responsables de leur bon ou mauvais comportement de santé, et peuvent distraire l'attention des causes environnementales ou socioéconomiques des problèmes de santé publique. Or le design pourrait aussi faciliter, plutôt que le perfectionnisme sanitaire individuel, la délibération collective sur les déterminants – non seulement comportementaux, mais aussi environnementaux et socio-économiques – de la santé et du bien-être.

Antoinette ROUVROY, Chercheur en philosophie du droit,
membre du Comité de la Prospective de la CNIL

1 / Desrosières, A. (2008) *Pour une sociologie historique de la quantification. L'argument statistique I*, Presses de l'École des mines, p. 10-11. – 2 / Buin, Y. (2003) 'Normopathie', *Le Passant Ordinaire. Revue Internationale de Création et de Pensée Critique*, 45-46

Partie 0.1 De nouvelles pratiques individuelles

SCÉNARIO PROSPECTIF : « LÉA ET SES CAPTEURS : UNE JOURNÉE EN L'AN 20.. »	08
LE QUANTIFIED SELF : POUR UNE MEILLEURE CONNAISSANCE DE SOI... ET DES AUTRES	10
LA TRANSFORMATION DES PRATIQUES MÉDICALES : PAROLES D'EXPERTS	15
L'INVASION DES CAPTEURS	17
CONTRÔLER ET VALORISER SES DONNÉES : LES NOUVELLES APPROCHES	21

Partie 0.2 Écosystème et Jeux d'acteurs

MARCHÉ DE LA SANTÉ SUR MOBILE ET MODÈLES ÉCONOMIQUES DES NOUVEAUX ENTRANTS	28
LES ACTEURS TRADITIONNELS DE LA SANTÉ, ENTRE INNOVATION ET DISPARITION ?	32
SCÉNARIO PROSPECTIF : « FUSIONS, ACQUISITIONS ET MODÈLES ÉCONOMIQUES DANS LE DOMAINE DES OBJETS CONNECTÉS DE LA SANTÉ ET DES ASSURANCES : OÙ EN EST LE MARCHÉ ? »	36
LE PROJET TRANSHUMANISTE : L'HOMME CAPTÉ, AUGMENTÉ, ... IDÉAL ?	38

Partie 0.3 Quels axes de régulation : les voies à explorer

QUELLE RÉGULATION POUR LA « SANTÉ MOBILE » ? À L'ÉCOLE DES EXEMPLES ÉTRANGERS...	44
POUR UN HABEAS CORPUS DE L'HOMME CAPTÉ	52
SCÉNARIO PROSPECTIF : « 2022, LE SOMMET DES HUMAINS DE RIO »	58

Bibliographie 60

Liste des experts interviewés 62

01



Partie 0.1

DE NOUVELLES PRATIQUES INDIVIDUELLES

<i>SCÉNARIO PROSPECTIF : " LÉA ET SES CAPTEURS : UNE JOURNÉE EN L'AN 20.. "</i>	08
<i>LE QUANTIFIED SELF : POUR UNE MEILLEURE CONNAISSANCE DE SOI... ET DES AUTRES</i>	10
<i>LA TRANSFORMATION DES PRATIQUES MÉDICALES : PAROLES D'EXPERTS</i>	15
<i>L'INVASION DES CAPTEURS</i>	17
<i>CONTRÔLER ET VALORISER SES DONNÉES : LES NOUVELLES APPROCHES</i>	21

À quoi pourrait ressembler une journée type d'un adepte du *quantified self* dans un futur proche ? Nous nous sommes amusés à imaginer la journée de Léa, salariée d'une grande entreprise de technologies installée en Californie. Ce texte s'inspire de lectures évoquant ce quotidien, en particulier du roman dystopique publié en octobre 2013 par Dave Eggers, « *The Circle* » (Editions Mc Sweeney's, 2014), une entreprise inventée devenue la compagnie technologique la plus puissante du monde après le succès de TruYou, un outil de présence numérique d'un individu, au travers d'une seule authentification... et d'une seule identité. Dorénavant, fort de son succès, *The Circle* peut mener à bien tous ses projets d'amélioration du monde par la technologie, même les plus fous.

LÉA ET SES CAPTEURS : UNE JOURNÉE EN L'AN 20..

L'harassante journée de Léa ne s'était achevée que tard hier lors du barbecue réunissant les employés du « campus » surplombant la Baie de San Francisco. Cela n'avait rien d'exceptionnel depuis qu'elle avait rejoint, suite au rachat de sa start-up, les équipes de la plus importante entreprise technologique du monde. En 5 ans à peine, l'entreprise avait supplanté Google, Facebook et consorts dans le cœur des utilisateurs comme des analystes financiers. Pourtant, le réveil de Léa se fait en douceur, comme tous les jours depuis qu'elle utilise le prototype de lecteur d'ondes cérébrales de l'entreprise. L'appareil est tellement simple qu'il paraît magique : il suffit de faire adhérer deux carrés souples de la taille d'un ongle sur les tempes, sans aucune gêne pour elle pendant la nuit, et les données sont transmises au bracelet et à sa tablette transparente dernier cri. Le bracelet s'est mis à vibrer doucement au moment idéal pour assurer un réveil pendant une phase de sommeil léger, et a transmis l'information à la tablette, qui se charge d'augmenter la luminosité, de régler la climatisation, de lancer la cafetière... et de publier l'information sur le service de réseau social de l'entreprise. Dans le même temps, les rendez-vous de son agenda sont mis à jour pour tenir compte des 15 minutes de sommeil qu'elle a économisées cette nuit-là...

Pendant le petit déjeuner, Léa vérifie distraitement ses PKPI (*personal key performance indicators*). Léa essaye de consulter régulièrement ces calculs issus d'algorithmes sophistiqués (et obscurs) et chargés d'optimiser automatiquement à la fois sa motivation et sa forme physique, adoptant ainsi pour sa vie personnelle, la vision de l'entreprise : « on ne peut pas améliorer ce qu'on ne peut pas mesurer, on ne changera pas ce qu'on peut cacher »... Et Léa reconnaît que cela fonctionne : depuis un mois, elle s'est déjà surprise plusieurs fois à reposer un soda dans son frigo, sachant que tout le monde aurait connaissance de ce petit écart... Elle a d'ailleurs perdu 2 kilos depuis que le bracelet et d'autres capteurs mesurent ainsi sa vie, non pas qu'elle l'ait voulue activement ou qu'elle pensait en avoir besoin... mais elle a reçu de nombreuses félicitations alors ! Aujourd'hui, son coach numérique lui recommande d'ailleurs 13 150 pas dans la journée et pas plus de 1850 calories... Après l'avoir félicité pour les 11 824 pas de la veille, en hausse de 1,2% par rapport à la semaine précédente qui était elle-même la seconde meilleure semaine de Léa depuis qu'elle a adhéré au programme de « santé active » de son employeur. Léa boit son café du matin (dont les teneurs en caféine, sucre et calories sont mesurées automatiquement par la tasse portant le logo de l'entreprise) tout en regardant d'un air absent l'avalanche de statistiques et de *dataviz* sur sa tablette. Elle ne peut cependant échapper à la plus visible : une augmentation de 2,4% par jour du nombre de calories quotidiennes ingérées depuis le début du mois. Cette croissance est certes corrélée à la baisse de 3°C de la température moyenne extérieure relevée par sa station météo d'appartement et celle de sa voiture, mais les chiffres révèlent une corrélation plus nette encore avec une hausse de 1,3% de son poids et de 0,8% de la proportion de masse grasse de son corps relevées par la balance connectée de la salle de bain. Refrénant l'envie de pulvériser cette moucharde, Léa soupire en lisant les recommandations au ton ouvertement positif et motivant du coach virtuel de l'application *ActivHealth*, qui recommande une modification de régime alimentaire et une hausse

importante de 10% des objectifs quotidiens du nombre de pas à forte intensité pour contrecarrer cette pente jugée funeste. En réalité, le coach virtuel annonce sur un ton triomphant qu'il avait intégré cette hausse de sa propre initiative dans les objectifs de la veille et que son poids a déjà baissé de 0,3% (un miraculeux 180 grammes de perdu, calcule rapidement Léa en finissant sa tasse). D'un soupir elle se rend également compte sur l'écran que l'analyse « humeur et stress » de sa journée de la veille a déjà provoqué des commentaires inquiets de certains collègues et de son manager « ça n'est pas grave, je te connais, tu ne resteras pas longtemps dans les 10% d'employés ayant la moins bonne humeur du département »... Léa est plus étonnée de voir un message de la responsable « *wellness analytics* » de sa direction qui lui rappelle qu'un excès de stress peut conduire à une dégradation de la santé et qu'elle doit faire attention à elle...

Léa se rend compte que le ton de ce dernier message, tout en compassion, est en fait tout sauf anodin. Tout cela peut avoir des conséquences sur son assurance santé, *ActivHealth* étant partie intégrante des services financés par l'entreprise. Celle-ci a certes l'une des politiques en ce domaine parmi les plus généreuses des États-Unis, mais cette politique n'existe qu'en contrepartie de l'adhésion aux valeurs de « transparence et de responsabilisation » d'*ActivHealth*. Le contrat « *Wellness* » de son entreprise permet en effet aux algorithmes de l'assureur (dont le géant des technologies est devenu le plus gros fournisseur de données et de solutions technologiques cette année...) de suivre les résultats de ses capteurs corporels. Ce n'est pas vraiment obligatoire, mais... l'assurance est bien moins coûteuse quand on consent « librement » à un tel partage. « Il va falloir faire descendre ce niveau de stress, même artificiellement » se dit Léa en songeant aux stratagèmes qu'elle pourrait employer pour tromper les capteurs. Au début des contrats d'assurance de ce type, c'était d'ailleurs un jeu très répandu : les employés accrochaient leur podomètre au collier de leur chien pour augmenter le nombre de pas parcourus par jour, par exemple. Les labradors de tout le pays étaient ravis, mais les assureurs se sont rapidement rendus compte de la faille... en croisant ces données avec celles issues de leurs bases d'assurance pour « animaux de compagnie ». Cela a permis à l'employeur de Léa d'entrer sur ce marché en leur fournissant un algorithme capable de distinguer les pas humains de ceux des animaux... Il paraît que certains cadres aisés d'entreprise payent des gens pour porter leurs capteurs le temps d'un footing,... mais c'est évidemment impossible pour un utilisateur identifié en permanence par ses objets connectés... D'autant que les dernières améliorations de l'algorithme de reconnaissance des pas devraient lui permettre de vérifier la cohérence de réalisation d'un pas en fonction des caractéristiques du porteur des capteurs (sexe, taille, poids, âge,...). « Je peux toujours me forcer à sourire un peu plus au bureau, les caméras ne manqueront pas de le détecter... » Perdue dans ces pensées, Léa tend machinalement la main vers un autre gâteau, mais son bracelet vibre doucement à l'approche de la puce sans-contact de l'emballage pour l'en dissuader. Elle change d'avis sans même y penser. Quelle chance de ne plus avoir à faire d'efforts pour être exemplaire et raisonnable !

Arrivée sur l'immense campus ensoleillé qui accueille son bureau, alors qu'elle appuie sur le bouton de l'ascenseur, son bracelet vibre. Sur l'écran « Et si vous preniez l'escalier ? ». Après un déjeuner calibré sur son nouvel objectif nutritionnel (et incluant un accompagnement à la carotte : son bracelet a détecté dans son sang une carence en vitamine A), Léa se replonge dans son travail avec intensité tout l'après-midi. Petite vibration : « Vous êtes stressée, faites donc une pause. » Elle retrouve le sourire. Brièvement. Encore une vibration. Fin de la pause. La fin de journée approche, et Léa se rend compte à 17h qu'un espace dans son agenda a été bloqué par *ActivHealth* et que, si elle le souhaite, 37% des machines de la salle de gym sont actuellement libres...

Après sa séance de sport (qui lui vaut de voir sur son bracelet un message de félicitation enthousiaste de la responsable *Wellness* de son pôle), Léa découvre sur son bureau un paquet. Son chef l'attend à côté. « Bonsoir Léa. Tes chiffres de stress sont meilleurs aujourd'hui, cela me rassure. Et cette séance de sport était une bonne idée, tu seras encore plus sereine demain je parie ! Tu seras rapidement revenue dans les 10% les moins stressés de l'équipe. Tu sais à quel point le bien-être de chacun est important pour nous... D'ailleurs, nous t'avons choisie pour tester le nouveau prototype du bracelet du programme *ActivHealth*. On se voit à la collecte de fonds pour le Bangladesh tout à l'heure ? Tu n'as pas encore répondu à l'invitation mais toute l'équipe sera là, on compte sur toi ! » Léa acquiesce tout en découvrant le magnifique nouveau bracelet : l'écran est souple et entièrement transparent. Le bracelet ne pèse que quelques grammes. Pourtant il sera entièrement gratuit d'après ce qu'elle comprend à partir du moment où les utilisateurs acceptent de partager leurs données avec des partenaires de l'entreprise, tout comme ils le font avec leur cercle d'amis, finalement !

Une fois chez elle, Léa s'accorde quelques minutes devant un film sur son écran mural. Pendant les pubs, elle se lève pour aller à la salle de bains. Son capteur vibre très légèrement : « Nous aimerions avoir votre avis sur les publicités en cours de diffusion. Vous obtiendrez des points et des promotions personnalisés ! Restez devant la caméra de votre écran pour accepter. » Elle ignore le rappel à l'ordre. Le bracelet se met à vibrer un peu plus fort...

LE QUANTIFIED SELF : POUR UNE MEILLEURE CONNAISSANCE DE SOI... ET DES AUTRES

“ Le mouvement de la quantification de soi n'est que le prolongement d'un phénomène plus général dans la continuité des usages du web. Il permet de faire des rencontres et d'accéder à des informations. On considère que le mouvement de la quantification de soi a émergé autour des années 2007-2008 mais il existait auparavant. Dès 2003, sous la forme des forums de patients : de manière anonyme, des internautes à la recherche de conseils voulaient échapper aux intervenants de santé. Des rencontres s'y font, des mécanismes d'entraide se mettent en place. À l'avenir, la santé et des sujets connexes, comme la sexualité vont devenir moins tabous ; les gens en parlent déjà sur les réseaux sociaux et devraient aller jusqu'à mesurer leur pratique sexuelle : le domaine d'extension de la quantification de soi devrait ainsi s'étendre vers l'intime, de manière plus ou moins anonymisée, pour se mesurer et se comparer à la norme. ”

Emmanuel Gadenne

consultant et auteur du Guide pratique du *Quantified Self*
Mieux gérer sa vie, sa santé, sa productivité

S'il y a bien un domaine où la production et l'exploitation des données par les individus eux-mêmes et à leurs propres fins se sont fortement développées, c'est certainement celui du *quantified self*. Traduit en français par auto-mesure, « soi quantifié » ou encore quantification de soi, le *quantified self* est un mouvement – voire pour certains un nouvel art de vivre (Henri Verdier [Connais toi toi-même petite Philosophie du #QuantifiedSelf](#)) – qui vise au « mieux-être » en mesurant différentes activités liées au mode de vie. Apparu en Californie en 2007, en particulier à l'initiative de deux

journalistes de la revue du numérique *Wired* (voir encadré « une petite histoire du *quantified self*), le credo de ce mouvement se résume à l'idée qu'on ne peut pas améliorer ce qu'on ne peut pas quantifier, ce qui n'est pas sans rappeler la célèbre formule de management « *You can't manage what you can't measure* ».

Qu'il s'agisse du nombre de pas réalisés dans la journée, de la qualité du sommeil ou de ses activités sportives, ce mouvement est particulièrement intéressant à étudier en ce qu'il concerne des données d'un nouveau genre, produites par les individus eux-mêmes et souvent destinées à être partagées – dans un domaine qui touche parfois à l'essence même de l'intimité.

Ces pratiques semblent illustrer un nouveau rapport au corps, aux données et probablement préfigurer de nouveaux usages liés au développement des objets connectés. Les capteurs utilisés dans une optique de *quantified self* peuvent en effet être appréhendés comme la première vague de l'Internet des objets – il y en aurait 75 milliards à l'horizon 2020 (source : Morgan Stanley, 2013) –, avec la particularité d'être portés par et « sur » les individus pour produire des données qui se situent à la frontière du bien-être et de la santé.

LA CONNAISSANCE DE SOI EN CHIFFRES : ENTRE RUPTURE ET CONTINUITÉ

La santé est un domaine qui évolue au rythme des progrès technologiques et où la pénétration du numérique apporte des changements inédits dans les usages et les comportements. Une nouveauté particulièrement « perturbante » est l'émergence de ce mouvement citoyen qui conduit certains à souhaiter être davantage acteurs de leur bien-être et de leur santé. Cette volonté s'appuie sur des outils qui peuvent être des capteurs connectés (synchronisés avec une application mobile) ou des applications mobiles (qui recourent aux capteurs du smartphone) pour mesurer un certain nombre de constantes liées au mode de vie – principalement dans les domaines de la forme, du bien-être et de la santé. Que ce soit au travers de capteurs ou d'applications mobiles, le fonctionnement de ces

UNE PETITE HISTOIRE DU MOUVEMENT « QUANTIFIED SELF »



Le mouvement est apparu en 2007 dans la Silicon Valley, et a été popularisé par deux rédacteurs de l'incontournable revue Wired : Gary Wolf et Kevin Kelly. En 2010 Gary Wolf a présenté lors de la fameuse conférence TED « [ce passe-temps intrigant](#) » selon les mots des organisateurs. Depuis, le mouvement s'est développé comme une « collaboration entre utilisateurs et fabricants d'outils qui partagent un intérêt pour la connaissance de soi à travers la traçabilité de soi » et en réunit les pionniers présents dans de nombreuses villes du monde dont Paris.

outils permet de conserver une trace des activités réalisées. Il existe aujourd'hui une gamme variée de capteurs et plusieurs dizaines de milliers d'applications qui concernent principalement les thématiques suivantes : quantifier une activité ou un paramètre physique (Runkeeper, Runtastic, Nike+, Fitbit,...) ; surveiller la nutrition au travers de l'estimation des calories (MyFitness Pal,...) ; surveiller le poids (balance connectée : Withings, Fitbit, Terraillon) ; suivre un facteur de risque (en particulier les maladies chroniques comme l'hypertension ou le diabète) ; mesurer la qualité du sommeil (Fitbit, Jawbone, isommeil,...) ; évaluer l'humeur, etc.

À l'exception des applications dédiées au médical, le parcours d'utilisation de ces différents outils est généralement orienté vers la performance et s'organise autour de trois grandes étapes.

- La première étape consiste en la fixation d'un objectif à atteindre qui servira de point de référence. Les activités, efforts, progrès peuvent ensuite être médiatisés au sein d'une communauté plus ou moins large : il peut s'agir de ne les partager qu'en direction des autres utilisateurs du même outil, ou de manière plus large en les publiant sur des réseaux sociaux généralistes (Facebook, Twitter, etc.).

- Deuxième étape, cette médiatisation des activités peut répondre à un double objectif de valorisation des efforts, et d'obtention d'encouragements. Elle a une vocation similaire au

« nudge » (coup de pouce) théorisé par Richard Thaler et Cass Sunstein : par une ingénierie douce du choix, on oriente la personne vers la « bonne » décision. Ici, la personne s'oriente elle-même vers le choix de « bonne santé » par exemple en mettant ses efforts sous le regard des autres, l'échec et l'abandon devenant d'autant plus coûteux.

- Enfin, une dernière étape importante est le compte rendu dans le temps des activités qui deviennent visualisables sous forme graphique au travers de courbes, de diagrammes, souvent avec des fonctionnalités calendaires permettant d'objectiver les pratiques.

Ces outils peuvent se différencier dans leurs modalités d'enregistrement et de captation des données. Dans certains cas, les données sont enregistrées « automatiquement » par un capteur – soit externe, soit incorporé au smartphone – et sont ensuite remontées vers l'éditeur de l'application ou du capteur. Dans d'autres cas, les données sont entrées manuellement, de manière déclarative, par l'utilisateur dans une interface dédiée (ex. : évaluation de l'humeur).

Cette dernière méthode est au centre de l'étude « Tracking for health » qui s'intéresse aux méthodes utilisées pour suivre un indicateur de santé. Publiée en janvier 2013 par le *Pew Internet Institute*, le *quantified self* est abordé avec comme point d'entrée la manière dont les Américains suivent un facteur de bien-être pour eux ou un proche. Les résultats montrent qu'une partie des usages du *quantified self* n'est que la déclinaison numérique et outillée d'anciennes habitudes pour suivre un état de santé. L'étude révèle ainsi que 69% des enquêtés déclarent suivre un indicateur de santé pour eux-mêmes ou un proche. Plus précisément :

- 60 % disent suivre leur poids, leur alimentation ou une autre habitude ; 33 % suivent un indicateur de santé (tension, diabète, sommeil) ; 12% celui d'un proche ;

- 21 % s'aident de technologies pour suivre ces indicateurs (tableurs, capteurs, smartphone) : 35% le font « sur papier » et 49% les mémorisent « de tête » sans les formaliser davantage ; 19% des possesseurs de smartphone utilisent au moins une application dédiée ;

- un tiers des utilisateurs partagent leurs données et, parmi eux, la moitié le fait avec un professionnel de santé.





- Ces résultats corroborent la typologie des *self-quantifiers* établie par Anne-Sylvie Pharabod *et al.* (mentionnée dans « La mise en chiffres de soi » Une approche compréhensive des mesures personnelles, Réseaux, 2013/1) qui, à partir de 40 entretiens réalisés avec des « quantificateurs », dessine l'analyse de trois « logiques stabilisées des chiffres personnels : surveillance, routinisation, performance ». La première logique désigne la *surveillance* d'un paramètre à risque pour lequel la notion de seuil est

centrale, et où la quantification ne vise pas à l'action, même si elle peut engendrer des effets en retour. Ce seuil est généralement défini par rapport à des normes (souvent médicales) et, dans un tel contexte, le partage d'une mesure qui concerne des paramètres médicaux ou intimes reste peu évident. La mesure de *régularité* (ou de routinisation) vise à rompre avec une mauvaise pratique ou à en adopter une meilleure. Elle est fréquente pour une catégorie de sportifs qui ne poursuivent pas un objectif de *performance*. Le fait de quantifier, de laisser une trace est alors essentiel pour le maintien de la motivation. La publication de données et le regard de tiers peuvent être recherchés pour s'encourager. La mesure de performance, enfin, sert à contrôler l'efficacité d'un effort spécifique où l'enregistrement de l'activité se confond avec l'activité elle-même. Le chiffre occupe ici une place essentielle pour rendre compte de la progression vers l'objectif. Le partage et l'échange en ligne s'engagent plus facilement sur les méthodes/outils de mesure ou sur les performances.

Ce mélange entre usages de technologies nouvelles et pratiques d'hygiène de vie plus anciennes est à la base de la philosophie du *self-tracking*. Les pionniers font d'ailleurs régulièrement référence aux groupes d'échange entre alcooliques anonymes pour souligner la dynamique d'entraide communautaire. Si ces pratiques étaient à l'origine plutôt le fait de petites communautés d'initiés, elles sont devenues aujourd'hui beaucoup plus « grand public », s'adressant à des personnes qui ont un intérêt à suivre un indicateur de forme de manière temporaire. Pour Bernard Benhamou, Délégué aux Usages de l'Internet, la démocratisation de ces nouveaux usages est liée à « l'arrivée des terminaux mobiles et tactiles qui a été l'élément déclencheur des mouvements de mesure de soi : ces terminaux ont créé une grammaire ergonomique et gestuelle commune. La rupture ergonomique a été le préalable indispensable. » Les tablettes et smartphones s'imposent en effet comme de nouveaux hubs, jouant un rôle central à la fois comme télécommande des objets connectés mais aussi comme interface préférentielle de consultation des données. Pour Emmanuel Gadenne, l'apparition du Web social à partir de 2006 a été déterminante en

permettant d'accéder à de nouvelles données, d'établir de nouvelles corrélations dans le prolongement de ce qui existait jusqu'alors sous la forme de forums de patients. Selon lui « la santé est une motivation indirecte, cachée. La motivation directe intervient lorsque l'on peut partager des données qui ne sont pas directement intimes, comme le nombre de pas réalisés. ». Un des objectifs poursuivis est aussi de pouvoir se mesurer et de se comparer à une norme.

PAR RAPPORT À QUOI SE QUANTIFIE-T-ON ? VERS UNE NOUVELLE « NORMOPATHIE » ?

Comme le rappelle la juriste et philosophe du droit Antoinette Rouvroy (voir avant-propos) en se basant sur les travaux d'Alain Desrosières portant sur l'histoire de la quantification, il faut distinguer la « mesure » de la « quantification », deux notions trop souvent confondues. Le verbe « quantifier » renvoie à l'idée de faire exister sous la forme d'un nombre ce qui, auparavant, était exprimé par des mots. Ce passage implique une série de constructions d'équivalences et de conventions qui, par essence, visent *in fine* à établir des comparaisons par rapport à une norme. La quantification vise ainsi à rendre comparable. Cette référence perpétuelle à une norme, à une moyenne des autres utilisateurs est peut-être une véritable rupture induite par la numérisation de ces pratiques. Henri Verdier, entrepreneur du numérique et directeur d'Etalab, y voit même l'intégration d'une idéologie du management appliquée au corps. Ce n'est d'ailleurs pas un hasard si l'ancêtre du mouvement du *quantified self* est le *lifelogging* – une forme d'archivage total de soi – où il s'agit de retranscrire la totalité de sa vie, sans idée de quantification au départ, pour avoir un double de soi, ce qui renvoie à des notions d'éternité et de posthumanisme selon Antoinette Rouvroy...

Si ce nouveau rapport au corps, appréhendable par les données, suscite l'intérêt de nombreux experts et chercheurs, certains demeurent plus critiques quant à l'avenir de ce marché ainsi que sur l'idéologie entourant la quantification. C'est en particulier le cas du Dr Laurent Alexandre, fondateur de DNA

Vision, pour qui « Le marché de l'automesure est aujourd'hui infinitésimal, anecdotique...il est loin d'être évident que le marché se développe dans le futur. Les personnes qui se mesurent se lassent très vite : cela les amuse un temps, puis elles abandonnent. En grossissant le trait, personne ne fait de l'auto-mesure durable, à part quelques hypocondriaques graves qu'il faut mettre sous Prozac – et qui sont minoritaires. Peu de gens vivent dans leur santé au quotidien. Pour se développer, le *quantified self* doit être automatique, sans capteur spécifique, à partir du smartphone. »

De son côté l'écrivain et chercheur Evgeny Morozov, spécialiste des impacts sociaux des technologies, voit dans ces outils l'incarnation d'une forme de « [solutionisme technologique](#) ». Il estime que déplacer la responsabilité du côté des utilisateurs est une approche particulièrement conservatrice, où les individus sont davantage considérés comme des consommateurs que comme des citoyens. La mise en capacité et l'autonomie de l'individu restent pour lui un mythe (cf. partie 1.4) et il considère que ceux qui s'auto-mesurent le font parce qu'ils n'ont rien à perdre, parce qu'ils sont en situation de prouver qu'ils sont « meilleurs » que la moyenne (ils conduisent plus prudemment, sont en meilleure santé...) et parce qu'ils vont finalement en obtenir des avantages. Evgeny Morozov pointe ainsi le caractère normatif de telles pratiques qui pourraient, en creux, rendre suspects ceux qui ne se quantifient pas, comme s'ils avaient quelque chose à cacher. On retrouve le même scepticisme chez Antoinette Rouvroy qui – reprenant l'essai de Guillaume Leblanc (*Les maladies de l'homme normal*) –, s'interroge sur cette « normopathie » où les individus ne seront jamais assez normaux. Selon elle, « dès que l'on commence à se comparer aux autres, et surtout lorsque les normes sont construites de façon dynamique et interactive, la normalité est un « savon qui glisse ». Le *quantified self* risque de discriminer les utilisateurs qui ne seront jamais assez performants, assez optimaux. D'autant plus que l'utilisateur se retrouve « grisé » par des interfaces composées de chiffres et de diagrammes qui peuvent lui donner l'illusion d'une approche scientifique des activités quantifiées. Pour Antoinette Rouvroy, le nouvel acteur clé c'est l'interface, ■■■

Aujourd'hui j'ai regardé
mon nombril 486 fois.



- modelée par des designers qui travaillent pour des acteurs qui peuvent avoir des intérêts divergents de ceux des utilisateurs. Le design, tout en étant transparent, n'est pas neutre. Il peut être mobilisé comme un outil de manipulation pour attirer et favoriser le partage de données à caractère personnel.

VOUS AVEZ DIT INTIME ?

Cette incitation au partage et à la circulation des données est à prendre en considération, compte tenu de la sensibilité des données concernées – y compris pour celles qui semblent être *a priori* les plus anodines. C'est d'ailleurs une difficulté à laquelle se trouvent confrontés les régulateurs lorsqu'ils ont à se prononcer sur le statut des données du *quantified self* (cf partie 3.2). Certaines de ces données peuvent paraître « neutres », par exemple lorsque l'on s'intéresse au nombre de pas. D'autres données de bien-être s'apparentent davantage à des données de santé, soit en raison de ce qu'elles peuvent révéler de manière brute (ex. : une donnée de tension), soit à cause de ce qu'elles pourraient révéler une fois combinées à d'autres (ex. : une

donnée de poids combinée à la taille peut permettre d'estimer un risque cardio-vasculaire). Ces potentialités d'inférence ne sont pas hypothétiques, puisque l'objectif de recoupement de différents jeux de données pour en dégager des corrélations est une finalité assumée aussi bien par ceux qui se quantifient que par les services de *quantified self*. En effet, les éditeurs de services cherchent à s'établir en tant que plateforme en hébergeant le maximum de jeux de données sur leurs utilisateurs qui peuvent ainsi procéder à un plus grand nombre de croisements (cf. partie 02).

Dans ce contexte où les frontières entre bien-être et santé sont de plus en plus floues, la problématique du partage des données devient d'autant plus prégnante.

Le partage le moins visible est celui qui est opéré à l'initiative des éditeurs de services ou des producteurs de capteurs à destination de sociétés tierces, sur des données plus ou moins anonymisées. Dans ces échanges, et dans une perspective de protection de la vie privée, les interrogations concernent la possible réutilisation des données, leur sécurisation, ainsi que l'information et le contrôle conférés aux utilisateurs. L'étude « *Mobile health and fitness apps what are the privacy risks ?* » menée en 2013 par *Privacy Rights Clearinghouse*, une association américaine de défense de la vie privée, sur 43 applications mobiles de santé et fitness montre ainsi qu'une grande majorité d'entre elles n'offre pas les protections suffisantes pour garantir la confidentialité des données de leurs utilisateurs. En particulier sont soulignés les défauts de sécurisation des communications (non chiffrées), le partage d'informations personnelles en direction d'annonceurs pour générer de la publicité ciblée et l'envoi de « données agrégées » mais susceptibles de permettre une ré-identification des utilisateurs par des tiers.

Mais les utilisateurs peuvent être eux-mêmes à l'initiative d'une autre forme de partage de leurs données à destination d'une communauté précise ou, plus largement, de leurs « amis ». Pour le Dr. Laurent Alexandre, « l'extériorisation de l'intimité s'est installée avec une facebookisation des données de santé ». Le communautaire a, selon lui, cassé tous les tabous sur le partage des données. Il est rejoint sur ce point par Bernard Benhamou et Emmanuel Gadenne. Le premier estime que les données de santé sont passées du statut de précieuses et cachées à celui de visible. Le second pronostique une extension des pratiques de quantification allant de plus en plus vers l'intime. ■

LA TRANSFORMATION DES PRATIQUES MÉDICALES : POINTS DE VUE D'EXPERTS

“ La frontière entre les domaines du bien-être et de la santé va s'estomper. L'objectif est que demain, les gens disent que c'est eux qui prennent soin de leur santé, avec l'aide de leur médecin et non plus leur médecin seul. Il faut que ces données deviennent utiles pour le corps médical, tout en sachant qu'elles doivent sans doute être filtrées car ce sont des mesures prises chez soi, hors protocole médical, et qui n'ont donc pas la même fiabilité que lorsqu'il s'agit d'un médecin qui opère ce type de mesures. Le patient devient expert, le médecin va devoir le prendre comme un partenaire. ”

Cédric Hutchings
PDG de Withings

Le floutage des frontières qu'introduit le *quantified self* en permettant simultanément le développement de pratiques liées à l'hygiène de vie qui relèvent de l'univers du bien-être et l'émergence d'actes d'auto-diagnostic et de soins, est à la fois source de questionnements et de promesses pour une nouvelle médecine 2.0. Comme le rappelle justement le rapport du Conseil général de l'économie, de l'industrie, de l'énergie et des technologies (CGEJET) « *Bien vivre grâce au numérique* », publié en février 2012, les technologies font évoluer la manière de voir la santé et corrélativement de faire de la médecine.

LE QUANTIFIED SELF DANS LES PRATIQUES MÉDICALES

Le concept de malade versus bien portant est à ce titre en train d'évoluer. L'autonomie pourrait être un fil conducteur, ainsi que la question de la responsabilité de chacun par rapport à sa propre santé...

Comme le confirme le Dr. Postel-Vinay, directeur du site *autom mesure.com*, il n'y a pas de frontière nette entre santé et bien-être mais un continuum. Dans ces conditions, il devient envisageable d'utiliser des données produites par les utilisateurs avec des outils de type *quantified self* dans un contexte médical. Il existe déjà des situations où les données sont générées directement par les patients, comme par exemple dans le cas de la télémédecine intégrant des dispositifs d'autom mesure.

En revanche, dès lors que ce sont les utilisateurs eux-mêmes qui s'équipent pour suivre leur état de santé, en dehors du geste médical, on sort du cadre traditionnel de la pratique médicale. Ces mesures réalisées en dehors d'une supervision soulèvent plusieurs séries de questions au premier rang desquelles celle de la fiabilité des dispositifs utilisés et par voie de conséquence des données captées et analysées. Pour Cédric Hutchings, une relation nouvelle doit également 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 ». Ces données brutes, produites « par le bas » nourrissent par ailleurs le scepticisme de certains sur la possibilité d'y recourir à des fins prédictives (analyses de type Big Data) ou médicales. Comment se fier à ces données (que l'on pourrait qualifier de « sales ») si elles ne sont pas fondées sur des normes ou des conventions d'enregistrement établies et reconnues ? Une manière de prendre en compte cette problématique de la fiabilité serait de recourir à des tiers de confiance. Une figure naturelle est incarnée par le médecin, qui pourrait occuper un rôle de prescripteur au cœur de ces pratiques d'auto-mesure en orientant les patients vers des outils et services sûrs, produisant des données fiables, utiles pour eux comme pour lui. Aujourd'hui cette démarche de conseil est relativement confidentielle selon le [2ème baromètre Vidal](#) (mai 2013) qui évalue à 8% la proportion de médecins utilisateurs de smartphones en France qui auraient déjà recommandé une application santé à leurs patients. Ils sont en revanche plus nombreux, 56% d'entre eux, à recourir à des applications médicales en utilisation professionnelle. Emmanuel Gadenne, particulièrement adepte des outils de *quantified self*, considère qu'il est important ...



- que le médecin garde un rôle actif. Selon lui il perçoit que l'on peut accéder à de nouvelles connaissances et cela lui permet de vérifier que le patient est capable de se gérer – meilleure observance – entre deux consultations. Cette voie qui consiste à combiner expertise médicale et prise en main de sa santé par chacun est encouragée par Bernard Benhamou qui y voit un bénéfice potentiel pour la santé publique. Pour ce dernier « les systèmes de e-santé en France, conçus dans une vision trop centralisatrice, ont échoué faute d'être suffisamment ergonomiques ». On pourrait imaginer à l'avenir un dossier de santé 2.0 intégrant des données produites par les utilisateurs et des informations établies par des professionnels de santé dans un contexte médical.

L' « ACTIENT » OU LE PATIENT 2.0

Sur ce point les avis divergent fortement. Pour Robert Picard, auteur du rapport du CGEJET cité plus haut, l'un des mouvements à l'origine de la quantification de soi est lié à l'émergence d'une forme de démocratie numérique où Internet permet l'accès à l'information et à l'échange (sur des forums par

exemple). La conséquence directe est que l'individu acquiert une forme de légitimité, une capacité à opposer une « connaissance profane » au savoir médical historique. « Le fait que les gens se renseignent avant la consultation perturbe le médecin dans l'exercice de sa profession. On peut faire le parallèle avec le métier de conseiller financier qui a connu le même phénomène il y a 10 ans. » Le degré de compréhension des médecins est variable. Selon les témoignages recueillis à l'occasion du rapport précité, un tiers des médecins considère que les technologies du côté des patients sont un facteur clé d'amélioration des soins ; un tiers affirme que la revendication des patients est normale et le dernier tiers y est indifférent, voire est d'avis que c'est un élément perturbateur. Le Dr. Laurent Alexandre, lui, est sceptique sur l'intégration de ces données dans un avenir proche, qui suppose en premier lieu que le médecin soit équipé, qu'il puisse prendre le temps et surtout qu'il existe une interopérabilité entre les applications grand public et les logiciels médicaux.

Enfin, le Dr. Postel-Vinay, tout en considérant qu'il y a plus d'avantages que d'inconvénients à ce que les patients aillent chercher des informations, estime que le médecin va perdre de plus en plus le contrôle par rapport à ses patients. Surtout, il s'interroge sur la prise de décision et le régime de responsabilité dans un contexte d'intégration croissante des technologies dans la santé. « La décision prise par la plateforme va-t-elle l'emporter sur la décision humaine ? Cela se fait déjà. Mais mieux vaut une bonne machine qu'un mauvais médecin – et inversement ». Pour le sociologue Dominique Cardon, le fait que les patients puissent être équipés de tensiomètres chez eux ne remet pas en cause le rôle du médecin, pas plus que le recours au monde médical dans son ensemble. Selon lui, le fait que les individus aient aujourd'hui accès chez eux à de nouveaux dispositifs médicaux contribue à augmenter simplement leur niveau d'exigence. D'une certaine manière ils montent d'une marche, au point que les médecins « n'ont jamais reçu autant de demandes de scanners ».

Pour Antoinette Rouvroy, dès lors que les pratiques de quantification de soi passent dans le domaine de la santé « on entre dans de la micro gestion individuelle de sa santé, dans une perspective individuelle de prévention et de perfectionnement qui n'est plus nécessairement médicalement étayée ni contrôlée, qui n'est plus nécessairement basée sur de l'evidence-based medicine, ni sur de l'expertise médicale ». ■

L'INVASION DES CAPTEURS

“ Today, digital sensors can: monitor your tire pressure and avoid dangerous blowouts; analyze the gait of elderly citizens and warn of falls before they occur; follow the gaze of shoppers and identify which products they examine - but don't buy - in a store; monitor which pages readers of a magazine read or skip; float in the air over a factory and independently monitor the plant's emissions; detect impacts in the helmet of an athlete and make it impossible for them to hide potential serious blows to their brains; reveal when a dishwasher, refrigerator, computer, bridge, or dam is about to fail; trigger a different promotion as a new customer walks by a message board; analyze the duration and quality of your sleep; warn drivers that they are about to fall asleep; prevent intoxicated drivers from operating a motor vehicle; warn a person before he or she has a heart attack; detect wasted energy in both homes and commercial buildings; warn a parent or boss when anger is creeping into their voice, to help prevent them from saying or doing things they will later regret; tell waiting customers how far away the pizza delivery guy is from their house; analyze the movements of employees through a factory to detect wasted time and efforts; trigger product demonstrations or interactive manuals when a customer picks up or examines a product; congratulate an athlete when she swings a tennis racquet properly or achieves an efficient stride while running. What can they do tomorrow? ”

Bruce Kasanoff et Michael Hinshaw
Smart Customers, Stupid Companies, 2012

Un **capteur** est un dispositif transformant une grandeur physique observée en une grandeur utilisable dans un instrument de mesure, un système d'acquisition de données. Demain, serons-nous tous captés et mesurés, chaque jour, que nous portions ces capteurs sur nous (ou en nous...) ou qu'ils équipent notre environnement immédiat (notre logement, notre bureau, notre ville, nos transports...)? Smartphone, *smart city*, *smart home*... : derrière l'omniprésence du vocable *smart* dans le marketing de l'innovation numérique se cache en réalité cette invasion des capteurs, des instruments d'acquisition de données et des outils d'analyse et d'aide à la décision qui en sont les compléments obligatoires. La montée en intelligence des objets semble même redonner vigueur et sens à l'expression maintes fois galvaudée d'« internet des objets ».

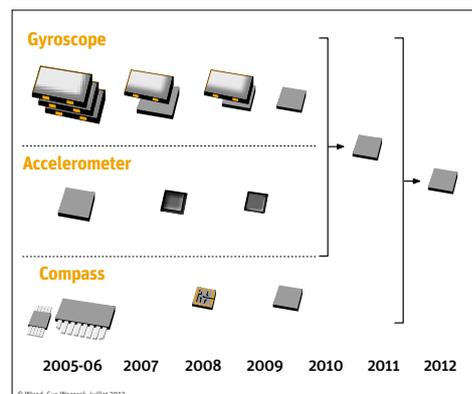
Le domaine de la santé au sens le plus large sera naturellement le marché phare de l'internet des objets : dans son rapport « [Disruptive Technologies](#) » de mai 2013, le McKinsey Global Institute considère que le secteur de la santé portera seul entre un tiers et la moitié de l'impact économique annuel mondial de l'internet des objets en 2025 (qu'il évalue par ailleurs au chiffre mirobolant de 2700 à 6200 milliards de dollars par an...), essentiellement par la réduction des coûts du traitement des maladies chroniques (cf. partie précédente).

Mais pourquoi alors que les technologies de mesure et d'analyse du corps existent depuis une trentaine d'années, et les puces RFID depuis 50 ans, n'émergent-elles que maintenant ?

L'AN 0 DES OBJETS CONNECTÉS

Comme le rappelle Bernard Benhamou, l'adoption de ces technologies a été lente en raison de l'absence d'outils pour les rendre accessibles au grand public. La rupture est venue de l'arrivée des terminaux mobiles et tactiles « intelligents », qui a été l'élément déclencheur, rendant possible le déploiement à grande échelle des dispositifs de mesure de soi.

L'essor de ce marché a eu un effet économique majeur sur le coût des capteurs : l'intégration massive de capteurs de toutes sortes dans des smartphones et tablettes vendus à des millions d'exemplaires a permis en quelques années de réduire drastiquement la taille et le prix de ces composants. À titre d'illustration, la revue *Wired* expliquait dans son [numéro de juillet 2012](#) qu'une puce de smartphone coûtant en 2012 17 \$ pouvait accomplir mesures et calculs qui auraient demandé 6 puces pour un coût total de 60 \$ en 2005 (voir l'illustration ci-après). ■■■



■ ■ ■ Cette démultiplication des capteurs semble être une tendance lourde pour les années à venir :

- chaque génération de smartphones embarque de nouveaux types de capteurs - qui seront demain « détournables » de leur usage premier. Ainsi, en 2013, le Samsung Galaxy S4 contenait, en plus des deux caméras et des micros, [9 capteurs](#) : les classiques gyroscopes (qui mesurent les rotations dans l'espace du téléphone), l'accéléromètre (qui mesure ces mouvements) et le compas, un détecteur de proximité, un détecteur de mouvement, un détecteur de lumière, un thermomètre (qui mesure également l'humidité) et enfin un baromètre. Le smartphone co-conçu par Google et LG, le Nexus 5, intègre pour sa part deux nouveaux capteurs spécifiques dédiés à l'enregistrement et à la mesure des mouvements (exemple : décompter les pas) et Google a annoncé en février 2014 le projet « [Tango](#) », un smartphone capable de capter, scanner et cartographier en 3D tout son environnement immédiat afin de donner à l'appareil, selon les termes de Google, « une compréhension à l'échelle humaine de l'espace et du mouvement ».

- Parallèlement le nombre d'objets connectés est en forte augmentation : par exemple, on estime que 17 millions de bracelets connectés et de montres intelligentes seront vendus en 2014 (source : Canalys) ;

- enfin, selon [Bloomberg](#), le marché des capteurs intégrés à des processeurs (capteurs dits intelligents) devrait passer de moins de 100 millions d'unités aujourd'hui à 2 800 milliards avant 2020, facilitant le développement de réseaux de capteurs déportés autonomes.

Cette démultiplication des capteurs s'associe à une connexion « pervasive » : ces différents capteurs sont en effet généralement intégrés à des objets connectés ou connectables (le smartphone jouant par exemple alors le rôle de *hub* pour un nuage de capteurs reliés à des objets non connectés au réseau global).

Au delà de cette simple rupture économique, les smartphones ont introduit une nouvelle « grammaire ergonomique et gestuelle », auprès du grand public, comme le souligne Bernard Benhamou, faisant écho aux théories du philosophe Bernard Stiegler sur la [grammatisation](#). C'est ici que l'expression d'internet des

objets trouve d'ailleurs sa limite : l'absence de lien à l'humain et au quotidien est en effet la raison principale du retard dans l'émergence de l'internet des objets dans les années récentes. L'internet des objets ne renvoie en réalité qu'au substrat technique sur lequel les pratiques (et marchés) peuvent fleurir : si l'on sait depuis quelques années intégrer techniquement capteurs et connexions dans un réfrigérateur ou une voiture, la véritable rupture est venue du design et de l'ergonomie introduite par Apple avec le lancement de l'iPhone en 2007. Cette révolution a ouvert la route à une croissance fulgurante des objets connectés et à l'émergence de nouvelles pratiques de vie et habitudes, bâties autour de ces capteurs.

L'autre changement de paradigme qui rend cette transition possible est l'essor du *cloud computing*, qui apporte, pour le meilleur et pour le pire, sa souplesse et ses capacités de stockage illimitées. En effet, si le smartphone sert de « *hub* » ou de télécommande aux objets connectés, il sera demain probablement de plus en plus rarement le réceptacle des données, celles-ci devant pouvoir être consultées partout et tout le temps : Bernard Benhamou le souligne en indiquant que si le cerveau de l'internet des objets reste l'« ordinateur mobile » (ce qu'est aujourd'hui par essence un smartphone) qui sert de plateforme de tri et d'analyse des données, ce ne sera pas le cas de la prochaine génération d'objets qui reposeront plus systématiquement sur le *cloud*, et des systèmes de connexions de machine à machine (M2M). De nombreux projets se concentrent d'ailleurs sur des technologies de communication à bas débit et longue distance - particulièrement utiles pour réunir des informations de réseaux de capteurs déportés - comme l'entreprise française [Sigfox](#) qui se définit comme « le 1^{er} opérateur cellulaire bas débit dédié au M2M et à l'Internet des objets » et qui fait la promotion de sa technologie en la présentant comme une infrastructure de communication des objets connectés, permettant de collecter à plusieurs dizaines de kilomètres des informations simples et légères diffusées par des capteurs (par exemple dispersés sur un réseau d'objets nombreux dont on surveille le bon fonctionnement : panneaux publicitaires, alarmes incendies, mobilier urbain...).

LA VIE QUOTIDIENNE AU CŒUR D'UN RÉSEAU DE CAPTEURS INTELLIGENTS

Les capteurs vont donc se multiplier autour de l'individu, mesurant chaque activité et moment de sa journée. Et ces capteurs, souvent dédiés à des fonctions ou finalités premières limitées, sont très aisément détournables : le capteur 3D de la nouvelle console de jeux X box One peut d'ores et déjà en théorie mesurer les battements de cœur à distance. Comme le soulignait en août 2013 le blogueur Robert Scoble, plus le réseau de capteurs nous entourant est dense, plus il est facile d'inférer des informations concernant nos intentions et notre contexte : « pour le moment, votre téléphone ne sait pas réellement si vous marchez, courez, skiez, faites des achats, conduisez ou faites du vélo, mais dans le futur, Google saura tout cela et pourra construire de nouveaux systèmes rendant des services dédiés pendant que vous faites chacune de ces activités (Robert Scoble, *The Next Web* : « [Google, the freaky line and why Moto X is a game-changer](#) »).

Cette connaissance s'infère de nano-informations captées (mouvement, température...) et enrichies de données les décrivant, ces

fameuses métadonnées (sur ce sujet, voir par exemple Hubert Guillaud, « [Big Data : pourquoi nos métadonnées sont-elles plus personnelles que nos empreintes digitales ?](#) » InternetActu 13 décembre 2013). Cette connaissance émerge aussi de l'usage des algorithmes prédictifs et d'autres données (donc du fameux *big data*) et permet de déduire des informations indirectes très intimes à partir d'une innocente collecte du nombre de pas ou d'une courbe de poids sur une longue durée. À terme, elle s'enrichira surtout de l'intimité croissante entre ces capteurs, le corps et son environnement direct, tendance symbolisée par les Google glass. Certains affirment que ces lunettes connectées « intelligentes » ne sont finalement guère plus intrusives qu'un smartphone et que les oiseaux de mauvais augure ne font que reproduire la techno-terreur qui avait saisi les contemporains des premiers appareils photos (c'est en particulier la thèse de Jeff Jarvis sur son site Buzz Machine : [I see you: The technopanic over Google Glass](#), 7 mars 2013). S'il est vrai que ces lunettes utilisent des capteurs qui sont déjà ceux du smartphone (caméra, micro, etc.), elles sont révolutionnaires en ce qu'elles voient tout ce que le porteur voit, alors que le téléphone ne voit que ce que son porteur lui montre. Il s'agit là d'un changement essentiel de perspective dans la mesure où certains de ces nouveaux objets peuvent être connectés en permanence, lorsque d'autres ne sont que « connectables » et n'ont pas nécessairement la capacité à transmettre leurs données de manière autonome. Ici émerge la spécificité du « *wearable computing* » et de l'informatique ambiante : les lunettes voient ce que je vois, la montre peut prendre mon pouls ou mesurer la température de ma peau... Et demain, peut-être, des capteurs mesureront mes ondes cérébrales en permanence. Science-fiction ? Réservés il y a quelques années à des utilisations scientifiques et médicales, des casques d'électro-encéphalographie (EEG) atteignent les rives du marché grand public : [L'EPOC](#) d'Emotiv coûte environ 300 \$ et le [Muse](#) d'interAxon, connecté au smartphone, vise directement un usage de bien-être : son utilisation se veut beaucoup plus transparente que celle des encombrants EEG standards et le Muse doit permettre au porteur de gérer son stress par des capteurs « qui détectent et mesurent l'activité du cerveau » ■■■



LES RISQUES DE PIRATAGE DES CAPTEURS : LES SENSORY MALWARES

Des délinquants informatiques pourraient-ils utiliser les capacités des capteurs pour collecter des informations concernant des personnes à leur insu ? Oui selon des chercheurs qui se penchent sur ces attaques par « sensory malwares » pouvant par exemple utiliser le micro du smartphone pour capter des paroles, sa camera pour photographier le logement, voire son accéléromètre pour inférer le texte saisi des frappes au clavier effectuées à proximité du smartphone. Ce sont des scénarios d'attaque crédibles : le projet « PlaceRaider » d'une équipe de recherche américaine a ainsi développé le concept d'une telle attaque. Leur outil se dissimule dans une application pour smartphone et utilise diverses failles pour prendre aléatoirement des clichés de ce que « voit » la caméra d'un mobile et reconstituer grâce aux capteurs une représentation 3D filmées des lieux... Les chercheurs concluent leur publication par plusieurs recommandations, parmi lesquelles la mise à disposition d'outils de contrôle des capteurs par la personne (permissions d'accès pour chaque application, etc.) ce qui d'ailleurs ne va pas sans poser à nouveau la question de l'efficacité d'une multiplication des contrôles à la charge du seul utilisateur, qui devrait alors devenir l'auditeur-sécurité de ses objets connectés. Au-delà de cet exemple précis, des scénarios d'attaque similaires sont imaginables dès qu'un objet du quotidien devient « smart », comme par exemple les téléviseurs connectés, les voitures et les compteurs intelligents.

Source : L'Atelier, « [La caméra et les capteurs trahissent le propriétaire d'un téléphone](#) », 12 octobre 2012

tout comme un cardiofréquence-mètre mesure l'activité du cœur ». Quand on sait que des chercheurs ont déjà réussi à deviner grâce à l'analyse de données cérébrales des codes secrets de cartes bancaires (voir Geeta Dayal, « *Researchers Hack Brainwaves to Reveal PINs, Other Personal Data* », in *Wired*, 29 août 2012 <http://www.wired.com/threatlevel/2012/08/brainwave-hacking/>) on peut s'interroger sur ce que ces bataillons de capteurs ambiants et omniprésents pourraient révéler de nous à notre insu. (Voir encadré « les risques de piratage des capteurs : les sensory malwares »).

L'ENJEU DES PROTOCOLES DE COMMUNICATION

Un enjeu de standardisation majeur pèse sur l'avenir de l'internet des objets et des communications de machine à machine (M2M). En effet, de nombreuses normes sont en compétition, à commencer par les traditionnels Wifi et Bluetooth, les technologies sans contact et RFID, des normes spécifiques de domotique ou d'objets communicants (Zigby, D-wave...) et des normes propriétaires. Cette situation limite l'expansion des services liés à l'internet des objets, mais elle réduit également la capacité à offrir un environnement de sécurité satisfaisant. Vinton Cerf, un des créateurs du protocole TCP-IP et actuellement Vice président et *Chief Internet Evangelist* de Google, a ainsi appelé de ses vœux la création d'un système d'authentification forte pour les communications entre machines : « beaucoup d'objets connectés vont faire partie de notre environnement et devront être gérés et contrôlés. Il pourrait y avoir 100 ou 200 objets qui nous sont associés, dans nos domiciles, nos voitures, nos bureaux, des choses que nous portons sur nous, et nous ne voulons pas qu'on puisse interférer avec eux, les contrôler ou qu'ils transmettent des informations à des acteurs autres que ceux que nous avons autorisés (...) Pouvons-nous utiliser [des puces d'authentification forte] pour nous aider à gérer ces objets d'une manière qui nous permette d'authentifier solidement les deux bouts d'une communication entre machines ? C'est un défi pour nous tous » ([Vidéo de la présentation](#) de Vint Cerf, Conférence RSA, 27 février 2013).

Un enjeu spécifique de régulation entoure donc l'internet des objets, et la CNIL n'est pas la seule à s'en saisir : face à l'augmentation des plaintes, l'agence fédérale de régulation du commerce aux États-Unis (la FTC) a ainsi lancé fin 2013 une réflexion autour du sujet « internet des objets et vie privée » (séminaire FTC « [Internet of things : privacy and security in a connected world](#) »). Le Groupe européen des autorités de protection des données (G29) se penche également sur la question de l'internet des objets et du *wearable computing*, comme il l'a annoncé dans son [programme de travail 2014-2015](#).

DU CORPS CAPTÉ AU CORPS CAPTEUR

Enfin, les capteurs, en particulier les capteurs intelligents, connaissent une miniaturisation croissante. Plus leur taille sera réduite, plus il deviendra facile de les lier au corps lui-même, voir d'intégrer certains composants dans la personne. La révolution de la captation pourrait donc faciliter l'essor des pratiques dites de « *biohacking* » touchant à l'adjonction d'artefacts technologiques au corps en les rendant plus simples, légères et moins visibles. Cette multiplication des capteurs serait donc un déclencheur ou accélérateur de la tendance à « l'augmentation » numérique de l'homme (cf. partie 02). Anders Colding-Jorgensen, professeur de psychologie à l'Université de Copenhague, pronostique ainsi qu'« avant 2022, vous et moi mettront à jour les données concernant nos fonctions corporelles aussi régulièrement que nous mettons à jour nos statuts Facebook » (voir article de Jesper Knudsen dans *Scenario Magazine*, juin 2012), formule curieusement proche du slogan de l'entreprise [Scanadu](#), qui lance des objets connectés de diagnostic médical « *Check your health as easily as your email* ». L'essor des interfaces entre biologie et informatique pourrait alors donner une nouvelle jeunesse au concept de cyborg, (qui aurait été utilisé pour la première fois dans les années soixante) c'est-à-dire d'organisme cybernétique dans lequel la symbiose entre biologie et technologie serait quasi complète. ■

CONTRÔLER ET VALORISER SES DONNÉES : LES NOUVELLES APPROCHES

“ [...] Les individus sont-ils intéressés à recevoir leurs données ? À l'évidence, il n'existe pas aujourd'hui une forte demande spontanée pour récupérer ses données personnelles, même si certains développements (le quantified self, les services d'agrégation de ses données bancaires...) constituent des signaux faibles dans cette direction. Par ailleurs, si l'on en juge par la faible connaissance et le faible usage que les citoyens européens font des dispositifs de protection de leurs données personnelles, le seul besoin de protection ne constituerait pas un motif suffisant pour qu'ils deviennent en quelque sorte gestionnaires de leurs propres données. La demande n'émergera que si se proposent des outils et des services considérés comme pertinents, utiles, enrichissants et simples d'usage. ”

MesInfos – cahier d'exploration de la FING (mai 2013).

Dans un contexte où l'individu, avec ce monde de capteurs qui se dessine, va se trouver de plus en plus confronté à un déluge de données, dont il est pour beaucoup à l'origine, des interrogations émergent concernant sa capacité à trouver du sens et à maîtriser lui-même son univers numérique. L'individu peut-il avoir prise sur son environnement numérique ou va-t-il au contraire se trouver submergé par les flux de données ? Une chose est sûre, il a un rôle crucial à jouer dans ce nouvel écosystème.

DES RELATIONS ASYMÉTRIQUES DANS LA MAÎTRISE DES DONNÉES

Les individus et les organisations tirant de la valeur de l'exploitation de leurs données personnelles ne jouent pas aujourd'hui à armes égales. Les individus,

malgré un arsenal juridique dédié à la protection de leurs droits, se trouvent souvent dans une situation d'incompréhension face à l'exploitation des données les concernant, et le domaine de la santé et du bien-être n'est pas épargné par l'exploitation des données personnelles, bien au contraire.

Dans l'étude portant sur [les applications mobiles de santé et de bien-être](#) menée en 2013 par l'association américaine *Privacy Rights Clearinghouse*, les politiques de confidentialité des applications sont notamment pointées comme particulièrement porteuses de risques pour la vie privée des utilisateurs. Les premières observations concernent le degré d'information fourni aux individus concernant la gestion des données personnelles : sur les 43 applications étudiées, 26 % des applications gratuites et 40 % des applications payantes n'avaient pas de politique de confidentialité. De plus, 39 % des applications gratuites et 30 % des applications payantes analysées envoyaient des données à des tiers sans qu'il en soit question dans les politiques de confidentialité.

Au-delà de l'évident manque d'information des personnes, l'étude dénonce le décalage qui existe entre les politiques de confidentialité présentées à l'utilisateur et la réalité des pratiques concernant ses données personnelles. Concernant les applications qui publient leur politique de confidentialité, les auteurs de l'étude ont observé que la majorité des pratiques potentiellement à risque pour la vie privée n'était pas décrite de façon claire et compréhensible. Les auteurs expliquent même avoir identifié « une corrélation entre le niveau de détail d'une politique de confidentialité et le risque dans l'utilisation de l'application concernant la vie privée. » Ils ajoutent : « plus la politique de confidentialité d'une application était détaillée, plus les pratiques constatées avaient tendance à porter atteinte à la vie privée. » Difficile pour un utilisateur dans ces conditions d'avoir une réelle maîtrise de ses données personnelles...

PROMOUVOIR LA MAÎTRISE NUMÉRIQUE DE SES DONNÉES

La maîtrise par l'individu des données le concernant pourrait pourtant être source d'« empowerment », c'est-à-dire qu'elle pourrait littéralement lui permettre d'être « mis en capacité d'agir ». Cela s'inscrirait dans une tendance sociétale plus large. Robert Picard, référent santé du Conseil général de ...

l'économie, de l'industrie, de l'énergie et des technologies (CGEJET), donne l'exemple de l'évolution du monde des services. Le consommateur y est invité à « faire soi-même », aussi bien le plein d'essence – le pompiste a disparu – que la gestion directe de son compte bancaire par internet, ce qui a contribué à modifier la relation avec sa banque.

Cette tendance est renforcée par la massification des usages du numérique. Et Internet facilite l'accès à une information potentiellement très spécialisée. Cette dynamique permet à l'individu d'acquérir une forme de légitimité, une capacité à opposer une « connaissance profane »

données ne semblent pas constituer une source de motivation suffisante pour faire évoluer les comportements, comme le soulignait Daniel Kaplan dans [Informatique, libertés, identités](#) (FYP éditions, 2010).

Comment alors créer une nouvelle dynamique redonnant un rôle non seulement central mais aussi actif aux individus dans la gestion de leurs données, et singulièrement des données concernant leur santé ?

Dans le domaine du marketing, certains, comme Doc Searls, militent pour une nouvelle approche dans la relation client. Doc Searls, chercheur associé au *Berkman Center for Internet*

CAHIER D'EXPLORATION MESINFOS



(connaissance du quotidien) à des savoirs historiques établis tels que celui du médecin par exemple. Ainsi, certains estiment qu'il est temps de penser un nouvel équilibre entre l'individu et ceux qui exploitent ses données.

Cette hypothèse de l'*empowerment* des individus pose à l'évidence la question de leur motivation à consacrer temps, énergie et efforts à la gestion ou à la valorisation de leurs propres données. La protection et la sécurité de leurs

and Society de l'Université d'Harvard est un des auteurs du fameux « [Cluetrain Manifesto](#) » qui a mis en évidence que les marchés étaient des « conversations » et que les entreprises avaient trop tendance à négliger la voix de leurs clients ou prospects. Il a théorisé ce qu'il a nommé le « *Vendor Relationship Management* » ([VRM - gestion de la relation vendeur](#)) dans son ouvrage « *The Intention Economy* » (*Harvard Business Review Press*, 2012). Face aux outils de « gestion de relation

client » des organisations (CRM) toujours plus sophistiqués, qui permettent d'analyser les informations relatives aux clients dans une optique de fidélisation, la philosophie du VRM, symétrique du CRM, est d'initier un rééquilibrage de la relation client-vendeur. Recentrer la relation autour du client n'est toutefois pas suffisant pour lui permettre de rétablir un rapport de force plus favorable. Ce dernier doit être doté d'outils lui permettant à son tour d'analyser les offres qui lui sont proposées par les entreprises. Le modèle du VRM encourage ainsi la réciprocité de la relation entre consommateurs et fournisseurs où les outils de CRM des entreprises sont capables de dialoguer avec ceux de VRM de leurs clients...

Plusieurs initiatives s'inspirent de ce modèle et souhaitent favoriser l'émergence d'un nouvel équilibre entre les individus et les entreprises tirant de la valeur de l'exploitation de leurs

données personnelles. Elles ont pour but de redistribuer ces données, et ce faisant, de redistribuer du pouvoir d'agir, avec l'émergence d'un écosystème de gestion des données, dans lequel de nouveaux intermédiaires produiraient et fourniraient aux individus des outils rendant intelligibles leurs données et leur fournissant sur la base de celles-ci des services à valeur ajoutée. Des pionniers de ce marché émergent de toutes parts. Selon les cultures et la nature des initiatives, la philosophie du VRM est cependant interprétée en fonction d'objectifs différents :

■ Aux États-Unis, une logique de modernisation des services publics : l'initiative américaine de *Smart Disclosure* (dévoilement intelligent) s'incarne ainsi en des boutons (*buttons*) cliquables de couleurs différentes, que l'on va retrouver sur les portails en ligne des services publics américains. Ces boutons matérialisent pour les individus la possibilité de télécharger des données ■■■

« BLUE BUTTON »

Le *Blue Button* est un des projets dit de *smart disclosure* (dévoilement intelligent) du gouvernement fédéral américain. L'idée de ce bouton est d'offrir aux usagers la possibilité de télécharger leurs données de santé (en quelque sorte leur dossier médical personnel). Le fait de passer par un bouton unique et reconnaissable simplifie l'utilisation. Ce projet lancé en 2010 était d'abord destiné aux anciens combattants de l'armée américaine, pour l'accès à leur dossier médical de « vétéran ». Plus de 500 organisations – des domaines de la santé, de l'assurance, de la pharmacie, de la défense des consommateurs, etc., certaines ayant plusieurs dizaines de millions d'affiliés – ont rejoint le projet. 2014 semble devoir être une année de quasi généralisation du projet à l'instigation du gouvernement fédéral : des textes de lois sur la santé mettent en avant le droit d'accès et de grands services tel que *Medicare*, le programme d'assurance santé du gouvernement fédéral pour les plus de 65 ans, investissent le projet. Par ailleurs, toutes les agences fédérales doivent prendre part au *Blue Button* pour leur système de prestations de santé au profit de leurs agents. Un [nouveau](#)



[site central](#) a été mis en ligne en février 2014. Ce changement d'échelle du programme passe aussi par des changements techniques : une version plus puissante du programme appelée *Blue Button +* est en cours de déploiement. Dans cette version, les données seront interopérables grâce à des standards et des API (*application programming interface*, c'est-à-dire des interfaces de dialogue entre programmes différents) afin d'inciter les développeurs à la création d'applications tierces qui utiliseront ces données à l'image d'*iBlueButton*, une application pour smartphone qui réorganise ergonomiquement les informations de *Medicare* (Melinda Beck, « [Next in Tech: App Helps Patients Track Care](#) », *Wall Street Journal*, 16 décembre 2013) et qui a remporté un concours de code et de développement (codeathon) centré sur le *Blue button*.

■ ■ ■ les concernant dans un format interoperable : les *green button*, *blue button*, et *purple button* leur permettent d'avoir accès et de télécharger, respectivement, leurs données de consommation énergétique, de santé et celles relatives à leurs diplômes. Fort de son succès, le *Blue Button* fait d'ailleurs l'objet de nombreux développements (voir encadré p. 23) qui tendraient à montrer que ces logiques « d'activation », en l'espèce des patients, sont particulièrement efficaces dans le domaine de la santé.

■ Au Royaume-Uni, une logique consumériste : le gouvernement porte le projet « Midata », qui regroupe des acteurs du commerce et de l'industrie, ainsi que des consommateurs. Il s'agit avant tout de donner la possibilité au consommateur de faire des choix éclairés. L'empowerment est donc principalement vu sous un angle consumériste. La personnalisation des services, encouragée dans le programme, peut avoir un impact dans le domaine de la santé et permettre une réduction des dépenses. C'est l'objectif de l'application MiHealth, dont le prototype est présenté sur le site du midata innovation lab. En favorisant une bonne compréhension par les utilisateurs de leurs données de santé, en les incitant à poursuivre des objectifs et en facilitant les échanges à distance entre utilisateurs et professionnels de santé, l'application est présentée comme une alternative à une intervention médicale.

■ En France, la Fondation Internet Nouvelle Génération (Fing) coordonne l'expérimentation MesInfos, qui réunit diverses entreprises privées et que la CNIL accompagne de son expertise. Cette expérimentation souhaite encourager l'émergence d'un marché des « services personnels de données », dans l'optique que ce mouvement de retour des données aux individus bénéficiera aussi aux entreprises, en leur permettant de recréer une réelle relation de confiance.

Dans une perspective « Informatique et Libertés », ces initiatives peuvent être appréhendées comme une forme de renouveau du droit d'accès et de rectification, plus « 2.0 », avec une dimension active de l'individu, qui s'orienterait vers un « droit d'accès et de récupération », voire un « droit de récupération et d'action ».

Toutefois, s'il est possible de considérer que ces initiatives correspondent à une aspiration des individus, il peut également s'agir, dans

certains cas, d'une stratégie d'entreprises qui auraient intérêt à faire porter la charge de la gestion des données personnelles sur le consommateur, ou encore, de manière cynique, à réduire les données personnelles à une forme de marchandise. Cette vision se rapproche finalement d'une conception de l'empowerment individuel qui repose sur la « patrimonialisation » des données personnelles. Divers projets aussi bien en Europe qu'aux États-Unis se revendiquant d'une approche « VRM » tentent en effet de créer une sorte de marché de la location/cession des données personnelles, où les individus ont la possibilité d'être rémunérés en espèces sonnantes et trébuchantes en échange de la communication de tout ou partie de leurs informations personnelles, qui pourraient potentiellement concerner la santé.

DES LIMITES À L'EMPOWERMENT ?

Face au volume et à la complexité des données personnelles qui seraient ainsi « restituées », il n'est pas assuré que les utilisateurs d'un service mettant à disposition ces données soient en mesure d'en tirer du sens et y trouvent un intérêt. Il restera tout d'abord toujours une part d'individus n'ayant pas la pratique des ordinateurs, smartphones, tablettes... nécessaires pour accéder à leurs données. De plus, la manipulation et la compréhension de données nécessitent du temps, des compétences, un apprentissage, ainsi que le développement d'interfaces et de dispositifs numériques de médiation à la donnée les plus simples possibles. Cette problématique pourrait être particulièrement prégnante dans le domaine du *quantified self*, où, faute d'une médiation médicale le risque est réel, par une mauvaise interprétation des chiffres, de susciter angoisse et prises de décisions erronées. Comment réagissons-nous face à ces quantités énormes de données concernant le fonctionnement de notre métabolisme et de notre corps ? Comment les interpréter ? Comment ne pas créer surtout l'empowerment d'une société hypocondriaque ?

Rafi Haladjian, spécialiste des objets connectés, fondateur de Sen.se et de Mother, [explique d'ailleurs que la motivation et l'intérêt des utilisateurs](#) pour leurs données passe par une

courbe d'apprentissage qui n'est pas linéaire dans le temps. En particulier, pour tirer de la valeur de ses propres données une fois passée par la période de découverte, il faut, selon lui, en avoir accumulé un certain volume. Pour arriver à cette masse critique, tout le challenge réside alors dans les outils techniques qui vont permettre aux individus de dépasser la phase qualifiée de « traversée de désert » par Rafi Haladjian où les efforts nécessaires pour acquérir de nouvelles données sont peu productifs au regard de la valeur générée. C'est pour cette raison que l'outillage mise à disposition des individus pour collecter, stocker et établir des corrélations entre leurs données est essentiel.

ENTRE REPLI SUR LE SELF ET DÉMARCHE CITOYENNE

Considérant ces phénomènes d'un point de vue global, la philosophe Antoinette Rouvroy pointe les limites des initiatives de retour des données aux individus. Elle appelle même à la prudence quand il s'agit de manier le concept d'*empowerment*. Elle explique qu'elle « ne pense pas que donner aux individus la propriété de leur propre trace et de leurs données suffise à leur donner du pouvoir ». Pour elle, « l'émancipation n'est pas séparable du collectif, d'une inter-individualité qui ne soit pas uniquement centrée sur le self ». Autrement dit, la seule maîtrise par l'individu de « ses » données, tout en lui conférant un sentiment de contrôle, ne l'incite guère à sortir d'un individualisme possessif, indifférent aux enjeux collectifs.

La possibilité de rendre les individus plus responsables de leur bonne ou de leur mauvaise santé risque ainsi de distraire l'attention sur les causes environnementales ou socioéconomiques de la mauvaise santé, au profit de causes comportementales (cf. avant-propos)...

Cela rejoint [l'analyse d'Evgeny Morozov](#) qui considère que le mouvement de retour des données aux individus ne doit pas occulter les questions éthiques - de surveillance par exemple - concernant la gestion des données en démocratie. Il explique : « Je voudrais que les citoyens soient plus politisés quant au rôle que jouent les données dans la vie démocratique. Je voudrais

qu'ils pensent au rôle que pourrait jouer leur propre participation sur le marché des données et comment cela pourrait avoir une incidence positive sur la démocratie. » (source : Place de la Toile, France Culture, 25 janvier 2014).

S'inscrivant dans cette logique, certaines initiatives entendent favoriser une mobilisation collective. Elles mettent en avant une approche « citoyenne » de la collecte et du traitement de données. Laurence Allard, sociologue, fait partie de l'association [Labo Citoyen](#), qui encourage les individus à produire eux-mêmes des données concernant leur environnement. Une expérimentation a ainsi été menée sur les données atmosphériques. La collecte de ces données s'est faite par l'intermédiaire de capteurs assurant aux utilisateurs la maîtrise des données produites, qui ne transitent par aucun tiers. Laurence Allard explique que l'usage des capteurs, en donnant une meilleure connaissance de leur environnement par les individus, va permettre d'alimenter des débats, voir de « faire agir » les individus. C'est ce qu'elle appelle le « nous quantifiant », en alternative aux « usages privatistes » du *quantified self*.

À terme, on peut imaginer que les données produites par les individus viendraient compléter celles des organisations publiques ou privées. Ce mouvement participerait à la diminution de l'asymétrie dénoncée par Doc Searls, et pourrait favoriser l'émergence de discussions collectives.

À l'occasion de l'expérimentation de l'association Labo Citoyen portant sur la pollution atmosphérique, les données de qualité de l'air produites par les individus à une échelle très locale ont ainsi pu compléter celles produites par des capteurs institutionnels et plus globaux de pollution. Cette complémentarité a permis une connaissance plus fine de la situation atmosphérique, mêlant données institutionnelles et données « crowdsourcées », issues de « la foule ».

Dans le domaine de la santé, on pourrait imaginer la même symbiose, entre des systèmes d'information collectifs en santé publique et les données fournies par les individus, ces derniers prenant alors pleinement part aux décisions les concernant. ■

02



Partie 0.2

ÉCOSYSTÈME ET JEU D'ACTEURS

MARCHÉ DE LA SANTÉ SUR MOBILE ET MODÈLES ÉCONOMIQUES DES NOUVEAUX ENTRANTS	28
LES ACTEURS TRADITIONNELS DE LA SANTÉ, ENTRE INNOVATION ET DISPARITION ?	32
<i>SCÉNARIO PROSPECTIF : " FUSIONS, ACQUISITIONS ET MODÈLES ÉCONOMIQUES DANS LE DOMAINE DES OBJETS CONNECTÉS DE LA SANTÉ ET DES ASSURANCES : OÙ EN EST LE MARCHÉ ? "</i>	36
LE PROJET TRANSHUMANISTE : L'HOMME CAPTÉ, AUGMENTÉ, ... IDÉAL ?	38

MARCHÉ DE LA SANTÉ SUR MOBILE ET MODÈLES ÉCONOMIQUES DES NOUVEAUX ENTRANTS

“ Alors que les technologies de mesure et d'analyse du corps existent depuis une trentaine d'années - les puces RFID depuis 50 ans - elles n'émergent que maintenant. Si l'évolution a été lente, c'est parce qu'il n'y avait pas d'outil pour les rendre accessibles au grand public. On assiste aujourd'hui à un changement du paysage industriel. La « logique d'Apple » va-t-elle s'appliquer, comme pour l'énergie, à la santé ? Probablement... Les objets coûtent beaucoup moins cher. Les acteurs en ont bien conscience : General Electric (constructeur de Scanner, d'IRM) sait que ses concurrents ne sont pas Siemens ou Nokia mais Apple et Google. ”

Bernard Benhamou,
Délégué aux Usages de l'Internet

Le marché de la « m-health » est une illustration intéressante du potentiel de développement de nouveaux usages numériques, au carrefour d'une offre grand public banalisée, de l'équipement massif en smartphones et de parcours de soins d'un nouveau genre.

Par ailleurs, les modèles économiques des acteurs produisant des capteurs ou des applications mobiles en ce domaine sont majoritairement fondés sur la monétisation des données produites par leurs utilisateurs.

PRINCIPALES TENDANCES ET ORIENTATIONS DU MARCHÉ DE LA M-SANTÉ À L'HORIZON 2017

Dans une étude publiée en mars 2013, le cabinet Research2guidance estime que le marché de la santé sur mobile

(m-santé) devrait représenter 26 milliards de dollars à l'horizon 2017 et concerner près de 1,7 milliards d'utilisateurs (*Mobile Health Market 2013-2017*).

Le marché de la m-santé y est appréhendé de manière large puisqu'il inclue les applications de *self-tracking* grand public ainsi que les applications destinées aux professionnels de santé.

Le développement de ce marché est caractérisé par 3 grandes étapes de maturité :

- une phase dite « pilote » de 2000 à 2008, avec l'apparition des premières applications mobiles de santé ;
- la création de l'Appstore de Apple en 2008, qui marque une rupture dans le développement du marché et l'entrée dans la phase de « commercialisation », avec la première place de marché permettant aux éditeurs de distribuer directement leurs applications ;
- enfin, la phase de « consolidation » attendue à partir de 2015/2016, qui devrait notamment se traduire par des applications pouvant s'intégrer directement dans un parcours de soins.

Le développement de ce marché qui, entre 2010 et 2012, est passé de 17 000 à 97 000 applications mobiles de santé disponibles dans les principaux magasins d'applications, est principalement entretenu par 5 grandes tendances :

- ▶ la croissance des équipements en smartphone de 2^{ème} génération,
- ▶ l'émergence de magasins d'applications spécialisés – comme [Happtique](#) créé en 2000 et qui référence plus de 7000 apps évaluées et classées notamment selon des critères de sécurité – qui ont vocation à guider les patients utilisateurs ou les professionnels de santé vers les applications les plus fiables,
- ▶ le rôle croissant des professionnels de santé dans la recommandation d'applications en direction des patients, en particulier pour des apps s'intégrant au parcours de soins,
- ▶ la spécialisation des éditeurs d'applications sur le diagnostic et le traitement des maladies chroniques comme l'obésité, l'asthme, l'hypertension ou le diabète,
- ▶ la diversification des sources de financement : en ce qui concerne la première génération d'applications de santé, les revenus étaient principalement issus du téléchargement de l'application et/ou des abonnements qui conditionnent l'accès aux services de santé pour une période de temps donné. Les prochaines générations d'applications santé plus sophistiquées vont voir leurs sources de revenus se diversifier par la vente de capteurs spécifiques, et de produits ou de services liés à ces capteurs (i.e : abonnements

payés par les professionnels pour suivre l'état de santé des patients à distance).

Ces évolutions devraient conduire à augmenter le nombre de téléchargements à plus de 4 milliards en 2017. La part des applications payantes devrait fluctuer pour atteindre un niveau moyen de 10% sur les 5 prochaines années.

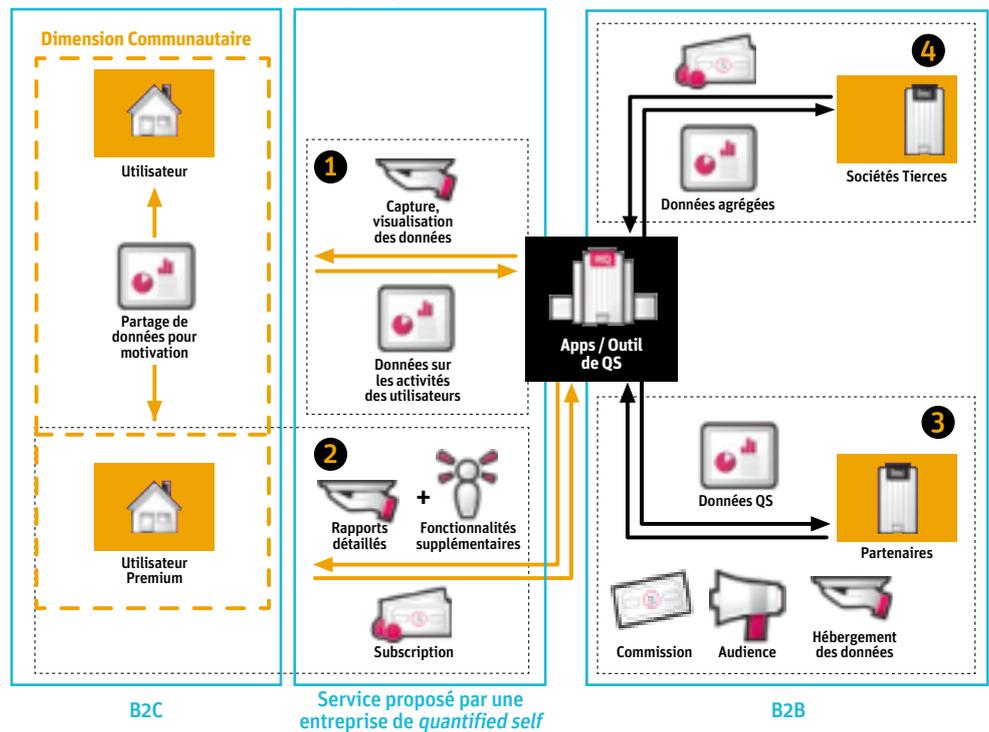
Les utilisateurs d'applications de m-santé téléchargeront entre 2,5 et 7 apps par an, avec une diminution du nombre moyen d'applications téléchargées avec le temps. D'une part en raison de la démocratisation du marché où les nouveaux utilisateurs ne viendront que pour un besoin spécifique, et en raison de l'amélioration des applications, plus fiables, qui conduira à ce que les utilisateurs n'en essaient pas plusieurs pour le même besoin.

LA DONNÉE AU CŒUR DU MODÈLE ÉCONOMIQUE DES NOUVEAUX ENTRANTS

Au-delà des revenus issus de la vente de capteurs ou d'applications (lorsque celles-ci sont payantes), le modèle économique des nouveaux entrants sur le marché du *quantified self* (tels que Withings, Fitbit, Runkeeper, Jawbone, Nike+...) est généralement organisé autour de 4 logiques économiques visant à monétiser des données personnelles.

Le schéma ci-après décrit les relations unissant un produit ou service à ses différents segments de clientèle (B et/ou C) et la manière dont ces relations sont monétisées. Le modèle économique se décompose en 4

MODÈLES ÉCONOMIQUES / MÉTHODOLOGIE DE BOARDOFINNOVATION.COM



Le marché potentiel des utilisateurs de m-santé (équipés en smartphone) va passer de 1 milliard en 2012 à 3,4 milliards en 2017, 50% du marché devrait être couvert en 2017 (un utilisateur aura téléchargé au moins une application). La vente d'appareils ou capteurs connectés devrait représenter la deuxième source de revenu avec près de 5 milliards de dollars alors que les services (i.e : abonnements payés par les professionnels pour suivre l'état de santé des patients à distance) pèseront pour plus des deux tiers.

parties, les deux premières concernent des logiques de monétisation directement auprès de l'utilisateur final (données, premium), les deux autres en direction d'acteurs économiques partenaires.

1. Données. La base du modèle économique de la plupart des éditeurs de service – qui est parfois résumé par l'adage « si vous ne payez pas pour le service, c'est que vous êtes le produit » – est d'offrir gratuitement l'accès à un service et de récolter en contrepartie des données d'usages, comportementales, relatives aux

- utilisateurs, leur permettant, par exemple, de proposer des publicités ciblées.

2. Premium. Le modèle *Freemium*, traditionnellement utilisé par les acteurs du Web pour monétiser les données des utilisateurs, consiste à offrir gratuitement les fonctionnalités basiques du service et à faire payer les fonctionnalités avancées. À titre d'exemple, Fitbit, la société qui propose depuis plusieurs années un podomètre connecté qui décompte le nombre de pas, les étages gravés et les calories brûlées qui y sont associées, fournit gratuitement une interface de visualisation aux utilisateurs finaux pour qu'ils puissent suivre l'évolution de leurs activités. En revanche, seuls les comptes payants (premium) ont la possibilité de pouvoir se comparer et de se situer par rapport à la moyenne des autres utilisateurs du service, d'avoir accès à des rapports détaillés ou de télécharger leurs données.

3. Revente « données agrégées ». Ces mêmes données peuvent aussi être revendues de manière « agrégée » ou « anonyme » à des tiers dans une logique B2B : les mesures liées au poids peuvent par exemple intéresser des équipes de recherche ou des laboratoires pharmaceutiques. Des sociétés commerciales peuvent aussi être intéressées par ces données en vue de l'implantation de points de vente (ex : un magasin d'articles de sport sur la base des données géolocalisées issues de Runkeeper). Ces données sont généralement décrites dans les politiques de confidentialité comme étant « non-nominatives » au sens non reliées directement à un individu mais demeurent des données à caractère personnel au travers des informations liées à la géolocalisation ou socio-démographiques qui peuvent y être intégrées. Cette partie du modèle économique et de la circulation des données est la moins visible pour l'utilisateur – en tout cas celle pour laquelle il dispose de peu d'informations.

4. Stratégie de Plateforme. La stratégie vers laquelle tendent la plupart des acteurs du monde du *quantified self* est de s'établir en tant que plateforme, en devenant une sorte de « Facebook des données de bien-être et de santé ». Runkeeper est probablement l'acteur le plus avancé dans cette stratégie qui consiste à inciter les utilisateurs à centraliser un maximum de leurs données sur la plateforme en proposant à des entreprises tierces d'avoir accès et/ou d'injecter des données au travers d'APIs (*Health Graph API* dans le cas de Runkeeper). Runkeeper était initialement une application pour smartphone permettant d'enregistrer la trace d'activités sportives en utilisant les capteurs du mobile, principalement le GPS (kilomètres parcourus,

dénivelé, calories consommées). Fort de 25 millions d'utilisateurs, Runkeeper a alors développé une stratégie consistant à basculer progressivement d'une logique de monétisation de fonctionnalités avancées de l'application (modèle premium) à une logique de valorisation des données. L'application mobile est alors devenue un simple moyen parmi d'autres pour générer des données de bien-être alimentant la plateforme. Cette stratégie s'est poursuivie par l'ouverture d'une API – une forme de prise ou de connecteur – permettant de pouvoir échanger plus facilement des données avec d'autres services partenaires. Le modèle de plateforme est certainement celui qui caractérise le mieux les modèles économiques du numérique, pour la plupart organisés en marché bi-face constitué des utilisateurs finaux d'un côté, et des entreprises partenaires de l'autre. Il est particulièrement adapté à la logique du *quantified self* dans la mesure où les utilisateurs finaux ont un intérêt à regrouper au sein d'un seul espace leurs différents jeux de données, ce qui en facilite la consultation, et surtout les possibilités de croisement en vue d'établir des corrélations, motivation importante des pratiques de *quantified self* (cf. partie 01). Du côté des entreprises partenaires, plusieurs formes d'incitations commerciales peuvent être proposées par la plateforme. La toute première est l'accès aux utilisateurs finaux membres de la plateforme qui constituent autant de nouveaux clients potentiels. La possibilité pour les partenaires d'obtenir des commissions sur la vente de produits ou services peut également être avancée. Runkeeper a mis en place un modèle d'affiliation de ce type pour les applications partenaires de son programme Health Graph API : si un utilisateur opte pour un compte payant par l'intermédiaire d'une application partenaire, cette dernière est rémunérée sous forme d'une commission sur l'abonnement. Enfin, la plateforme peut proposer une mutualisation (ou l'économie) des coûts liés à l'hébergement des données. C'est aussi ce que Runkeeper valorise en direction de ses partenaires en leur ouvrant sa plateforme de stockage.

Finalement, les modèles économiques des acteurs du *quantified self* empruntent des logiques que l'on retrouve chez les grands acteurs du Web et reposent en grande partie sur la valorisation des données, véritable « pétrole » pour certains, « oxygène » pour d'autres de l'économie numérique. En effet, pour que la plateforme existe et perdure il importe que des tiers, des « sur-traitants » comme les nomment Henri Verdier et Nicolas Colin dans « L'Âge de la

Multitude », puissent avoir accès aux données des utilisateurs pour bâtir des services à valeur ajoutée. C'est le modèle popularisé par Facebook laissant la possibilité aux membres d'installer des applications tierces sur leur profil. À titre d'exemple, une application populaire sur la plateforme Runkeeper est Earndit. Elle permet aux membres l'ayant installée de gagner des points à chaque nouvelle activité enregistrée. Concrètement, il s'agit de convertir des kilomètres parcourus ou des minutes d'efforts en points. Ces points sont ensuite ré-utilisables sous forme de bons de réduction auprès de partenaires sélectionnés par Earndit, et généralement en lien avec les activités de l'utilisateur. Le contrat entre l'utilisateur et l'application est ainsi de laisser l'accès à ses données en contrepartie d'avantages ou de services additionnels.

Pour l'acteur qui joue le rôle de plateforme, tout l'enjeu est de réussir à transformer ses concurrents potentiels en partenaires. Dans un environnement concurrentiel où plusieurs acteurs poursuivent la même stratégie, « le gagnant » est celui qui parvient à fédérer l'écosystème le plus étoffé autour de sa plateforme. Il va permettre de générer des applications et des usages innovants, susceptibles d'attirer de nouveaux utilisateurs et partenaires, qui vont conforter son positionnement...

Ces différents modèles ne sont pas exclusifs les uns des autres, les applications et services proposant la captation et l'analyse des données de bien-être mobilisent souvent plusieurs logiques.

LES API, PIERRE ANGULAIRE DES STRATÉGIES D'ACTEURS

Du fait du caractère émergent de ces usages et applications, le positionnement des acteurs, leur modèle économique et en particulier leur stratégie en matière d'API restent fragiles. Aujourd'hui, dans un souci d'accompagnement de démarrage du marché, la plupart des acteurs économiques ont choisi une approche ouverte et réciproque permettant d'exporter / d'importer des données vers / en provenance de leurs concurrents-partenaires, dans un mouvement de collaboration opportuniste que sacralise l'expression « coopération ».

Cette relative ouverture peut d'ailleurs permettre à des *pure players*, ne proposant ni application, ni capteur connecté d'essayer de se faire une place en proposant un service basé exclusivement sur des fonctionnalités de visualisation et d'agrégation de données éclairées jusque-là sur différents services. C'est par

exemple ce qu'ambitionne le projet Human Api (www.humanapi.co) qui, dans une philosophie très « VRM » en apparence (cf. partie 01), propose aux utilisateurs de services d'automesure de connecter l'ensemble de leurs données en vue de « bâtir l'infrastructure des données de santé ». Or, et comme le montre la courte histoire du Web, ce type de stratégie ne s'avère pas toujours gagnante car elle est par nature extrêmement dépendante des politiques d'API des autres services. Les exemples de Facebook avec l'API de contact de Gmail, ou plus récemment d'Instagram avec Twitter montrent que le caractère ouvert, gratuit et réciproque des API mises en place par ces acteurs peut être remis en question en fonction de l'évolution du positionnement stratégique des autres acteurs. Google n'émettait pas d'objection à ce que Facebook puisse parcourir les carnets d'adresses des utilisateurs de Gmail tant que le réseau social restait d'une envergure modeste et ne concurrençait pas ses activités. De la même manière Instagram avait tout intérêt à ce que les photos de ses membres soient directement visibles depuis la *timeline* Twitter lorsqu'il était en phase d'acquisition de nouveaux utilisateurs...

Ces stratégies s'affinent donc progressivement, ce qui peut compliquer – voire invalider – le modèle d'affaire de certains acteurs, et affecter par là même les utilisateurs finaux qui n'auraient plus accès à certaines fonctionnalités.

En termes de protection des données personnelles et de la vie privée, ces modèles économiques soulèvent plusieurs séries d'interrogations, dont la première, essentielle, est liée au fait même que la donnée personnelle soit au cœur de ces modèles : dans quelle mesure et à quelles conditions peut-on admettre que ces données issues du corps humain puissent faire l'objet d'une monétisation ? (cf partie 03)

- En outre, la centralisation de ces données, par nature sensibles, interroge leur sécurisation;
- Le partage et la circulation des données, au cœur des modèles économiques posent tout autant de questions : où sont-elles réellement stockées ? L'utilisateur en a-t-il conscience ? Dispose-t-il d'un contrôle réel ? Est-il informé de la revente possible de ses données ?
- Enfin, une caractéristique des marchés bi-face est qu'ils sont susceptibles de générer des tensions entre les différents segments de clientèle dont les intérêts ne sont pas nécessairement alignés. En particulier, un service de *quantified self* pourrait avoir intérêt à favoriser les intérêts de ses partenaires économiques au détriment de ceux des utilisateurs finaux. ■

LES ACTEURS TRADITIONNELS DE LA SANTÉ, ENTRE INNOVATION ET DISPARITION ?

“ La médecine, dans le nouveau paradigme, doit d'abord s'intéresser à la santé des gens sains. (...) On s'intéresse aux individus sains, non pas tant avec l'objectif de les guérir ou de les préserver d'une maladie que pour leur permettre une gestion optimale de leur santé, en fonction d'une évaluation continue de son état. (...) L'assurance maladie doit-elle prendre en charge cette médecine de la santé ? Il n'y a aucun risque à couvrir, seulement un service d'examens et de conseils à fournir en continu. Doit-elle se cantonner dans sa fonction traditionnelle qui est de donner accès aux soins pour les personnes qui tombent malades ? Doit-elle financer une offre pour cette médecine de la santé, cette médecine perpétuelle ? La question ouvre sur une deuxième interrogation : l'assurance maladie peut-elle le faire, au sens où elle serait légitime à le faire ? Ne peut-on pas craindre qu'on ne l'accuse de vouloir surveiller ses assurés ? Les données produites par la médecine prédictives ne relèvent-elles pas de la *privacy* la plus privée ? N'y a-t-il pas, de ce point de vue, des motifs suffisants pour que l'on sépare rigoureusement les deux circuits de la médecine prédictive et de la médecine curative, financée par l'assurance ? N'est-ce pas ce que de nombreux législateurs ont voulu faire en rendant ces données indisponibles pour certains types d'assurance ? ”

François Ewald,

professeur honoraire au CNAM, « Assurance, prévention, prédiction... dans l'univers du Big Data », rapport pour l'institut Montparnasse, 2012.

L'émergence de nouveaux acteurs et de nouveaux usages investissant les champs de la santé et du bien-être n'est pas sans effet sur les acteurs « traditionnels » de la santé. Ces derniers, qu'il s'agisse du corps médical, de l'industrie pharmaceutique, du monde de l'assurance ou de la protection sociale, commencent à investiguer de nouvelles opportunités. Un environnement santé / bien-être émerge, dans lequel des acteurs historiques côtoient désormais de nouveaux entrants, porteurs d'usages et de modèles économiques « disruptifs ». Des modalités de partage des rôles au sein de ce nouvel écosystème s'esquissent.

LE MÉDECIN, PREMIER TIERS DE CONFIANCE

L'arrivée d'acteurs économiques mobilisant le numérique comme un moyen de développer de nouvelles approches de la santé et du bien-être ne doit pas être interprétée uniquement comme l'ouverture d'une lutte entre les représentants du « vieux monde » et les « modernes ».

Les modèles économiques des nouveaux acteurs reposent en grande partie sur la valorisation des données des utilisateurs. Ce traitement des données peut être source d'inquiétude chez les utilisateurs. Celles-ci peuvent être considérées comme sensibles par les individus, car ayant trait à leur intimité. L'enjeu pour les créateurs d'applications et/ou de capteurs est donc de fournir un environnement adapté à la nature de ces données et d'instaurer une relation de confiance avec leurs utilisateurs.

Or, s'il y a bien un acteur qui bénéficie d'un fort capital de confiance concernant la confidentialité des données touchant à la santé, c'est le médecin. Les nouveaux acteurs s'aventurant sur la frontière santé / bien-être peuvent avoir intérêt à mobiliser ce capital confiance. Selon un sondage Ifop pour l'Atelier BNP Paribas réalisé en novembre 2013, « [Les objets connectés, au centre d'un nouvel écosystème de santé ?](#) », 63% des Français considèrent qu'en cas de partage de données de mesure issues d'objets connectés, ce sont les professionnels de santé qui sont les plus à même d'en assurer la gestion. Mais dans le même temps, se rapprocher du médical au point d'être considéré comme un acteur intégré au parcours de soins peut être source de contraintes réglementaires supplémentaires. Les nouveaux acteurs, qui semblent parfois hésiter entre bien-être et santé, vont être confrontés à cette quête de la confiance des utilisateurs, ce qui semble-t-il imposera de donner un rôle actif au médecin et de porter sans doute plus attention aux contraintes de sécurité.

DES SYSTÈMES DE SANTÉ EN TRANSFORMATION

Cette analyse au seul prisme de la confiance n'est pas suffisante pour appréhender les changements à venir pour les acteurs traditionnels du domaine de la santé. Ceux-ci vont se trouver aux prises avec les nouveaux entrants amenant avec eux une perturbation des modèles économiques en place.

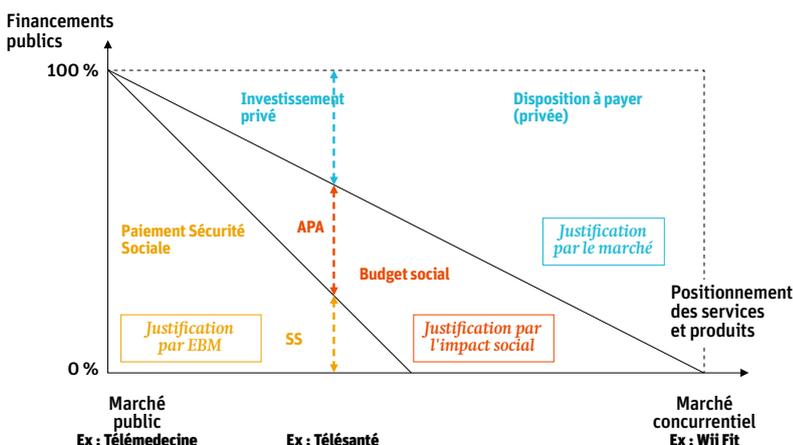
Les modèles économiques des acteurs de santé sont traditionnellement centrés autour d'une médecine fondée sur les faits (Evidence-Based Medicine, EBM), basée sur les expertises des cliniciens et des données statistiques externes, afin de proposer des traitements adaptés aux patients. Cette expertise externe est assurée principalement par des financements publics. Lors du colloque « [Le numérique au service de la santé et du médicosocial : passer de l'expérimentation au déploiement](#) » (Colloque de la Mission Ecoter, avril 2013), Robert Picard a souligné le fait que cet écosystème était en train de se complexifier, avec l'émergence d'un marché plus large de bien-être et de prévention. Le schéma ci-dessous présente les différentes facettes du marché de la santé à l'heure du numérique. À côté du « marché public » de la santé numérique, financé par la sécurité sociale, qui s'appuie sur la médecine fondée sur les faits, Robert Picard identifie un second cas, dans lequel le financement n'est pas assuré par la sécurité sociale, mais par un budget dédié aux affaires sociales. La justification se base sur un « impact social » identifié, nécessitant une prise en charge publique : il donne l'exemple de l'Allocation Personnalisée d'Autonomie (aide sociale en faveur des personnes âgées et dépendantes) et de la possibilité de mettre en place des dispositifs de télésanté. Il identifie enfin une situation dans laquelle une logique de marché prévaut. Le financement est privé, il repose sur la « disposition à payer » des individus, en fonction d'objectifs de bien-être par exemple. Ce marché concurrentiel est la porte d'entrée dans la santé des nouveaux acteurs de la santé et du bien-être numérique.

Les innovations numériques dans le domaine de la santé et du bien-être ont en plus vocation à s'intégrer dans un monde connecté qui n'est pas restreint à ce seul domaine. Pour Nicolas Colin, auteur avec Henri Verdier de *l'Âge de la multitude*, « [le logiciel dévore le monde](#) », et il y a une convergence entre des innovations numériques initiées dans de multiples domaines. Dans l'article « [un jour, Google construira des maisons](#) » (source : le Moniteur, 24 janvier 2014), il montre ainsi le lien entre capteurs dédiés à l'habitat et capteurs de santé : « Si l'opérateur déploie les bons capteurs dans votre habitat, ceux-ci pourront mesurer votre rythme de vie, les conditions atmosphériques à l'intérieur de l'habitat et établir des corrélations entre votre état de santé et ce qui se passe dans votre logement afin de favoriser une meilleure régulation de votre rythme de sommeil, faire en sorte que vous soyez moins malade... » Le marché est immense et les acteurs y sont multiples et inattendus - comme l'explique également Bernard Benhamou.

LES STRATÉGIES D'ADAPTATION DES ACTEURS TRADITIONNELS

L'industrie pharmaceutique semble commencer à réagir, en prenant conscience que ses modèles économiques vont être bouleversés dans les années à venir. Une étude conduite par Arthur D. Little et le Karlsruhe Institute of Technology auprès des acteurs de l'industrie pharmaceutique, publiée en décembre 2013, « [Impact of Digital Health on the Pharmaceutical Industry - Will Business Models be Reshaped by Digital Health?](#) », pointe les évolutions majeures qui vont toucher l'industrie pharmaceutique dans les années à venir, du fait du développement de la e-santé. Par e-santé, les auteurs désignent la convergence entre les technologies numériques - dont les Big Data - et les structures de la chaîne de valeur traditionnelle de la santé. Au sein de cet univers, la m-santé est particulièrement porteuse de changements. Intégrée aux parcours de soin, elle joue en effet le rôle d'un catalyseur, qui permet aux multiples facettes de la e-santé d'exprimer leur potentiel : l'éducation des individus à leur propre santé en ligne, le suivi en ligne de routines quotidiennes ayant trait à la santé, les capteurs, les objets intelligents permettant de suivre l'observance d'un traitement par les patients, etc. Cette dynamique portée par la m-santé modifie le marché, et peut être source de réduction des coûts. Pour ■■■

REPRÉSENTATION CARTOGRAPHIQUE DU MODÈLE ÉCONOMIQUE, ROBERT PICARD



- s'adapter à ces changements et être en mesure d'intégrer ces évolutions à leurs offres, les acteurs de l'industrie pharmaceutique doivent mener une stratégie active. Le rapport souligne que les programmes de e-santé sont encore au stade de l'évaluation. Mais 73% des professionnels de l'industrie pharmaceutique interrogés considèrent qu'ils seront mis en place d'ici à 2020. Pour mener cette évolution, les acteurs de l'industrie considèrent qu'ils devront développer de nouvelles compétences et de nouveaux partenariats, avec les financeurs, les professionnels de santé, les entreprises de logiciel et les entreprises produisant des dispositifs médicaux.

À court terme, l'adaptation des acteurs traditionnels des assurances passe par l'intégration des applications mobiles santé / bien-être à leur stratégie. Cette démarche pourrait consister à inciter d'ores et déjà les assurés possesseurs de smartphones à télécharger des applications spécifiques. Elle serait rapide à mettre en place car elle s'appuie sur des usages préexistants. Elle pourrait s'accompagner le cas échéant d'une démarche de labellisation par les autorités sanitaires.

Le *quantified self* pourrait ainsi s'intégrer dans les offres des assurances, *a minima*, dans un premier temps, dans une logique préventive. Julien Guez, directeur de la stratégie, du marketing et des affaires publiques chez Malakoff Médéric, grand groupe français de protection sociale et assureur complémentaire santé, explique que des animations de sensibilisation autour de l'automesure durant lesquelles sont présentés des capteurs, de type balance ou

tensiomètre, ont d'ores et déjà lieu. En Suisse, la mutuelle « Groupe Mutuel » proposait de [rembourser à hauteur de 25%](#) l'achat par ses assurés d'un produit de la gamme Fitbit.

L'idée défendue par Julien Guez est que, dans les années qui viennent, « le rôle de l'assureur sera d'orienter les assurés dans l'offre de soins et de leur donner les moyens de devenir acteurs de leur propre santé, comme le fait déjà Malakoff Médéric ». Selon lui, les objets de santé connectés répondent à ce besoin car ils permettent à chacun de mieux connaître son état de santé en suivant l'évolution de sa tension, son poids, sa glycémie... Dans cette perspective, c'est une véritable « protection sociale co-active » qui pourrait émerger et qui reposerait sur une logique préventive plutôt que curative.

Pour Norbert Paquel, délégué général de Edisanté, le poids des complémentaires santé va être de plus en plus important : ils deviendront les financeurs des capteurs et autres objets connectés.

Pour pénétrer le marché, les nouveaux entrants ont dû développer une approche bien-être, dans laquelle les individus achètent directement en magasin les dispositifs d'automesure. Pour s'adapter aux changements dans les besoins des individus ou à l'obsolescence des dispositifs, Norbert Paquel estime qu'« un modèle basé sur la location de matériel par des opérateurs intermédiaires pourrait s'imposer. Cette location pourrait être supervisée par des assureurs ». Et si les assureurs sont effectivement amenés à jouer ce rôle, outre le fait qu'ils seraient « à l'origine d'une extension des usages », « il n'est pas exclu qu'ils jouent un rôle important » dans le contrôle des données issues de capteurs.



« PAY AS YOU WALK », L'ARRIVÉE DES LOGIQUES « USAGE » DANS LE MONDE DES ASSURANCES SANTÉ

S'appuyant sur le fait que les usages de monitoring du bien-être se développent chez les particuliers, les créateurs d'applications et de capteurs dédiés explorent de nouveaux partenariats. Aux États-Unis, ces créateurs de dispositifs de suivi du bien-être travaillent avec employeurs et assureurs afin de les intégrer dans les programmes de bien-être.

Ainsi, Fitbit promeut sa plateforme [Fitbit @ work](#) auprès des employeurs, et cherche à prouver l'existence d'une corrélation entre l'usage des dispositifs mobiles Fitbit et la fréquence de visites chez un médecin par un employé. Tout

l'intérêt pour l'entreprise serait de montrer que l'usage de dispositifs Fitbit chez les employés permettrait de réduire les coûts des soins médicaux, ce qui profiterait à la fois à l'employeur et à l'assureur, tout en favorisant, dans la logique de l'entreprise, le bien-être des employés. Aux États-Unis, Virgin HealthMiles, entreprise du groupe Virgin, a ainsi intégré Fitbit à son offre en ligne autour du bien-être destinée aux employés. Autre exemple, quelques mois après sa prise de fonction, Marissa Mayer la nouvelle dirigeante de Yahoo! a doté les 11 000 salariés de l'entreprise d'un bracelet Jawbone...

Le scénario dans lequel une assurance santé ou une mutuelle conditionnerait l'obtention d'un tarif avantageux à l'accomplissement d'un certain nombre d'activités physiques, chiffres à l'appui, se dessine. Dans les années à venir, les individus pourraient être priés d'apporter les preuves d'un comportement sain, sur le modèle de l'« *usage-based insurance* ». Ce modèle en vigueur dans le monde de l'assurance automobile - c'est le « *pay as you drive* » (« payez selon votre conduite ») - permet à l'assuré de payer (ou d'obtenir des avantages) en fonction des kilomètres qu'il a parcourus, mesurés à l'aide d'un logiciel de géolocalisation.

Une problématique soulevée par ces évolutions concerne le droit de regard des employeurs sur les données produites par leurs employés. Les offres actuelles prévoient de donner accès uniquement aux données agrégées concernant le taux d'équipement ou d'utilisation des dispositifs par ces derniers. Par ailleurs, on peut imaginer que les salariés pourraient être fortement incités à se doter de ces dispositifs, employeurs comme assureurs ayant tout intérêt à ce que les employés gèrent au mieux leur forme. Qu'en est-il de l'employé qui refuse de s'équiper ? Si l'on en croit Antoinette Rouvroy, un tel refus, face à l'accord des autres employés, pourrait être interprété comme un indice de « mauvais risque » par l'employeur ou l'assureur (cf. partie 03)... Et être source de discrimination ?

« CONDAMNER » L'INDIVIDU A ÊTRE RESPONSABLE DE SA SANTÉ

Dans une perspective plus large, c'est le fait même de vouloir reporter sur l'individu son maintien en bonne santé qui pose question. [Pour Evgeny Morozov](#) (interview de theguardian.com, 9 mars 2013), les pouvoirs publics trouveront toujours plus facile, plus économique et

plus moderne de s'appuyer sur les discours technophiles des sociétés qui développent des outils de *quantified self* pour traiter des problèmes de santé publique, plutôt que d'engager des réformes structurelles pour s'attaquer à leurs causes réelles.

Comme le rappelle Antoinette Rouvroy, cette situation est dépendante du contexte culturel. Les États-Unis et l'Europe sont construits sur des théories de la justice, différentes. En Europe, il y a l'idée que les individus n'ont pas à supporter seuls les désavantages relatifs qui sont dus à des causes sur lesquelles ils n'ont aucun contrôle, et c'est donc à la société d'assurer cette prise en charge. Aux États-Unis au contraire, la société n'a pas à compenser les désavantages individuels. Cédric Hutchings, PDG de Withings, dont les produits sont commercialisés à l'international, explique d'ailleurs que le développement des pratiques de *quantified self* est plus rapide aux États-Unis où les employeurs sont de véritables acteurs de la santé et ont un intérêt économique à améliorer la santé de leurs employés en encourageant ce type d'outils pour mieux négocier les contrats avec leurs mutuelles.

Or, pour Antoinette Rouvroy, « faire des individus des entrepreneurs d'eux-mêmes, y compris dans le domaine de la santé, risque peut-être de « détricoter » l'État Providence. En tenant les individus pour personnellement responsables de leur destin biologique (les personnes en mauvaise santé seraient rendues personnellement responsables de n'avoir pas été suffisamment entreprenantes dans la prévention), l'individualisation de la prévention pourrait tendre à délégitimer la prise en charge collective de la maladie et du handicap. »

Le rôle des pouvoirs publics est donc une question majeure, et encore peu abordée. Or, comme le fait remarquer Bernard Benhamou, si l'acteur public ne prend pas lui-même en charge ces évolutions, en intégrant davantage les développements en matière de e-santé / m-santé, ce seront des acteurs comme Apple et Google qui occuperont le terrain. C'est ce que laisse présager les informations disponibles relatives à l'iWatch, la montre connectée d'Apple qui devrait être commercialisée en 2014 et qui intégrerait une multitude de capteurs de santé. De plus, la prochaine version du système d'exploitation mobile d'Apple, iOS 8, devrait intégrer nativement une application dédiée à la santé - Healthbook - qui collecterait et organiserait les données de santé et de bien être de l'utilisateur issues d'applications tierces, des capteurs du téléphone, ou de l'iWatch. ■

Comment les marchés de la santé et de l'assurance pourraient-ils changer dans un futur proche dans l'hypothèse d'une croissance forte des outils de quantification et de la disponibilité de données « de santé » ? Pour imaginer des réponses à cette question, nous avons pastiché un article de presse économique évoquant les grandes et petites manœuvres d'acteurs existants ou imaginaires.

Quelques sources d'inspiration :

- Patrick Thourot et François Ewald, « Big Data, défis et opportunités pour les assureurs », Revue Banque & Stratégie n°315, juin 2013.
- Brian Womack and Trish Regan, « Google's Schmidt Says Data Can Change Insurance, Health Care », Bloomberg, 21 novembre 2013
- Guillaume Champeau, « La médecine personnalisée, ou la santé confiée à Google et Apple ? », Numerama, 20 février 2014.

LES GÉANTS DE L'ASSURANCE PEUVENT ILS ENCORE BATTRE LES GÉANTS DU CALCUL ?

Les entreprises technologiques sont elles en passe de se tailler la part du lion dans la valeur ajoutée de l'industrie de l'assurance ? Après avoir dévoré les marges des constructeurs automobiles et des groupes de l'immobilier et de la construction par l'ajout de services « intelligents » à leurs produits et services, la Silicon Valley et ses équivalents indiens et chinois sont en effet devenus des partenaires incontournables des assureurs. Tellement incontournables que l'équilibre des pouvoirs a peut-être déjà irrémédiablement basculé comme le montre les rumeurs autour d'acquisitions...

Les 5 dernières années ont bien sûr avant tout été marquées au plan économique par l'essor d'un important marché de la santé personnelle et de la médecine personnalisée. Alimenté à la fois par l'essor des capteurs et objets connectés reliés aux corps (le « *wearable computing* » qui a ajouté du « smart » à bas coût dans la plupart des objets du quotidien, du mobilier aux vêtements) et par la hausse permanente – et incontrôlable – des dépenses de santé dans les pays les plus riches (en particulier due au vieillissement de la population), ce marché est devenu l'un des plus rentables. Personnalisée, la médecine est surtout devenue plus prédictive. Le marché de la santé a été révolutionné

Fusions-acquisitions et modèles économiques dans le domaine des objets connectés de la santé et des assurances : où en est le marché ?

Les géants des technologies numériques se positionnent au cœur des chaînes de valeur de chaque domaine qu'ils abordent. Après l'automobile, la santé. Après la santé ?

en quelques années par les projets de génomique personnelle qui ont « révolutionné la notion même de gestion des risques de santé des individus » selon un responsable d'un grand cabinet international de conseil en stratégie, auteur d'un rapport sur « la génomique de nouvelle génération ». « Un génotypage efficace et porteur de résultats utilisables ne coûte aujourd'hui pas plus cher que nombre de tests médicaux, » ajoute-t-il, « et il permet d'enregistrer une quantité énorme de données sur les individus ». Les puissances de calcul disponibles ont en effet permis la création d'énormes bases de données contenant des millions de profils génétiques et des péta-octets de données, permettant aux chercheurs et à l'industrie pharmaceutique de découvrir des « signatures génétiques » nouvelles et de cibler les traitements. La biologie de synthèse et les algorithmes ont fait le reste... et cette omniprésente « data science » a permis à des géants comme IBM et Google ainsi qu'à plusieurs entreprises plus récentes et spécialisées de devenir des acteurs incontournables des marchés de la santé. Google a ainsi fêté l'année dernière ses 20 ans en annonçant que le domaine de la santé représentait maintenant une part significative de son chiffre d'affaires qui justifiait la réorganisation de l'entreprise autour de sa nouvelle branche « Life ».

Cette annonce était une nouvelle preuve du changement progressif de modèle économique de l'entreprise qui s'éloigne de plus en plus du modèle purement publicitaire initial pour être de plus en plus, comme l'affirmait récemment Larry Page, le CEO du géant de Mountain View lors d'une conférence au Brésil, «le moteur de l'économie d'analyse des données», installant toujours plus l'entreprise comme un partenaire aidant les autres entreprises à tirer partie des données disponibles pour «résoudre des problèmes du monde». Mais les industriels de l'automobile le savent: la guerre des «OS des voitures» de 2015 entre Microsoft, Google et Apple a essentiellement dévoré leurs marges, les obligeant de plus en plus à adapter leurs technologies à celle de ces fournisseurs omnipotents. Le monde de la santé, en croissance, a subi moins fortement cette tendance, mais les grands noms de la santé sont aujourd'hui des entreprises technologiques.

QUI SERA LE PROCHAIN SUR LA LISTE À SUBIR LES ASSAULTS DES SCIENTIFIQUES DES DONNÉES?

Il suffit de regarder en arrière pour le savoir: dès la fin de l'année 2013, le président exécutif de Google de l'époque (deux ans avant son départ de l'entreprise), Eric Schmidt, l'annonçait dans une conférence: «l'assurance est l'industrie qui est le plus évidemment à la veille de voir les usages du *big data* exploser». En réalité, aujourd'hui, l'assurance est plus simplement en train d'exploser en tant qu'industrie. Le *big data* et l'analyse de données, en particulier génétiques, ont totalement renversé les modèles classiques des assurances. Ses trois dernières années, les assureurs ont certes pu augmenter leurs profits de manière extrêmement rapide grâce à l'analyse de données: la médecine prédictive et les algorithmes ont permis aux assureurs de réduire les risques en devenant des experts de la prévention personnalisée. Les assureurs ont financé des programmes incitant les individus à s'équiper en capteurs et à adhérer à des programmes de génétique personnelle, et des milliers de vies ont pu être sauvées grâce à l'essor de ce qu'un responsable d'un grand groupe international d'assurance a appelé «des frappes préemptives contre les maladies». Les profits des grandes entreprises d'assurance ont crû fortement, car les assureurs sont rapidement devenus les seuls capables de maîtriser les coûts de santé. Mais cet âge d'or est aujourd'hui terminé car à force de se spécialiser dans la singularisation des risques, les assureurs ont fait disparaître l'essence même de leur métier: la mutualisation de risques incertains. Les pratiques discriminatoires des assureurs, qui ont développé des attaques par inférence pour trouver statistiquement leurs clients les plus «risqués» et les exclure n'ont fait que démontrer qu'en réalité, aujourd'hui, la réponse au problème de la gestion des risques n'est plus entre les mains des assureurs, mais de leurs fournisseurs de technologies. Ces mauvaises pratiques ont en outre provoqué des réactions politiques et médiatiques très fortes, comme certaines lois nationales, en Allemagne et en France, l'ont prouvé en répondant par des réglementations juridiques et éthiques draconiennes aux polémiques qui ont secoué les opinions publiques à propos des pratiques discriminatoires des assureurs. Drogées par l'idée de lutter contre les aléas moraux et l'asymétrie d'information, les grandes compagnies d'assurance font en fait aujourd'hui une overdose: donnant l'impression de pouvoir sélectionner parfaitement les risques par des algorithmes, les assureurs détruisent jour après jour la mutualisation qui les a fait naître. Et les «meilleurs» clients ont aujourd'hui un pouvoir de négociation qui leur permet de choisir d'être assuré «autrement» et à très bas prix.

L'analyse prédictive a ouvert un âge d'or de l'assurance, mais en détruisant à rythme accéléré ce qui fait l'essence même de cette industrie: la confiance et la mutualisation.

S'assurer autrement ? Le boom des *start-ups* assurantielles.

Depuis deux ans, de nombreuses *start-ups* se sont données comme objectif de renverser le marché des assurances par une approche de rupture. Suivant l'exemple de leurs prédécesseurs du financement participatif, des centaines d'entreprises se sont mises à inventer des modèles de segmentation et de mutualisation des risques aux antipodes des logiques assurantielles classiques, au grand dam des tenants de la science actuarielle, qui ont fait appel aux pouvoirs publics pour se protéger de ces nouveaux acteurs (parfois avec succès comme le montre la directive européenne de 2017 sur les services d'assurances). Peu d'entreprises nouvelles ont connu le succès, la plupart n'ont réussi qu'à lever des fonds pour ensuite pivoter sur des *business models* plus classiques, en particulier en devenant apporteurs d'affaires ou de technologies pour les assureurs classiques, voire en s'imposant comme des intermédiaires aux services des clients avec lesquels les acteurs classiques doivent compter. Mais depuis 2 ans les choses changent, et des géants du numérique font leur marché dans ce vivier de *start-ups*. Google a ainsi racheté 42 *start-ups* dans ce domaine, pour un montant total d'acquisition qui dépasse les 50 milliards de dollars. D'autres entreprises des technologies ont fait de même, tout en continuant à investir massivement dans les bases de données génétiques et les technologies d'algorithmes et de *machine learning*. Aujourd'hui, tous les éléments semblent en place pour que les géants du numérique deviennent les fossoyeurs de l'industrie traditionnelle de l'assurance. En 2020, à la question «qui est votre assureur?» vous répondrez peut-être «personne, Google s'en occupe».

LE PROJET TRANSHUMANISTE : L'HOMME CAPTÉ, AUGMENTÉ, ... IDÉAL ?

“ La démocratisation du « bricolage du vivant » devrait débuter en 2015. À partir de cette date, nous pourrions commencer à augmenter nos capacités, à remplacer nos pièces défectueuses par des implants ou par des prothèses, à nous greffer des électrodes dans le corps, à modifier notre ADN... Bref, ce sera le début de l'ère de l'amélioration. ”

Laurent Alexandre,

PDG de DNAVision. Co-fondateur de Doctissimo

DE « L'HOMME RÉPARÉ » À « L'HOMME AMÉLIORÉ »

Il n'a pas été nécessaire d'attendre la multiplication des prothèses médicales et l'apparition de la bio-ingénierie pour que la technologie pénètre le vivant. La « médecine d'amélioration » existe depuis longtemps, au moins depuis l'invention des lunettes et elle compte parmi les causes de l'accroissement continu de l'espérance de vie.

Mais aujourd'hui, l'apport de la technologie dans le domaine médical va beaucoup plus loin et certains ne veulent lui fixer aucune limite. C'est ce qui caractérise le transhumanisme, un courant de pensée qui s'est cristallisé en Californie dans les années 80 et qui s'est fixé pour objectif la transformation radicale de l'être humain grâce à la fusion progressive de la technologie et de la vie. Pour ses adeptes, les progrès scientifiques permettront à l'homme non seulement de s'améliorer, d'augmenter ses capacités, de s'affranchir des limites du corps et de la biologie, mais aussi d'accéder à de nouveaux sens, voire à un niveau de conscience supérieur. Il s'agit de passer de « l'Homme réparé » à « l'Homme amélioré » ou « augmenté » et, peut-être un jour, à un Homme immortel. Cette

conception conduit à faire de l'être humain « un être en perpétuelle évolution ».

C'est ainsi que la technologie essaie parfois de créer une vie artificielle en « bricolant le génome », comme lorsque le chercheur et homme d'affaires Craig Venter fabrique en éprouvette, en mai 2010, le premier chromosome artificiel, avant de l'introduire dans une bactérie. À d'autres moments, la technologie cherche même à surclasser la biologie grâce au développement de l'intelligence artificielle et de l'apprentissage automatique (« *machine learning* »).

Le moteur de recherche Google relève fondamentalement de cette approche. Il n'y a pas lieu d'en être surpris, s'agissant d'une entreprise qui est fortement marquée par l'idéologie transhumaniste. D'après Laurent Alexandre, les dirigeants de Google comprennent l'Homme comme « la version Beta des post-humains ».

TRANSHUMANISME ET QUANTIFIED SELF

On retrouve une partie de la même philosophie transhumaniste dans le mouvement *Quantified Self*. Si les pratiques visent d'abord une meilleure « connaissance de soi », on bascule, en effet, assez aisément dans une logique d'augmentation, d'amélioration de l'Homme. Les outils de « quantification » visent à mettre en chiffres le maximum d'informations relatives au corps humain, que celles-ci se rapportent à des performances physiques, à des comportements, à des émotions, ou même à la capacité de compréhension de l'homme.

Sans doute, les capteurs restent-ils, à l'heure actuelle, disposés à l'extérieur du corps. Mais rien n'indique qu'il en sera de même demain. D'ailleurs, les objets connectés ne sont, en réalité, rien d'autre que de nouveaux yeux et de nouvelles oreilles ou, *a minima*, des extensions des sens et des organes, tandis que les données collectées sont perçues comme de nouvelles sources de connaissance. Quant aux conditions de leur exploitation, elles reposeront surtout sur de l'intelligence artificielle.

En fait, le monde est déjà engagé dans une logique transhumaniste sans que nous nous en soyons rendus compte. À terme, bien des choses devraient être possibles : se faire greffer un cœur artificiel, composé de matériaux plastiques et biologiques pour prolonger l'espérance de vie ; troquer ses jambes pour d'autres, artificielles mais beaucoup plus rapides ; se faire implanter



RAY KURZWEIL, GOOGLE ET LE POST-HUMANISME

Ray Kurzweil, peu connu en Europe, l'est beaucoup plus aux États-Unis. Informaticien de talent, il est l'inventeur de plusieurs technologies, par exemple d'analyses automatiques de caractères ou de la voix. Il est surtout célèbre aux États-Unis comme « futurologue » et pour ses idées transhumanistes, mouvement dont il est devenu l'une des figures de proue, que ce soit au travers de nombreuses interventions publiques ou de ses best-sellers autour de l'allongement de la vie et du futur de l'intelligence artificielle, des nanotechnologies, de la robotique et des biotechnologies. Il est en particulier connu pour deux ouvrages : « *The Age of Spiritual Machines* » (2000) et « *The Singularity is Near* » (2005). Ray Kurzweil pense que la Singularité, c'est-à-dire le moment où l'augmentation exponentielle de la puissance de calcul des ordinateurs fera émerger une intelligence supérieure à l'intelligence humaine, aura lieu avant la moitié du XXI^{ème} siècle. En décembre 2012, Ray Kurzweil a

rejoint Google en tant que « director of engineering » avec une mission définie avec Larry Page, PDG et co-fondateur de l'entreprise : faire avancer la capacité de Google à comprendre le langage naturel et les mécanismes du cerveau, de l'apprentissage. Ray Kurzweil rejoint Google parce qu'il s'agit de l'une des organisations les mieux dotées dans le monde pour atteindre ses objectifs en terme de « machine learning » et d'intelligence artificielle. Pour autant, il serait très excessif de dire que le fait pour Google d'embaucher Ray Kurzweil implique d'adhérer à son « agenda transhumaniste ». Il est cependant intéressant de relever, comme le fait Laurent Alexandre, certaines proximités par exemple dans la lutte contre la maladie et le vieillissement, ou bien dans le contenu de l'ouvrage signé d'Eric Schmidt, président du Conseil d'administration de Google et de Jared Cohen, directeur du *think tank* « *Google ideas* » : « À nous d'écrire l'avenir » (titre original *The New Digital Age*, 2013).

des yeux bioniques pour voir les infrarouges ou dans le noir, ou pour filmer ce qu'ils voient ; augmenter son intelligence grâce à des interfaces cerveau-machine et aux neurosciences ; télécharger son esprit ou sa mémoire dans un avatar...

Mais au-delà de cela, le projet transhumaniste est politiquement beaucoup plus ambigu : il faut « tuer la mort » pour paraphraser le titre d'un livre de Laurent Alexandre (« *La mort de la mort* », 2011), c'est-à-dire offrir aux humains l'immortalité. Google a d'ailleurs créé en septembre 2013 une filiale, baptisée Calico, qui doit s'attaquer au défi de l'âge et des maladies associées, ce qui poussa le magazine *Time* à se demander, à la une, si Google peut « résoudre la mort » (Septembre 2013).

DES IDÉES QUI ESSAIMENT

Les partisans du transhumanisme, appelés aussi « bio-progressistes », sont peu présents en Europe (à l'exception notable de l'[Institut pour le Futur de l'Humanité](#) de l'université d'Oxford et de son directeur depuis 2005, Nick Bostrom), mais particulièrement puissants autour du Pacifique (Californie, Chine, Corée du Sud...). En Californie, ces idées ne sont pas perçues comme farfelues : de grands chercheurs s'impliquent par exemple dans les travaux de l'[Université de la Singularité](#), institut créé en référence à l'expression popularisée par Ray Kurzweil (voir encadré), pour lequel la singularité sera le seuil au-delà duquel l'intelligence artificielle aura surpassé l'intelligence humaine. La NASA est par exemple un contributeur important de cette université d'un genre unique. Pour ces personnes, la vie s'apparente à une « nanomachine particulièrement sophistiquée », mais aussi largement manipulable. C'est pourquoi certaines d'entre elles essaient d'ores et déjà de modéliser l'intelligence de l'être humain, son autonomie, sa mémoire, le désir, la douleur, le rêve ou la conscience... Tous ces travaux visent à faire disparaître, à terme, toute opposition entre le naturel et l'artificiel, le vivant et le non-vivant, le conscient et son contraire.

La revendication d'égalité, qui s'appuie sur la logique de « normativité perfectionniste » propre au *quantified self* (cf. avant-propos d'Antoinette Rouvroy), est un puissant vecteur de justification de ces transgressions biotechnologiques. La « démocratie radicale » des transhumanistes suppose, en effet, de permettre à chacun de se libérer, grâce à la technologie, de la tyrannie ...

- du destin, de la nature (« les incertitudes de la sélection darwinienne », la maladie et le vieillissement) et de sa condition sociale.

LA « RÉVOLUTION NBIC »

Pour cela, les transhumanistes s'appuient sur ce que l'on a pris l'habitude d'appeler la « révolution NBIC », qui est le fruit de la convergence des Nanotechnologies, de la Biologie - en particulier de la génétique -, de l'Informatique et des sciences Cognitives - c'est-à-dire de l'intelligence artificielle et des sciences du cerveau. Les découvertes réalisées dans l'un de ces domaines servent à la recherche dans les autres. Ces quatre disciplines ont été pour la première fois liées entre elles en 2002 dans un vaste programme scientifique doté par le gouvernement des États-Unis de plusieurs milliards de dollars.

C'est ainsi que l'association des nanotechnologies et de la biologie devrait permettre de réparer des organes du corps humain ; que l'augmentation exponentielle des vitesses de calcul informatique et l'intelligence artificielle pourraient conduire à la création de robots

plus intelligents que les humains ; que l'association des sciences cognitives à la génétique, aux biotechnologies et aux nanotechnologies vise à mieux comprendre le cerveau, à en développer les capacités, puis à bâtir de nouvelles formes d'intelligence artificielle et de « *machine learning* ».

En elles-mêmes, les nanotechnologies tiennent déjà leur dimension révolutionnaire de leur capacité à manipuler le vivant. Peu de choses, en effet, distingue une molécule vivante d'une molécule chimique. Le « bricolage du vivant » devrait donc avoir tendance à se banaliser comme le montre le succès de « [La paillasse](#) », « laboratoire communautaire pour les biotechnologies citoyennes » en région parisienne, qui a le soutien de la mairie de Paris. Rien n'interdit ainsi de penser que, demain, des nanorobots seront en mesure de circuler dans le corps humain, d'établir des diagnostics et d'agir en présence d'un problème physique. On peut imaginer que se développent, d'ici une dizaine d'années, la transformation du corps grâce à des composantes électroniques, les thérapies et ingénieries cellulaires et tissulaires, grâce notamment à la réécriture du génome, ainsi qu'une nano-médecine préventive personnalisée (cf. partie 01).

Le passage de ces technologies dans la médecine collective ne devrait être qu'une question de quelques décennies. Les maladies les plus graves seront sans doute les premières à être traitées grâce à la reprogrammation génétique. Mais certains transhumanistes ont souhaité prendre de l'avance. Les « *body hackers* » essaient depuis des années de « s'améliorer » eux-mêmes, en modifiant leur corps pour en augmenter les capacités, ou développer de nouveaux sens. L'un des plus connus, le professeur de cybernétique Kevin Warwick, se voit comme le premier « *cyborg* » de l'histoire depuis qu'il s'est greffé des puces dans le corps et que des électrodes, placées dans un bras, sont reliées à son système nerveux et à un ordinateur. Il peut ainsi commander par la pensée un ordinateur ou une main robotisée. De son côté, Amal Graafstra, auteur du livre *RFID Toys* (2006), s'est fait implanter une puce RFID dans chaque main pour démarrer sa moto, ouvrir son coffre-fort ou s'authentifier plus facilement lorsqu'il rentre chez lui. Une autre « *body hacker* » s'est fait greffer une caméra à l'arrière





du crâne pour filmer tout ce qui se passait derrière elle. Les transhumanistes rêvent ainsi que *l'human enhancement* de demain, c'est-à-dire l'homme augmenté ou amélioré, puisse bénéficier d'une amélioration de ses caractéristiques physiques (vitesse, résistance...), de ses capacités cognitives (mémoire, capacités de calcul...), de sa vie affective (émotions, motivation...), de sa résistance aux maladies ou, bien sûr, d'une durée de vie plus longue... La course à la création d'hybrides semble ainsi être lancée. Après l'homme-machine, pourquoi pas un homme-animal ?

TRANSHUMANISME OU POSTHUMANISME ?

En réalité, ne serait-il pas préférable de parler de posthumanisme ? La plupart des opposants à ce courant de pensée (certains parlent de « bio-conservateurs ! »), tel le professeur de philosophie des technologies

d'information et de communication Jean-Michel Besnier, déplorent qu'il n'engage aucune réflexion existentialiste sur la nature de l'humanité : « Ce que veut le transhumanisme, ce n'est pas parfaire l'humanité, mais nous arracher à l'humanité. Faire de nous des êtres qui ne naîtront plus mais qui seront fabriqués, lisser la vie psychique, ne plus vieillir grâce au téléchargement de la conscience, éradiquer la souffrance et donc le plaisir. Le désir même, alors que c'est le moteur de l'humanité... Arrêtons de dire que c'est au service de l'humanité, alors que ce n'est que pour la détruire ».

D'autres critiques, à l'image de Marc Roux, le président de l'association transhumaniste française « Technoprog ! », mettent l'accent sur les risques sociaux et démocratiques attachés à certaines formes de transhumanisme. Ils craignent la naissance d'une humanité à deux vitesses : « L'un des risques, c'est qu'une oligarchie s'accapare cette technologie et que nous tombions dans une sorte de dictature ». ■

0.3



Partie 0.3

QUELS AXES DE RÉGULATION ? LES VOIES À EXPLORER

QUELLE RÉGULATION POUR LA « SANTÉ MOBILE » ? À L'ÉCOLE DES EXEMPLES ÉTRANGERS...	44
POUR UN <i>HABEAS CORPUS</i> DE L'HOMME CAPTÉ	52
SCÉNARIO PROSPECTIF : "2022, LE SOMMET DES HUMAINS DE RIO"	58

QUELLE RÉGULATION POUR LA « SANTÉ MOBILE » ? À L'ÉCOLE DES EXEMPLES ÉTRANGERS...

“ Peu d'autorités ont développé une stratégie précise quant à l'approche de la question des objets et applications liés au bien-être des personnes. La question du *quantified self* est ainsi très peu traitée de manière expresse dans la législation.

La difficulté principale identifiée concerne le champ de la définition de la notion de donnée de santé. La notion de donnée de santé n'étant, dans l'ensemble que peu définie par les autorités, l'interprétation qui en a été faite a généralement été large et inclusive sans être, pour autant, claire. De ce fait, la notion est souvent définie de manière empirique, selon les circonstances du traitement et le type d'informations concernées. Les outils et applications de *quantified self* utilisant ou aidant à la création de données – pour certaines nouvelles – à la frontière de la santé au sens strict du terme et d'une notion générale de bien-être, conduisent à s'interroger concrètement sur le caractère approprié de l'application du régime contraignant applicable aux données de santé pour ces données. (...)

L'analyse a également révélé l'existence d'un nombre assez significatif d'initiatives publiques ou privées relatives au contrôle des applications de santé – y compris en France. La multiplicité des efforts dans ce secteur et l'absence de standard commun dans ce cadre semble pour l'heure limiter l'efficacité et l'impact de ces outils. ”

Hogan Lovells (Paris) LLP,

Étude benchmark sur les réglementations concernant l'utilisation dans le domaine de la santé et du bien-être des capteurs, smartphones et autres objets connectés (décembre 2013)

Les objets connectés et les applications mobiles dédiés au bien-être et à la santé font-ils l'objet de réglementations spécifiques, tant au niveau national qu'international ? Et, lorsque c'est le cas, quel en est le contenu, notamment en matière de protection des données personnelles ?

Pour répondre à ces questions, une étude *benchmark* internationale a été conduite à la demande de la CNIL par le cabinet d'avocats Hogan Lovells, pour identifier les pays qui ont déjà mis en place une réglementation spécifique, sont en train de le faire, ou ont mis à jour leur réglementation en ce domaine (ex. : sur les dispositifs médicaux). L'étude devait également décrire et analyser les différentes composantes de cette réglementation (ex. : les procédures de déclaration, d'agrément ou de classification applicables selon le niveau de risque de l'application ; les modalités de contrôle des fabricants, des dispositifs techniques et des plateformes ; les normes de sécurité et de qualité applicables ; les régimes de responsabilité ; les systèmes d'intermédiation, obligatoire ou non, d'un professionnel de santé ; les exigences en matière de notice d'information...), en mettant l'accent sur les règles de protection et de sécurisation des données personnelles et sur les droits des personnes.

Il ressort de cette étude menée en Europe, aux États-Unis d'Amérique ainsi que dans certains pays (Corée du Sud, Russie, etc.), que la santé mobile (ou *m-santé*) ne fait encore l'objet d'aucune loi spécifique. En revanche, plusieurs lois relatives à la e-santé, qui traitent donc de tous les aspects numériques touchant de près ou de loin à la santé, abordent les questions de réglementation des applications de santé mobiles et de protection des données personnelles de *m-santé*. Dans certains pays, ces questions sont indirectement réglementées par des lois qui régissent l'activité des professionnels de santé, dans d'autres, par une loi à caractère général qui définit les règles de base de la protection des données personnelles, toutes catégories de données confondues. Ce chapitre donne un aperçu de ces divers modes de réglementation, en prenant quelques exemples parmi les plus significatifs.



LES ÉTATS-UNIS D'AMÉRIQUE, PIONNIERS D'UN NOUVEAU TYPE DE RÉGULATION

Depuis 1996, les États-Unis disposent d'une loi fédérale (dite HIPAA) sur le traitement des données de santé dans le secteur médical, qui correspond à leur approche sectorielle habituelle de la protection des données personnelles. Ses dispositions devraient s'appliquer à certaines des applications de santé mobiles. Son champ d'application inclut, en effet, l'ensemble des informations qui ont trait à l'état de santé présent, passé ou à venir de la personne et aux soins correspondants, du moins lorsque ces données sont traitées par un hôpital, une clinique... ou une société d'assurance.

Cependant, d'autres acteurs peuvent être soumis à cette législation, tels que les partenaires d'affaires des établissements de santé, lorsque les fonctions ou services qui leur sont confiés impliquent qu'ils recourent à des données médicales, ou même qu'ils y aient simplement accès. Il peut s'agir d'associés dans le cadre d'un programme de santé, de services de transmission de données médicales, d'experts-comptables, de consultants, d'avocats... ou de fournisseurs de technologie de santé mobile.

Dans tous les cas, il appartient à l'établissement de santé de s'assurer par contrat que les utilisations et transferts de données de santé effectués par ses partenaires seront conformes à ses propres règles de « *privacy* ».

Cette loi oblige les établissements de santé à informer leurs patients sur les conditions dans lesquelles ils utilisent et protègent les données personnelles en leur possession (sur les finalités envisagées, les transferts prévus à des tiers, les modalités d'exercice des droits individuels...).

La même loi interdit la divulgation et, *a fortiori*, la vente de données personnelles de santé en l'absence d'une autorisation du patient concerné. Plus généralement, les transferts de données médicales qui ne résultent pas d'une obligation légale nécessitent l'autorisation écrite préalable des intéressés. Ces conditions de réutilisation des données de santé ne sont assouplies que pour quelques finalités bien précises, telles que la levée de fonds auprès des patients de l'établissement de santé ou la recherche médicale.

Les responsables de traitement sont tenus de mettre en œuvre des mesures appropriées - mais raisonnables - pour protéger les données médicales contre tout usage non autorisé. La loi prévoit aussi l'établissement de standards de sécurité pour le traitement des données de santé ...

- et impose aux acteurs d'informer sur les failles de sécurité découvertes dans leurs systèmes informatiques, tant le département fédéral de la santé (*Department of Health and Human Services*) que les personnes concernées et les médias, du moins lorsque ces failles concernent plus de 500 personnes. Ces prescriptions devraient s'appliquer aux fournisseurs de technologies mobiles utilisées dans le secteur médical.

Aucune sanction n'est encourue si la violation de l'une de ces règles n'est pas le résultat d'une négligence répétée, sous réserve

de sa correction dans les 30 jours suivant sa découverte. Dans le cas contraire, la sanction encourue, qui peut être autant civile que pénale, peut atteindre 250 000 dollars et 10 ans d'emprisonnement. Elle est alourdie en cas de vente ou d'utilisation commerciale de données médicales.

Les États-Unis ont également mis en place une régulation des dispositifs médicaux qui est confiée à l'agence fédérale de contrôle des produits alimentaires et des médicaments (*Food and Drug Administration - FDA*). Ceux-ci y sont définis comme tout objet ou logiciel dont l'usage prévu est soit le diagnostic d'une maladie ou d'un état de santé, soit le traitement, la guérison ou la prévention d'une maladie. Un objet ou logiciel entre également dans le champ d'application de la loi dès lors qu'il est destiné à influencer sur la structure ou sur une fonction du corps humain. Cette définition reste étroitement liée à l'activité des professionnels de santé. Il en résulte que toute application mobile susceptible de remplacer un acte de diagnostic ou d'influer sur le choix d'un traitement sera considérée comme un dispositif médical.

C'est dans ce contexte que la FDA a élaboré, en juillet 2011, un premier projet de recommandations relatives aux applications médicales mobiles, qui lui a donné l'occasion de préciser les conditions dans lesquelles elle exercerait ses pouvoirs de contrôle et d'autorisation. La FDA y envisageait, dès l'origine, de centrer son attention sur les applications qui constituent l'accessoire d'un dispositif médical ou qui transforment un terminal mobile en un dispositif médical. Ce premier projet de recommandation de la FDA en matière d'applications mobiles a fait l'objet de vifs débats jusqu'au Congrès, certains redoutant la mise en place d'une réglementation trop lourde et de procédures administratives trop lentes. Au total, le dispositif mis en place n'a qu'un caractère temporaire, dans l'attente de la création d'un régime spécifique et peut-être d'une direction dédiée disposant de moyens propres au sein de la FDA. C'est en septembre 2013 que la FDA a émis les lignes directrices de sa régulation des applications mobiles. Sa compétence se limite aux applications mobiles qui sont considérées comme des dispositifs médicaux au regard de

LA FDA ET LE KIT DE GÉNOMIE PERSONNELLE 23ANDME

La FDA a demandé, le 22 novembre 2013, à la société de génomique personnelle *23andMe* de cesser la commercialisation de son kit, pour infraction à la législation sur les dispositifs médicaux.

La société *23andMe*, dont Google est actionnaire depuis 2007, propose sur internet depuis fin 2012 un kit grand public d'analyse du code génétique pour 99 dollars. L'utilisateur est invité, pour recevoir diverses informations, à retourner un échantillon de salive au moyen du kit qui lui est fourni.

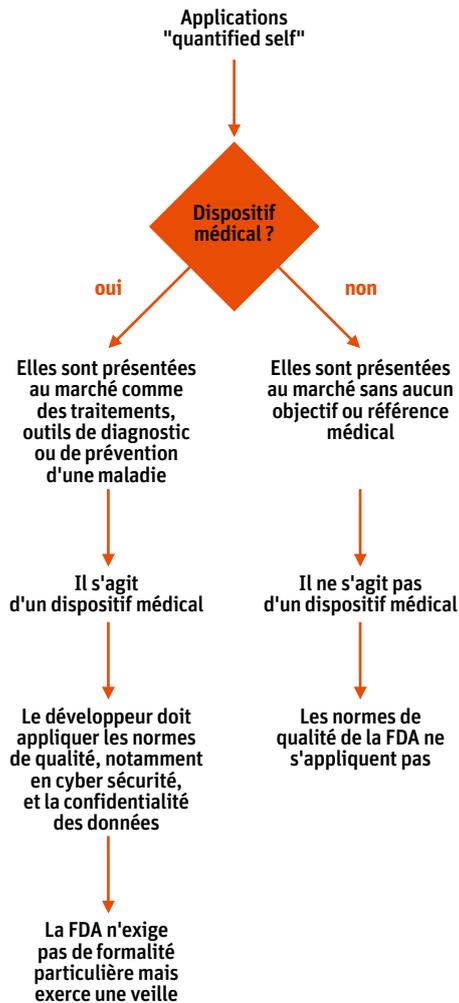
Dans un premier temps, le kit a été présenté comme le moyen d'obtenir des renseignements sur l'origine de ses ancêtres. Puis, à partir de 2009, l'offre a été recentrée autour de la santé de l'utilisateur, l'entreprise lançant même une grande campagne de publicité axée sur la santé. Les informations communiquées, sensées être liées au patrimoine génétique de l'utilisateur, ont alors changé de nature : elles ont été présentées comme pouvant révéler une prédisposition à développer certaines pathologies et la réactivité de l'organisme face à certains médicaments.

Après plusieurs mois d'échanges avec la société, la FDA a décidé de stopper la commercialisation du kit, en l'absence d'informations suffisantes sur la fiabilité des diagnostics et conseils de prévention donnés aux usagers. En effet, les résultats transmis pouvaient leur faire courir de sérieux risques en cas de mauvaise interprétation. Par ailleurs, si le kit relevait de la législation sur les dispositifs médicaux, c'est parce qu'il était présenté comme un système d'aide au diagnostic. La FDA en conclut qu'il pouvait être compris comme se substituant au diagnostic d'un médecin. Il aurait donc dû faire l'objet d'une autorisation de l'agence avant sa commercialisation.

Depuis fin 2013, le site *23andme* affiche un bandeau indiquant que le kit permet d'obtenir un rapport sur l'origine de ses ancêtres ou des données brutes, mais qu'il ne permet pas d'accéder à des données de santé. Dans une [interview au Guardian](#) en mars 2014, Anne Wojcicki, co-fondatrice du site, a reconnu que l'intervention de la FDA avait significativement ralenti la diffusion du kit.

À cette date, elle revendiquait 650 000 clients... ce qui en fait, selon elle, la plus grande base de données de ce type dans le monde.

GRILLE D'ANALYSE DES APPLICATIONS DE QUANTIFIED SELF UTILISÉE PAR LA FDA
(source : Hogan Lovells)



la loi. Par ailleurs elle distingue les applications de m-santé qui sont « certainement » des dispositifs médicaux de celles qui ne le sont que « peut-être ». La FDA explique ne pas avoir l'intention d'appliquer de manière stricte la loi à la seconde catégorie, qui recouvre surtout les applications mobiles de bien-être (ex. : les podomètres, les moniteurs de fréquence cardiaque).

Sont ainsi exclues du champ de contrôle de la FDA les applications mobiles dont la finalité est de permettre aux particuliers d'enregistrer, suivre, évaluer ou prendre des décisions individuelles, ou encore celles qui formulent des suggestions relatives au développement ou à l'entretien de la santé ou du bien-être général de leur utilisateur (ex. : pour respecter un régime diététique, encourager le recours à un mode de

vie plus sain, suivre ses habitudes de sommeil, tester « l'âge du cerveau »).

Sans doute, ces applications mobiles pourront-elles, après analyse, relever de la compétence de la FDA si on peut les considérer comme des dispositifs médicaux, en particulier si elles sont présentées au public comme devant être utilisées pour le diagnostic, la prévention, le traitement ou la guérison d'une maladie (voir encadré *infra*. le cas particulier de *23andMe*). Cependant, même dans cette hypothèse, la FDA ne compte pas exiger de leurs développeurs qu'ils respectent les procédures de dépôt ou d'agrément établies par la loi. L'agence se contentera à leur égard d'assurer une veille et de se réserver le droit d'intervenir en cas de détection d'un risque avéré.

De même, les normes de qualité définies par la FDA ne s'imposeront-elles aux applications mobiles de bien-être que lorsque l'agence en aura décidé ainsi par une mesure individuelle. Ce principe vaut notamment pour les recommandations publiées en juin 2013 en matière de cyber-sécurité et de protection de la confidentialité et de la sécurité des données, qui doivent, en revanche, être prises en compte dès la conception des applications de m-santé qui s'apparentent le plus à des équipements médicaux professionnels (ex. : mise en œuvre de mesures d'authentification, déconnexion automatique, renforcement des mots de passe, mise en œuvre de mesures d'auto-blocage et de récupération des informations), (voir schéma ci-contre).

Une troisième législation est à prendre en compte : L'agence fédérale du commerce (*Federal Trade Commission* - FTC), qui est chargée de proscrire tout acte commercial déloyal, est en effet compétente pour intervenir en cas de collecte et/ou d'utilisation déloyales de données personnelles, c'est-à-dire en l'absence d'un objectif légitime et d'un consentement de l'utilisateur concerné. C'est ainsi qu'elle a sanctionné l'éditeur d'une application mobile qui prétendait que la lumière du téléphone pouvait guérir de l'acné.

En 2013, la FTC a publié des lignes directrices relatives à la protection des données personnelles dans le contexte des applications mobiles. Elle y encourage notamment les plateformes de distribution de contenus à augmenter

- leur vigilance à l'égard des applications qu'elles diffusent, à développer les mesures de transparence et d'information du consommateur, par exemple en intégrant un système de notification lorsqu'une application commence à collecter certaines informations telles que la géolocalisation, ainsi qu'à être plus exigeantes en matière de protection des données personnelles dans leurs contrats avec les développeurs d'applications mobiles.

La FTC recommande aux développeurs d'applications mobiles d'obtenir le consentement explicite de l'utilisateur en cas de collecte

L'EXEMPLE DE LA PLATEFORME HAPPTIQUE

La plateforme *Happtique* a été créée par l'Association des Hôpitaux de la Région de New York. Cette plateforme a vocation à délivrer des labels pour toute application de santé qui se conforme aux normes *Happtique*. Celles-ci comportent quatre types de standards : des normes d'opérabilité, des normes de protection de données personnelles, des normes de sécurité et des normes relatives aux contenus.

Elles s'appuient en partie sur des normes existantes (ex. : des normes applicables à des dispositifs médicaux). Les normes en matière de protection des données personnelles se divisent en six catégories, selon la nature de l'information donnée à l'utilisateur lors de la collecte des données : sur les types de données collectées par l'application, sur les modalités du traitement et l'identité de son responsable, sur le consentement explicite de l'utilisateur avant toute collecte de données de santé ou de géolocalisation, sur l'interdiction du partage de données avec un tiers sans un accord qui en garantit la sécurité et la confidentialité (Standard P1) ; sur la durée de conservation des données (Standard P2) ; sur l'accès de l'application à d'autres données présentes dans le Smartphone (ex. : données GPS, liste des contacts, photos, SMS) ou sur des réseaux sociaux, ainsi que sur sa raison d'être et ses modalités (Standard P3). Le Standard P4 exige la mise en œuvre de toutes les obligations de la loi HIPAA, le Standard P5, la limitation de la collecte de données relatives aux enfants, le Standard P6 le recours systématique au consentement de l'utilisateur et la notification aux usagers de tout changement dans la politique de protection des données personnelles.

Il apparaît cependant que seule une vingtaine d'applications sont aujourd'hui certifiées sur cette plateforme et que ce dispositif de labellisation n'a pas rencontré le succès escompté. Il se recentre d'ailleurs sur des applications purement hospitalières...

de données de santé, sur la base d'une information succincte présentée lors de la collecte des données. Enfin, elle a prévu d'organiser en 2014 [un séminaire dédié aux applications mobiles de santé](#) pour aborder les problèmes qui leur sont spécifiques.

L'agence nationale des télécommunications et de l'information (*National Telecommunications and Information Agency - NTIA*) intervient également en matière d'applications mobiles depuis qu'elle a lancé, sous l'impulsion de la Maison Blanche, une [plateforme de co-régulation](#) qui fait intervenir les agences gouvernementales, les principaux acteurs économiques du secteur, ainsi que les représentants de la société civile et des droits civiques. L'objectif est de développer des codes de conduite. Toute entreprise signataire sera tenue d'en respecter les engagements, leur violation pouvant être sanctionnée par la FTC.

Un premier projet de code de conduite, publié en juillet 2013 et encore en phase de test, porte sur l'information des usagers des applications mobiles. Ses souscripteurs doivent publier une notice d'information sur leur pratique en matière de protection des données personnelles. Des labels simplifiés doivent être utilisés pour informer les consommateurs sur les catégories de données traitées et leurs destinataires.

Enfin, il convient de mentionner les initiatives d'autorégulation prises par plusieurs hôpitaux et facultés de médecine pour guider les patients et les médecins parmi les applications médicales en en proposant une classification sur la base de grilles d'évaluation et de référentiels établis par des experts (voir encadré *infra*, sur Happtique).

DES RÉFLEXIONS EN COURS EN EUROPE

Les lois générales de protection des données personnelles des pays de l'Union Européenne (UE), issues de la directive 95/46/CE, classent les données de santé parmi les données les plus sensibles. Leur traitement est interdit, sauf dans des cas précisément définis (ex. : suivi médical ; santé publique ; le consentement de l'intéressé ; lorsque la protection de la vie l'exige ; si les données ont déjà été

rendues publiques...). Les transferts de données personnelles de santé hors de l'UE peuvent être interdits, à moins que la législation de l'État de destination ne leur organise un niveau de protection adéquat.

Le Groupe européen des autorités de protection des données – groupe dit de l'Article 29 (G29) - a précisé en 2007 ce que recouvrait la notion de « donnée de santé » : les informations qui 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.

Par ailleurs, le Conseil des ministres des télécoms de l'UE a affirmé en 2008 la nécessité de reconnaître un « droit au silence des puces » RFID. On parle aujourd'hui plutôt d'un "droit au contrôle" des puces. Ce droit, au-delà de la problématique générale des objets connectés, pourrait très utilement s'appliquer aux appareils de *quantified self*, et garantir à leurs usagers la maîtrise de la diffusion des données personnelles produites par ces outils et autres applications mobiles. Ceci supposerait que leurs utilisateurs puissent à tout moment désactiver la fonctionnalité permettant la communication des données, en application de leur droit d'opposition.

La Convention européenne des droits de l'homme protège par ailleurs le droit au respect de la vie privée et familiale, ainsi que la confidentialité des données de santé. La plupart des États de l'UE se réfèrent également à la déclaration de 1994 de l'Organisation mondiale de la santé (OMS) sur la promotion des droits des patients, qui met l'accent sur le droit à l'autodétermination de chacun et sur le droit au respect de sa vie privée. Bien évidemment, ces principes n'excluent pas l'existence d'exceptions (ex. : pour les maladies transmissibles à déclaration obligatoire).

L'UE dispose également d'une législation sur les dispositifs médicaux, dont la finalité est de s'assurer que ces produits offrent aux patients, aux autres utilisateurs et aux tiers un niveau de protection élevé et qu'ils atteignent les objectifs que leur a assignés le fabricant. Chacun de ces produits se doit d'être conforme à des « exigences essentielles » en matière de sécurité, de performance et de réduction des risques sanitaires qui sont définies par la directive qui lui est applicable selon sa nature

(cf. les directives 90/385/CEE sur les dispositifs médicaux implantables actifs, 93/42/CEE sur les dispositifs médicaux et 98/79/CE sur les dispositifs médicaux de diagnostic *in vitro*, qui sont actuellement en cours de révision). À cette fin, les fabricants peuvent se référer à des « normes harmonisées », officielles, dont l'application n'est jamais obligatoire.

Cette législation met également en place des procédures d'évaluation de la conformité des dispositifs médicaux. Pour ceux qui ne présentent qu'un faible risque, le fabricant peut évaluer lui-même son produit à partir des « exigences essentielles » officielles, puis adresser une « déclaration écrite de conformité » avant d'apposer le marquage CE sur son dispositif médical. Lorsque le risque encouru est plus fort, la procédure d'évaluation de la conformité doit faire intervenir un « organisme notifié » qui est chargé de délivrer des « certificats de conformité ». Les autorités officielles se limitent au contrôle et à la surveillance du marché.

Cette législation concerne notamment les applications de santé mobiles et autres objets connectés dès lors que constitue un dispositif médical tout appareil, équipement ou logiciel destiné par le fabricant à être utilisé chez l'homme à des fins :

- de diagnostic, prévention, contrôle, traitement ou atténuation d'une maladie, d'une blessure ou d'un handicap ;
- d'étude, remplacement ou modification de l'anatomie ou d'un processus physiologique ;
- de maîtrise de la conception ;

et dont l'action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens. Il en va ainsi des logiciels autonomes qui ne se limitent pas à stocker ou communiquer des données, mais calculent, quantifient, qualifient ou interprètent des données médicales pour le bénéfice de clients individualisés, lorsqu'ils sont spécifiquement destinés à l'une des actions médicales précitées. Cette législation ne contient aucune disposition particulière concernant la protection des données personnelles collectées par un dispositif médical. À cet égard, la Commission européenne a lancé une consultation sur la m-santé en avril 2014.





■ ■ ■ Par ailleurs, les textes européens ne s'opposent aucunement à la mise en place d'initiatives d'autorégulation, telles que celles qui existent déjà au Royaume-Uni et en Allemagne.

C'est ainsi que le Service national de santé anglais (*National Health Service*) a ouvert un portail qui propose au grand public une sélection [d'applications mobiles de santé « de confiance »](#) et une procédure d'évaluation de ces applications en fonction de leur pertinence médicale et de leur conformité à la loi sur la protection des données personnelles. Les applications référencées ont été préalablement évaluées et sont classées en trois catégories : pathologies, vivre en bonne santé (forme, sexualité, nutrition, perte

de poids...), information des patients. Chaque application donne lieu à une brève description. Les usagers sont également invités à communiquer leur avis.

En Allemagne, la première initiative d'autorégulation a été développée par une université et un pharmacologue. Il s'agit d'offrir un label de qualité aux applications de santé disponibles pour le grand public au vu d'un code de conduite qui exige notamment le respect des règles de protection des données et la limitation de l'utilisation des données aux finalités de l'application justifiées par ses fonctions. Une seconde plateforme d'évaluation des applications de santé – pour l'instant limitées au suivi du diabète – est développée

par l'institut en charge de l'analyse de l'utilisation potentielle des nouvelles technologies dans le secteur de la santé et financée par l'État de Rhénanie du Nord - Westphalie.

Au total, il faut constater que peu d'autorités européennes se sont clairement exprimées sur le statut des outils et applications de *quantified self*, n'y ayant été probablement que peu confrontées.

L'APPROCHE PROACTIVE DE LA CORÉE DU SUD

Parmi les autres pays, il y a surtout lieu de citer la Corée du Sud, bien que sa législation en matière de protection des données personnelles ne définisse, pas plus que les autres, la notion de donnée de santé. Celles-ci y sont également considérées comme des données sensibles, ce qui signifie que leur traitement ne peut intervenir que si le responsable de traitement a dûment informé les personnes et obtenu leur consentement explicite et spécifique. Cependant, les autorités compétentes ont adopté une définition restrictive des données de santé, qui doivent nécessairement être liées à une pathologie définie. Dans le cas contraire, les données traitées ne relèvent pas de cette catégorie. Il en résulte que les données généralement collectées dans le cadre d'applications mobiles de santé ne devraient pas être considérées comme des données de santé en droit coréen.

La KFDA (*Korean Food and Drug Administration*) s'est notamment prononcée sur le statut d'une application mobile destinée à « calculer la probabilité de cancer de la prostate par le biais d'une biopsie de la prostate ». La KFDA y a vu un dispositif médical qui aurait dû faire l'objet d'une autorisation de commercialisation de sa part. En l'absence d'une telle démarche, la commercialisation de l'application a été interdite en Corée du Sud. En revanche, un nouveau smartphone comportant un capteur de fréquence cardiaque ne sera pas certifié en tant qu'équipement médical.

La KFDA en a profité pour indiquer que les applications mobiles seraient exemptées du régime des dispositifs médicaux et des obligations qui y sont associées lorsqu'elles ne seront utilisées que pour gérer des informations

simples ou aider à prendre soin de soi en fournissant au particulier qui l'utilise des informations médicales. Plus précisément, la KFDA a donné la liste des catégories d'applications pouvant être commercialisées sans autorisation préalable : celles qui aident à l'auto-surveillance notamment en matière de nutrition, de surveillance du poids, d'hypertension ou de diabète, et celles qui sont utilisées pour soulager l'anxiété de personnes souffrant de désordres mentaux (ex. : en proposant de la musique de relaxation).

Enfin, une nouvelle loi devrait, à terme, distinguer les appareils médicaux des appareils de loisirs ou de bien-être.

EN RÉSUMÉ

Au terme de cet examen de quelques législations étrangères parmi les plus significatives, un constat s'impose. Tous ceux qui ont cherché à distinguer entre les données de santé au sens originel, c'est-à-dire traitées par des professionnels de santé, et d'autres données qui seraient davantage liées à la notion de "bien-être", ont rencontré des difficultés pour la mettre en oeuvre. La volonté d'une telle distinction correspond à l'idée qu'il serait excessif d'appliquer à la seconde catégorie le régime juridique des données de santé au sens originel, jugé trop contraignant. Cette approche a été retenue par les autorités des Etats-Unis et de Corée du Sud, qui se sont prononcées sur l'étendue de leurs compétences et sur le champ d'application de leur législation sur les dispositifs médicaux. Pourtant, les données traitées dans les deux hypothèses sont parfois exactement les mêmes. Ne faudrait-il pas, dès lors, chercher dans une autre direction ? ■

POUR UN *HABEAS CORPUS* DE L'HOMME CAPTÉ

“ *We shall not lay hand upon thee* » (« Nous ne lèverons pas la main sur toi »). Telle était la promesse faite dans la Magna Carta : celle de respecter le corps dans son intégralité (*Habeas Corpus*). Cette promesse a survécu au progrès technologique. Chaque intervention sur le corps, chaque opération de traitement de données à caractère personnel doit être considérée comme touchant le corps dans son ensemble, comme touchant un individu qui doit être respecté dans son intégrité à la fois physique et mentale. C'est là un nouveau concept global de l'individu, et sa traduction dans la réalité donne le droit de revendiquer le respect total d'un corps qui, aujourd'hui, est à la fois physique et électronique. Dans notre monde actuel, la protection des données à caractère personnel remplit la mission de garantir le « *Habeas Data* » que rend nécessaire un environnement modifié, devenant ainsi une composante inaliénable de notre civilisation, comme l'a été l'*Habeas Corpus*. ”

Groupe européen d'éthique des sciences et des nouvelles technologies auprès de la Commission européenne

Avis consacré aux aspects éthiques des implants TIC dans le corps humain (16 mars 2005)

Comment appréhender les nouvelles pratiques de *quantified self* du point de vue de la régulation ? Les réglementations existantes sont-elles adaptées ?

Si dans quelques pays, une réflexion sur ce sujet se fait jour, seuls les États-Unis se sont engagés dans la voie d'une régulation plus ou moins spécifique mais inspirée de la législation sur les dispositifs médicaux, donc essentiellement sur le plan du risque sanitaire (cf. partie précédente). Sous l'angle de la protection des données personnelles, la question commence cependant à être discutée tant aux États-Unis, en Corée du sud qu'en Europe.

Pourquoi ? Parce que ces pratiques, représentatives d'un nouveau mode de rapport des individus à leurs données, soulèvent à l'évidence des enjeux spécifiques pour la vie privée et l'identité humaine, à l'horizon du Monde des capteurs qui se profile (cf. partie 01).

Car si l'on résume, le *quantified self*, c'est la volonté de chacun de capter des données issues ou au plus près de son corps, pour une meilleure connaissance de soi et ce, généralement, sans médiation médicale. Il s'agit de données d'un genre ou d'un usage nouveau, qui, pour certaines (ex. : tension, rythme cardiaque), étaient traditionnellement recueillies et analysées dans le cadre du fameux colloque singulier patient-médecin.

Mais c'est aussi, paradoxalement, une pratique communautaire de partage de ces données, intimes, que l'on gardait jusqu'à présent plutôt pour soi ou que l'on confiait à son médecin.

Et c'est enfin, pour assurer le traitement et l'analyse de ces données, l'intervention, dans un domaine ressortant traditionnellement de la sphère médicale, d'acteurs tiers, fabricants de matériels, dispositifs et objets connectés, éditeurs d'applications, plateformes, et ce dans des rôles économiques encore difficiles à définir aujourd'hui (cf. partie 02).

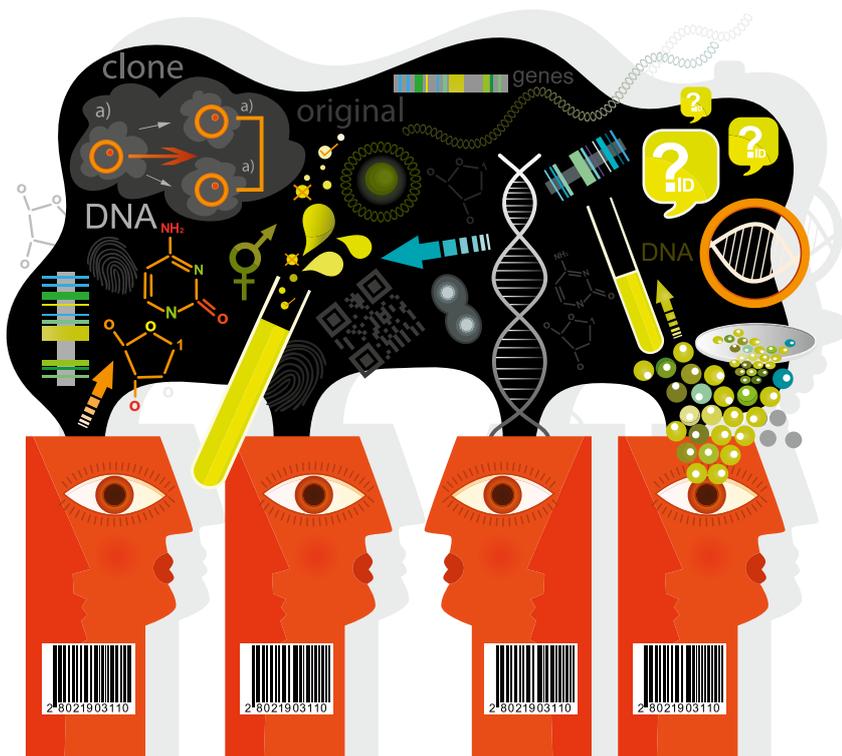
Comment analyser ces pratiques au prisme des concepts et principes de protection des données personnelles ?

DES ÉLÉMENTS DU CORPS HUMAIN AVANT TOUT

Les données produites via les dispositifs de *quantified self*, en tant qu'elles se rapportent à des « éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale » (au sens de l'article 2 de la directive européenne sur la protection des données personnelles), constituent à l'évidence des données personnelles dans ce qui peut être considéré comme l'essence même de la donnée personnelle, l'intime.

Mais s'agit-il de données de santé ? Cette question est posée car la réponse apportée conditionne le régime de protection des données applicable, au moins pour les pays qui disposent d'une régulation en la matière.

En Europe, les données personnelles relatives à la santé constituent une catégorie particulière de données (qualifiées de « sensibles ») et leur traitement est en principe interdit, sauf exceptions encadrées par la loi. Ainsi les données de santé ne peuvent être utilisées et communiquées que dans des conditions déterminées par la loi et dans l'intérêt des personnes (assurer le suivi médical,



faciliter sa prise en charge par l'assurance maladie...), pour les besoins de la santé publique ou encore, point important, si la personne concernée a donné son consentement exprès.

Toutefois, même dans ce cas, l'État peut prévoir, par la loi, que ce consentement ne suffit pas pour permettre à un tiers d'utiliser ces données. Ceci procède implicitement de l'idée selon laquelle les individus ne sont pas libres de faire n'importe quel usage de leur corps.

L'objectif, comme l'a souligné le Groupe européen d'éthique des sciences et des nouvelles technologies auprès de la Commission européenne dans son avis du 16 mars 2005 consacré aux aspects éthiques des implants TIC dans le corps humain, est de « protéger la partie la plus sensible du "corps électronique" en empêchant la personne concernée d'y donner elle-même un accès susceptible de compromettre son intégrité ».

Il s'agit, fondamentalement, de préserver de tout usage contraire à l'intérêt public ou à l'intérêt de la personne des données considérées comme relevant de ce qui est au plus intime de l'homme, de le protéger contre d'éventuelles pratiques discriminatoires à son encontre, fondées sur son état de santé. Poursuivant la

réflexion, Antoinette Rouvroy souligne d'ailleurs qu'un acte de renonciation à un droit comme la vie privée (comme celui de consentir à la divulgation de ses informations) « n'est pas qu'un *self-regarding act* : il a aussi un impact sur la société car la divulgation volontaire par certains d'informations personnelles dans des contextes compétitifs comme celui de l'emploi ou de l'assurance oblige tous les autres à divulguer eux aussi des informations du même type sous peine de subir un désavantage compétitif ou de voir leur refus de divulgation interprété - par l'employeur, par l'assureur - comme un indice de « mauvais risque » (cf. Cahiers IP n°1 de la CNIL, « [Vie privée à l'horizon 2020](#) », 2012). Dans le même esprit, Laurent Alexandre rappelle que les données génétiques sont avant tout des données familiales et ne peuvent du fait de ce statut particulier être partagées comme n'importe quelle donnée.

Ces raisons justifient par exemple qu'en France la loi interdise aux assureurs de disposer des résultats de tests génétiques et ce même avec le consentement des personnes.

De la même manière, la CNIL a toujours considéré que les données personnelles de santé ne pouvaient être utilisées à des fins commerciales même si les textes ne le consacrent explicitement que pour certaines catégories de données de santé (recueillies dans le cadre des prescriptions médicales ou de l'assurance maladie) et certaines activités notamment d'hébergement. À cet égard, la France dispose d'une législation particulière, unique en Europe, puisque ces activités d'hébergement sont soumises à agrément ministériel après avis de la CNIL.

Mais si l'Europe dispose d'une législation contraignante en matière de données de santé, curieusement, sauf exceptions dans certaines législations nationales, cf. chapitre 3.1) il n'existe pas de définition officielle de la donnée de santé. 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 services de santé à cette personne ».

Il ne semble *a priori* pas contestable de considérer que des données confiées à un médecin ou issues de sa pratique médicale (diagnostics, résultats d'examen, soins) ressortent naturellement de la catégorie de données de santé et ■■■

- ■ ■ doivent donc bénéficier d'un régime de protection renforcé.

Alors qu'en est-il du *quantified self* ? Certes, l'Organisation Mondiale de la Santé définit la santé comme « un état de complet bien-être physique, mental et social et ne consiste pas seulement en une absence de maladie ou d'infirmité ». Nombre de pas, poids, heures de lever et de coucher..., dans une première approche, on pourrait être tenté de considérer comme anodines ces données prises isolément et en dehors de tout contexte. On ne peut semble-t-il considérer que les données collectées dans le cadre des outils et applications du *quantified self* sont toutes, par nature, des données de santé. Cependant, certaines informations, prises indépendamment et en valeur absolue, peuvent dans des situations précises être considérées comme données de santé, en raison de l'information objective qu'elles sont susceptibles de transmettre. Par exemple, un poids objectivement excessif peut révéler une pathologie telle que l'obésité.

Néanmoins, dans la plupart des cas, il faut au minimum obtenir une moyenne de ces données ou la variation de ces données sur une certaine période de temps pour obtenir une réelle information relative à la santé de cette personne. Ainsi, une mesure de rythme cardiaque sans indication complémentaire notamment sur l'activité de la personne au moment où ce rythme cardiaque a été mesuré peut ne révéler aucune information utile sur cette personne.

Cependant, la compilation de ces données, leur analyse en référence à une « norme » ou encore leur croisement avec d'autres données, sont à l'évidence susceptibles de révéler non seulement des habitudes de vie, des comportements mais aussi dans certains cas, un état de santé, des comportements « anormaux » et induire, potentiellement, des risques de discrimination.

Ainsi, les données du *quantified self* peuvent aussi devenir des données de santé selon l'usage qui en sera fait ou du traitement qui leur sera appliqué. On retrouve donc trois facteurs susceptibles de conditionner le caractère sensible de ces données : le contexte de production d'abord (médical ou non) ; ensuite, les informations objectives véhiculées par la donnée brute ; enfin la destination de ces données.

Comme le souligne Emmanuel Kessous, « aujourd'hui c'est l'utilisation possible des données qui en définit la sensibilité ; par exemple, c'est le système de santé de plus en plus assurantiel qui rend les données de santé sensibles » (cf. Cahiers IP n°1 de la CNIL, « [Vie privée à l'horizon 2020](#) », 2012).

Ces contours flous constituent une véritable

difficulté dans l'appréhension du *quantified self* au regard des exigences de la protection des données personnelles. En effet, les contraintes attachées en France et dans l'Union Européenne à la qualification de donnée de santé peuvent créer un risque de « sur-régulation » ou de « régulation excessive » pour certains outils dont les finalités et les traitements demeurent pour l'heure bénins ou, à l'inverse, générer une trop faible régulation à l'égard d'outils susceptibles, dans certaines conditions, de se révéler dangereux pour leurs utilisateurs compte tenu des données collectées ou de l'usage qui en serait fait. Ce flou résulte aussi du caractère émergent de ce marché où les stratégies des acteurs peuvent changer rapidement...

Plusieurs solutions sont envisageables :

- Éviter une définition trop précise de la donnée de santé de façon à donner une marge d'appréciation au régulateur dans l'application de la réglementation et de moduler ses actions en fonction de risques identifiés ou avérés. Cependant, la législation actuelle semble binaire : données sensibles ou non. Le régulateur ne dispose donc pas d'une réelle souplesse dans ce domaine.

- Établir une définition claire de la notion de donnée de santé intégrant ou non les données du *quantified self* ou à tout le moins préciser si ces données relèvent ou non de cette catégorie. Cette solution serait susceptible d'offrir un plus grand degré de sécurité juridique tant pour les développeurs d'outils et d'applications que pour leurs utilisateurs.

Elle pourrait aussi, paradoxalement, induire un moindre niveau de protection des données personnelles recueillies dans le cadre du *quantified self* dans la mesure où en l'état actuel des textes, dès lors que ces captures de données sont fondées sur le volontariat et donc le consentement de la personne, elles sont *a priori* légales et ne sont soumises à aucun contrôle particulier (et notamment aucune autorisation préalable des autorités de protection des données). Certes il pourrait être argué qu'en France elles nécessitent, à tout le moins, un agrément des prestataires hébergeant ces données. Toutefois, le cadre juridique n'apparaît pas non plus adapté puisqu'il concerne essentiellement les activités d'hébergement des données de santé recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins, sauf à considérer que les pratiques du *quantified self* s'inscrivent toutes dans le cadre d'activités de prévention ?

- Définir des « degrés de sensibilité » des données de santé : il pourrait être envisagé d'établir, sur

la base d'études d'impact de risque, une nomenclature des données de santé, leur conférant un degré de sensibilité selon divers critères tels que le caractère objectif ou subjectif de l'état de la personne (potentiel élément de distinction entre santé et bien-être), la gravité de la pathologie, sa fréquence dans la population, etc. Dans ce cadre, le régulateur pourrait également envisager de prendre en compte les risques liés à la détection ou la compilation de plusieurs catégories de données, etc. Un tel exercice qui suppose, outre des connaissances scientifiques, d'anticiper tous les cas d'usage, paraît délicat à mener.

■ Mais ne convient-il pas d'aller au-delà du concept de donnée de santé ? Il pourrait être considéré que les données du *quantified self*, en ce qu'elles « captent » le corps (extérieurement pour le moment, mais demain peut-être via des dispositifs plus intrusifs, implantés...) constituent finalement des éléments de notre corps (données que l'on pourrait d'ailleurs qualifier de données biométriques au sens premier du terme, mesure du vivant), et doivent par conséquent se voir reconnaître aussi un statut particulier et par là même un mode de régulation plus global, repensé à l'aune des perspectives d'utilisation futures (cf. partie 02).

Si l'on tente un parallèle avec les réflexions menées par le Groupe européen d'éthique des sciences et des nouvelles technologies auprès de la Commission européenne à propos des implants TIC dans le corps humain, sujet tout de même connexe au *quantified self*, ne serait-il pas nécessaire d'envisager un encadrement global, tant éthique que juridique, des usages non seulement médicaux mais aussi non médicaux des dispositifs de *quantified self* ?

Selon le comité d'éthique, ce cadre juridique, s'agissant des implants TIC, pourrait découler des principes généraux qui sous-tendent les législations nationales et les instruments de droit international en vigueur (notamment la Charte des droits fondamentaux de l'Union européenne), énoncés dans des textes concernant tant la bioéthique que la protection des données personnelles, le principe de consentement éclairé comme la définition des dispositifs médicaux.

Certes, même si aujourd'hui aucune application de *quantified self* ne semble faire appel à des capteurs implantés dans le corps, force est de constater que l'on s'en approche de plus en plus.

Ne conviendrait-il pas, dès lors, de poser certains garde-fous ? Et ainsi de rappeler d'ores et déjà certains commandements éthiques fondamentaux ?

Ainsi, dans quelle mesure n'y aurait-il pas lieu de rappeler dès à présent et par anticipation, dans les réflexions en cours sur le cadre de régulation à construire, certains principes tels que le respect de la dignité humaine – seul droit interrogeable, valeur absolue, comme le rappelle Mireille Delmas-Marty (cf. Cahiers IP n°1 de la CNIL, « Vie privée à l'horizon 2020 », 2012) –, l'intégrité et l'inviolabilité de la personne, la non-instrumentalisation du corps, ainsi que les principes d'équité et d'autonomie ?

Il s'agit bien ici d'accompagner l'innovation en étant vigilant et de procéder à une évaluation continue des risques inhérents au développement de ces technologies de mesure de soi et de leurs impacts potentiels sur l'homme, et ce dans toutes ses dimensions. D'ailleurs, les acteurs économiques du marché sont aujourd'hui dans une phase de tâtonnement et plusieurs études pointent l'attente d'une régulation avec des lignes directrices plus claires pour sécuriser le développement du marché.

Pour toutes ces raisons, le cadre de la régulation qui doit se construire ne peut, à l'évidence, concerner uniquement la protection des données personnelles. Il doit combiner ou intégrer différentes approches : bioéthique, sécurité sanitaire (dispositifs médicaux), protection sociale, économie de la santé...

PRÉVOIR DES RESTRICTIONS D'USAGE

La liberté d'user de son corps est spécifiquement limitée par de nombreux textes en vertu desquels il est interdit de faire du corps humain et de ses parties et/ou produits une source de profit (article 3 de la Charte européenne des droits fondamentaux ; article 21 de la Convention du Conseil de l'Europe sur les droits de l'homme et la biomédecine ; article 4 de la Déclaration universelle de l'Unesco...).

Pour le comité d'éthique européen, une interprétation large de ces principes de non-commercialisation et de non-instrumentalisation pourrait pousser à conclure que l'implantation de dispositifs TIC à des fins que l'on pourrait qualifier de mercantiles (par exemple, l'accès à une discothèque à des conditions préférentielles), ne devrait pas être autorisée.

De la même façon n'y aurait-il pas matière à consacrer définitivement dans notre droit l'idée que, parce que leur recueil et leur utilisation comportent des risques potentiels de discrimination et d'atteinte à l'identité humaine, ■■■

- les données personnelles relatives au corps humain (ce qui intègre les données de santé) doivent faire l'objet de restrictions d'usage et, à tout le moins, ne peuvent, même avec le consentement de la personne, faire l'objet d'exploitations commerciales sous une forme identifiante ?

ÉVALUER ET CERTIFIER L'INTÉRÊT DE SANTÉ DES DISPOSITIFS

En tout état de cause, le principe de finalité comme l'actuelle réglementation des dispositifs médicaux commande d'opérer au moins une distinction entre applications à visée médicale et applications non médicales.

Opérer cette distinction permettrait, pour les applications qualifiées de médicales (outil de diagnostic d'une maladie, aide au traitement ou à la prévention de maladies, outil pouvant intervenir dans la relation entre le patient et l'équipe médicale), de prévoir un mécanisme d'évaluation scientifique et de certification obligatoire (enregistrement ou agrément) s'inspirant ou résultant de l'extension de la réglementation applicable en matière de dispositifs médicaux et de la législation en matière de protection des données. Il s'agirait de s'assurer que ces applications offrent aux patients, utilisateurs et tiers un niveau de protection élevé contre d'éventuelles atteintes physiques et atteignent les performances que leur a assignées leur fabricant. Outre la sécurité sanitaire et la fiabilité de ces outils, il s'agirait aussi de garantir la confidentialité et les droits des personnes. Il pourrait alors être envisagé de concevoir un guichet unique permettant une application combinée de ces réglementations.

Si l'on prend le cas de la France, comme le suggère M^e Pierre Desmarais, « cela signifierait qu'il appartient au législateur d'intervenir, aucune « agence » sanitaire ne pouvant d'elle-même imposer une certification, quitte à déléguer au ministre de la Santé ou à un « *consortium* », constitué de la Haute Autorité de Santé (HAS), de l'Agence Nationale de Sécurité du Médicament (ANSM), de l'Agence des Systèmes d'Information Partagés de Santé (ASIP) et de la CNIL, le soin d'en déterminer le contenu et la forme (cf. Revue de communication et de commerce électronique n°3 mars 2013, étude 5 : « Quel régime pour la m-health ? »). L'objectif poursuivi serait de traiter aussi bien les problématiques liées à la fiabilité des applications ou dispositifs proposés, aux droits des utilisateurs

en matière de protection des données personnelles, qu'à la sécurisation de ces données.

Cela supposerait d'abord d'établir une classification des applications relevant ou non du champ de la m-santé, tâche certes délicate, mais qui pourrait reposer pour partie sur des études d'impact et de risque. Cette classification devrait se traduire par un marquage spécifique permettant au public de distinguer ce qui relève ou non du médical. Ceci devrait aussi conduire les plateformes d'applications à en faire explicitement mention. La question du rôle joué par les magasins d'applications reste ouverte, dans la mesure où ils constituent le canal préférentiel de distribution des services de *quantified self*. On y retrouve d'ailleurs généralement des catégories « médecine », « santé », « fitness » ou « forme » qui permettent de guider les utilisateurs vers ces usages. Un marquage spécifique, reconnu par les utilisateurs, est une piste à prendre avec considération, compte tenu de la structure de marché des appstores où 90 % des téléchargements sont concentrés sur les 5 plus grands magasins d'applications : Play (Android), Appstore (Apple), Windowsphone Store (Microsoft), Appworld (BlackBerry), Ovi (Nokia) (source : Étude Resarch2Guidance 2013).

Les utilisateurs d'applications et d'appareils de *quantified self* n'ont, en effet, pour une majorité d'entre eux, qu'une conscience assez limitée des problématiques relatives à la protection de leurs données personnelles dans le cadre de leur usage de ces nouveaux outils. Cette méconnaissance peut être liée à différents facteurs, tels que le faible niveau d'information, la méconnaissance du fonctionnement de ces nouveaux outils, le design d'interface des applications ou services qui ne place pas nécessairement les intérêts des utilisateurs au premier plan, etc. Une information assurée conjointement par les autorités sanitaires compétentes, les autorités de protection des données, mais aussi par les fabricants, éditeurs d'applications et plateformes pourrait être diffusée à destination du grand public afin d'attirer son attention sur les bonnes pratiques à mettre en œuvre.

Ainsi, une application qui se présenterait uniquement comme un outil de suivi personnel d'activités physiques ou de sommeil, sans référence à une maladie, et qui n'interviendrait pas pour donner des conseils et recommandations, dans un traitement ni dans les relations entre un professionnel de santé et le patient, ne serait pas considérée comme poursuivant une finalité médicale. Elle ne serait donc pas soumise à une procédure de certification. Il pourrait cependant



être souhaitable de prévoir une procédure d'enregistrement de ces applications auprès du guichet unique, permettant ainsi une veille en continu (à l'instar de la FDA).

Au-delà, il pourrait être envisagé un cadre de régulation à l'égard des fabricants et développeurs d'outils et d'applications de *quantified self*, qui, à court terme et dans un premier temps, pourrait prendre la forme de recommandations notamment des autorités de protection des données mais qui devrait se traduire à plus long terme par une législation spécifique au plan européen.

Outre l'instauration de certaines restrictions d'usage des données personnelles (notamment de cession commerciale), il pourrait ainsi être envisagé de limiter les catégories de destinataires susceptibles de recevoir ces données afin, notamment, d'éviter tout risque de partage à des fins potentiellement discriminantes pour les personnes concernées (par exemples avec des sociétés d'assurance, banques, etc). Au niveau européen, le recours à des *Privacy Impact*

Assessments pour les applications de *quantified self* pourrait être encouragé à l'instar du cadre applicable aux applications RFID (Recommandation de la Commission européenne du 12 mai 2009). Cette approche serait cohérente avec le projet de règlement européen concernant les données personnelles, qui exige une étude d'impact pour les traitements qui présentent des risques pour les utilisateurs.

Elle pourrait être accompagnée d'un degré d'exigence plus élevé en matière, d'une part de sécurité des données (par exemple par la définition de standards), d'autre part d'information des personnes par les fabricants, éditeurs d'applications et plateformes, notamment sur le caractère médical ou non des dispositifs, les conditions d'utilisation des données, les modalités de suppression de celles-ci...

ACCOMPAGNER LES INITIATIVES D'AUTO- OU CO-RÉGULATION ?

De façon complémentaire, ne conviendrait-il pas d'encourager les initiatives d'auto-régulation ou de co-régulation au niveau national et international ? Ces initiatives présenteraient un intérêt certain dès lors que, par des mécanismes d'évaluation des applications de bien-être, elles offriraient aux utilisateurs des repères dans le choix de leurs applications, et ceci non seulement du point de vue de la fiabilité mais aussi de la sécurité et de la protection des données en général. Ce type d'initiatives aurait par ailleurs le mérite d'éduquer les utilisateurs à la prise en compte des aspects relatifs à la protection de leurs données et de leur vie privée dans leurs usages numériques – *a fortiori* sur smartphone.

Les autorités de protection des données pourraient-elles envisager de conduire elles-mêmes de tels tests ou, à tout le moins, de contribuer à ces initiatives, en fournissant par exemple une grille d'analyse et d'évaluation des applications pour ce qui concerne le traitement des données personnelles ?

Enfin, sous réserve d'évaluer les potentialités de ce type de démarche, ne faudrait-il pas envisager le développement d'un label protection des données (ou de codes de bonne conduite) pour les applications de santé et de bien-être, permettant aux fabricants et aux développeurs de s'engager, s'ils le souhaitent, dans le respect de certaines exigences en matière de protection des données personnelles, afin de rassurer leurs clients et de prouver leur engagement dans une relation de confiance ? ■

Le débat sur ces données du corps et leur utilisation pourrait dans les années à venir prendre sa part dans un débat plus large sur les questions d'éthiques liées au rapprochement du corps et des technologies. La question de ce qui fait l'humain et d'éventuelles limites à son « augmentation » technologique, numérique ou autres, pourrait être un des grands débats politiques et philosophiques autour des droits humains dans un futur proche. Nous avons ici cherché à relater le débat se cristallisant autour d'un grand événement international, une sorte d'équivalent pour les droits de l'homme dans la société numérique des « Sommets de la Terre » en imaginant un extrait de la déclaration finale d'une conférence de ce type, et un document d'activistes publiés en marge de ce sommet officiel.

Quelques sources d'inspiration

- Déclaration Finale en français du Sommet « Rio+20 », 2012 :
- Avis du Groupe européen d'éthique des sciences et des nouvelles technologies auprès de la Commission européenne consacré aux aspects éthiques des implants TIC dans le corps humain (16 mars 2005)
- Cours de Mireille Delmas-Marty au Collège de France, en particulier : *Hominisation et humanisation*, Sens et non-sens de l'humanisme juridique (2010-2011), Vers une communauté de valeurs ? (2006-2007 et 2007-2008)

2022, LE SOMMET DES HUMAINS DE RIO

Le 24 octobre 2022, représentants des gouvernements, des autorités des droits et libertés numériques et de la société civile se sont réunis (physiquement ou en télé-présence) à Rio pour une conférence mondiale sur les droits de « l'homme augmenté ». La déclaration finale a été signée par 140 États, autorités et organisations et pose les bases d'un « habeas data » tant attendu. Attendu, mais craint par certains, en particulier des activistes qui ont organisé un contre-sommet numérique mondial dont le retentissement a été très fort sur l'ensemble de la planète. Leur propre déclaration finale restera longtemps liée à celle du Sommet officiel, comme le revers de la médaille.

24 octobre 2022

Extraits de la Déclaration finale du Sommet international sur les droits et libertés numériques de l'homme et de la Conférence des Nations unies sur les libertés numériques

UNE SEULE HUMANITÉ

1./ Nous, chefs d'État et de gouvernement et représentants de haut niveau, réunis à Rio de Janeiro (Fédération des États du Brésil) du 20 au 24 octobre 2022, avec la participation pleine et entière de la société civile et des citoyens du monde, affirmons solennellement notre engagement à faire émerger une nouvelle génération de droits de l'homme et de libertés fondamentales, adaptées à la numérisation de l'humanité et de la société et au rapprochement des technologies avec le corps.

2./ Il y a 30 ans, en 1992, Rio accueillait le « Sommet de la Terre », qui fut un moment fondamental (après Stockholm en 1972) dans l'affirmation d'une évidence : nous partageons une seule terre. Nous avons symboliquement choisi cette même ville de Rio pour affirmer une autre évidence, que les douloureuses années récentes ont pourtant mise à mal : nous partageons une seule commune humanité.

3./ Nous reconnaissons que l'essor des technologies numériques, cognitives et

génétiques offre à l'humanité des possibilités insoupçonnées pour faire reculer la maladie, la sénescence, les handicaps, pour réparer et améliorer le corps humain. Ces bienfaits ont cependant leur revers : les inégalités, les discriminations et des divisions de plus en plus brutales entre les humains augmentés et ceux qui ne le peuvent ou ne le veulent pas. L'intégration de technologies au corps humain est une chance, mais elle ne doit pas altérer l'identité humaine et conduire à attenter à la dignité de la personne humaine.

4./ Nous réaffirmons en conséquence notre volonté de faire respecter plus que jamais les droits de l'homme et les libertés fondamentales bouleversés par ces évolutions techniques et sociétales.

5./ Nous sommes donc déterminés à aboutir à l'adoption d'un nouvel « *habeas corpus* » qui étendra et adaptera la protection de la personne humaine à ce qui fait sa personnalité et son humanité, au-delà des notions de propriété et de patrimoine immatériel. Un nouveau concept global de l'individu

impose de revendiquer le respect total d'un corps qui, aujourd'hui, est à la fois physique et électronique.

6./ Nous réaffirmons que les technologies ne doivent porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Aucune machine intelligente ou automatisme décisionnel ne doit porter atteinte aux droits et libertés fondamentaux des humains.

7./ Nous réaffirmons que plusieurs principes inviolables sont à la base de ces droits : la non-instrumentalisation qui affirme comme commandement éthique le principe selon lequel l'individu ne doit jamais être considéré simplement comme un moyen, mais toujours comme une fin en soi, le respect de la vie privée comme principe éthique de non-ingérence et d'autonomie de l'individu, la non-discrimination comme principe d'égalité de traitement et d'équité de droit, sauf raison justifiant une différence, ...

8./ »

Société de protection de l'humain (SPH)

**Réduire le corps à une machine,
réduire l'humain à une espèce :
l'homme augmenté est un homme
réduit. Battons nous contre
la robotisation des humains !**



Le Sommet de Rio n'est pas un Sommet de l'Humain, comme les médias du système le célèbrent pour favoriser l'acceptation par les citoyens de cette réification de l'homme et de la femme, mais un Sommet du Post-Humain.

Sous prétexte de défendre ce qui nous unit, ce sommet ne fait en réalité qu'avaliser le projet techno-utopiste de dépassement des limites de l'humanité par la science et la technique. Il est un pas de plus vers la machinisation de l'homme, vers son « amélioration radicale ».

Ne nous y trompons pas, et même si le lobby post-humain affirme que ce projet ne va pas assez loin pour reconnaître le « droit de tous à l'augmentation et à la libération des limites de l'humanité » (voir les propos des militants de la « Fondation pour l'Humanité Future ») : ce Sommet reconnaît la primauté de ce discours post-humain.

Nous entrons dans une période où les connaissances scientifiques permettent de changer le mode de reproduction et les caractéristiques de l'espèce humaine, de fabriquer des hybrides homme/machine. Nous sommes au seuil d'un risque de diversification de l'espèce humaine.

Nous, simples humains libres et égaux en droit et en technologie, affirmons que le véritable Habeas Corpus n'est pas un Habeas data, mais une réaffirmation simple de cette ligne rouge issue de la Grande Charte de 1215 : « Nous ne lèverons pas la main sur toi ».

L'amélioration du monde et le solutionnisme technologique ne lèveront pas la main sur nous !

Nous affirmons ainsi solennellement ces droits de l'homme inaliénables, révolution technologique ou pas :

- Les hommes naissent, demeurent et meurent libres et égaux en droits et en dignité. Cette dignité n'est pas à vendre, même contre un morceau d'immortalité.
- Nous avons tous le droit à l'anonymat, le droit de disparaître sans laisser de traces.
- Nous affirmons solennellement que nous avons le droit au mensonge, à refuser de jouer le jeu.
- Ce qui compte vraiment ne se mesure pas.
- Chaque être humain est singulier et pourtant chacun appartient à la même communauté : l'humanité
- Les robots humanoïdes ne sont pas des humains, leur reconnaître des droits est une aberration
- Les humains ne doivent pas devenir des robots. L'augmentation technologique du corps doit être limitée par la Loi.
- L'acceptation de la machinisation de l'homme ne doit pas être le prix, exorbitant à nos yeux, à payer pour la bonne santé et le bien-être.

BIBLIOGRAPHIE

ALEXANDRE, L., (2011). La mort de la mort : comment la technomédecine va bouleverser l'humanité. Paris : Editions JC Lattès. 425 p. - (Essais et documents)

ALEXANDRE, L., (2013). Transhumain oui. Posthumain non. La revue du Cube [en ligne] (page consultée le 3 janvier 2014) <http://www.cuberevue.com/transhumain-oui-posthumain-non/2293>

ANDREESSEN, M., (2011). Why Software Is Eating The World. Wall Street Journal [en ligne et en anglais], article payant, août 2011 (page consultée le 26 février 2014) <http://online.wsj.com/news/articles>

ATELIER(L), (2012). La caméra et les capteurs trahissent le propriétaire d'un téléphone. [en ligne], (page consultée le 26 février 2014) <http://www.atelier.net/trends/articles/camera-capteurs-trahissent-proprietaire-un-telephone>

ATELIER BNP Paribas, (2013). Sondage « Les objets connectés, au centre d'un nouvel écosystème de santé ? » réalisé par l'Ifop sur un échantillon de 1001 personnes du 20 au 22 novembre 2013 et publiée en décembre 2013

BESNIER, J.M., (2013). L'humanité: une expérience raté ? Versions du transhumanisme. Futuribles, novembre-décembre 2013, p. 5.

CANALYS (2014). 1.6 million smart bands shipped in H2 2013, [en ligne et en anglais] (page consultée le 25 février 2014) <http://www.canalys.com/newsroom/16-million-smart-bands-shipped-h2-2013>

CERF, V., (2013). Strong Authentication and Pseudonymity on the Internet. Conference US 2013 Keynote, RSA Conference, 25 février - 1^{er} mars 2013, San Francisco, USA. [vidéo en ligne et en anglais], (page consultée le 26 février 2014) <http://youtu.be/ZYAJaOVuyxI?t=15m46s>

CONSEIL GENERAL DE L'ECONOMIE, DE L'INDUSTRIE, DE L'ENERGIE ET DES TECHNOLOGIES (CGEJET), (2012). Rapport : 'Bien vivre grâce au numérique'. [en ligne], (page consultée le 25 février 2014) <http://www.cgeiet.economie.gouv.fr>

CNIL, (2013). « Étude benchmark sur les régulations concernant l'utilisation dans le domaine de la santé et du bien-être des capteurs, smartphones et autres objets connectés », réalisée par Hogan Lovells. *Étude réalisée sur commande de la CNIL pour son usage exclusif.*

CNIL, (2012). Cahier IP Innovation et Prospective n°1 « Vie privée à l'horizon 2020, Paroles d'experts ». <http://www.cnil.fr/ip>

COLIN, N., VERDIER, H., (2012). L'âge de la multitude : Entreprendre et gouverner après la révolution numérique. Paris : A. Colin. 288 p.

DAYAL, G., (2012). Researchers Hack Brainwaves to Reveal PINs, Other Personal Data. Wired Magazine, août 2012 [en ligne et en anglais], (page consultée le 26 février 2014) <http://www.wired.com/threatlevel/2012/08/brainwave-hacking/>

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

DESROSIERES, A., (2008). Pour une sociologie historique de la quantification : L'Argument statistique I. Paris : Presses de l'École des Mines, 329 p.

FOX, S., DUGGAN, M., (2013). Tracking for Health. Pew Research Center's Internet & American Life Project. [en ligne et en anglais] (page consultée le 25 février 2014) <http://www.pewinternet.org/2013/01/28/tracking-for-health/>

FEDERAL TRADE COMMISSION (2013). Conférence publique : "Internet of Things - Privacy and Security in a Connected World". [en ligne et en anglais], (page consultée le 26 février 2014) <http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world>

FONDATION INTERNET NOUVELLE GENERATION, ALBAREDE, M., FRANCOU, R., KAPLAN, D., (2013). Cahier d'exploration "Mes Infos" de la FING [en ligne]. (page consultée le 26 février 2014). <http://fing.org/>

GADENNE, E., (2012). Guide pratique du Quantified Self. Mieux gérer sa vie, sa santé, sa productivité. Limoges : Éditions Fyp. 224 p.

Groupe européen d'éthique des sciences et des nouvelles technologies auprès de la Commission européenne, (2005). Avis consacré aux aspects éthiques des implants TIC dans le corps humain [en ligne] (page consultée le 26 février 2014) http://ec.europa.eu/bepa/european-group-ethics/docs/avis20_fr.pdf

GUILLAUD, H., (2013). Big Data : pourquoi nos métadonnées sont-elles plus personnelles que nos empreintes digitales ? Internet Actu [en ligne], (page consultée le 26 février 2013) <http://internetactu.blog.lemonde.fr/2013/12/13/big-data-pourquoi-nos-metadonnees-sont-elles-plus-personnelles-que-nos-empreintes-digitales/>

GUILLAUD, H., (2013). La mise en chiffres de soi (article en 2 parties). InternetActu, mai et juin 2013 [en ligne] (page consultée le 3 mars 2014) <http://www.internetactu.net/2013/05/22/la-mise-en-chiffre-de-soi-12-qui-sont-ceux-qui-se-mesurent/> <http://www.internetactu.net/2013/06/11/la-mise-en-chiffres-de-soi-22-les-chiffres-ne-savent-pas-toujours-repondre/>

HALADJIAN, R., (2012). Rafi Haladjian, Founder, Sen.se talks about "The Meaning of Life". Conférence LeWeb Paris. [vidéo en ligne et en anglais], (page consultée le 10 mars 2014) <http://www.youtube.com/watch?v=GeJw7uuhhVc>

HINSHAW, M., KASANOFF, B., (2012). Smart Customers, Stupid Companies: Why Only Intelligent Companies Will Thrive, and how to be One of Them. [en anglais]. New York : Business Strategy Press, 187 p.

INSTITUT MONTPARNASSE, (2012). Rapport de F. EWALD : Assurance, prévention, prédiction... Dans l'univers du Big Data. Collections Recherches [en ligne], (page consultée le 9 avril 2014) http://www.institut-montparnasse.fr/wp-content/files/Collection_recherches_n_4.pdf

JARVIS, J., (2013). I see you: The technopanic over Google Glass. [en ligne et en anglais], (page consultée le 26 février 2014) <http://buzzmachine.com/2013/03/07/i-see-you-the-technopanic-over-google-glass/>

KAPLAN, D., (2010). Informatique, libertés, identités. Limoges : FYP. 142 p.

KHARIF, O., (2013). Trillions of Smart Sensors Will Change Life. [en ligne et en anglais] (page consultée le 25 février 2014) <http://www.bloomberg.com/news/2013-08-05/trillions-of-smart-sensors-will-change-life-as-apps-have.html>

KNUDSEN, J., (2012). SelfTracking – The Next “Big Thing”? Scenario Magazine [en ligne et en anglais], juin 2012 (page consultée le 26 février 2014) <http://www.scenariomagazine.com/self-tracking-%E2%80%93-the-next-%E2%80%93-big-thing%E2%80%99/>

LEBLANC, G., (2004). Les maladies de l'homme normal. Bègles : Éditions du Passant, 219 p.

MANYIKA, J., CHUI, M., BUGHIN, J., et al. (2013). Disruptive technologies: Advances that will transform life, business, and the global economy [en ligne et en anglais]. (page consultée le 25 février 2014) http://www.mckinsey.com/insights/business_technology/disruptive_technologies

PHARABOD, A., NIKOLSKI, V., GRANJON, F., et al. (2013). La mise en chiffres de soi : Une approche compréhensive des mesures personnelles. In : *Réseaux*, n° 177 (Février - Avril 2013), Paris : La Découverte, 97-129

PRIVACY RIGHTS CLEARINGHOUSE, (2013) Mobile Health and Fitness Apps: What Are the Privacy Risks? [en ligne et en anglais], (page consultée le 25 février 2014) <https://www.privacyrights.org/mobile-health-and-fitness-apps-what-are-privacy-risks>

RESEARCH2GUIDANCE, (2013). Étude « Mobile Health Market Report 2013-2017 » [payant, disponible en ligne et en anglais]. (page consultée le 27 février 2014) <http://www.research2guidance.com/shop/index.php/mhealth-report-2>

SAMSUNG, (2013). What You May Not Know About GALAXY S4 Innovative Technology. [en ligne et en anglais] (page consultée le 26 février 2014) <http://global.samsungtomorrow.com/?p=23610>

SCOBLE, R., (2013). Google, the freaky line and why Moto X is a game-changer. The Next Web, août 2013 [en ligne et en anglais], (page consultée le 26 février 2014) <http://thenextweb.com/google/2013/08/02/google-the-freaky-line-and-why-moto-x-is-a-game-changer/#!ss6ok>

STIEGLER, B., (2005-6), Individuation et grammatisation : quand la technique fait sens... Éditions : *Documentaliste-Sciences de l'Information*, 2005/6 Vol. 42, p. 354-360. <http://www.cairn.info/revue-documentaliste-sciences-de-l-information-2005-6-page-354.htm>

SUSSAN, R., (2005). Les utopies posthumaines. Sophia-Antipolis : Omniscience. 287 p.

TIERNAN, R., (2013). Internet of Things: Mammoth Morgan Stanley Note Tries to Explain It. [en ligne et en anglais] (page consultée le 25 février 2014) <http://blogs.barrons.com/techtraderdaily/2013/09/26/internet-of-things-mammoth-morgan-stanley-note-tries-to-explain-it/>

THOMSON REUTERS FOUNDATION, MHEALTH ALLIANCE, BAKER & MCKENZIE ET AL., mHealth Alliance, Baker & McKenzie et al.. Rapport « Patient Privacy in a Mobile World – A Framework to address Privacy Law Issues in Mobile Health », Juin 2013

TUCKER, I., (2013). Evgeny Morozov: “We are abandoning all the checks and balances”. The Guardian [en ligne et en anglais], (page consultée le 25 février 2014) <http://www.theguardian.com/technology/2013/mar/09/evgeny-morozov-technology-solutionism-interview>

VENTER, C., (2010). Creation of a Bacterial Cell Controlled by a Chemically Synthesized Genome. *Science Mag* Vol. 329 n° 5987 pp. 52-56 [en ligne et en anglais], (page consultée le 3 mars 2014) <http://www.sciencemag.org/content/329/5987/52.full>

VERDIER, H., (2012). Connais toi toi-même (petite Philosophie du #QuantifiedSelf). [en ligne] (page consultée le 25 février 2014) <http://www.henriverdier.com/search/label/Quantified%20%20Self>

VIDAL, (2013). 2^e baromètre sur les médecins utilisateurs de smartphone en France [en ligne]. (page consultée le 25 février 2014) <http://corp.vidal.fr/presse/espace-professionnel/583-2eme-barometre-sur-les-medecins-utilisateurs-de-smartphone-en-france>

VION-DURY, P., (2013). Le transhumanisme français: que des surhommes, pas de sous-hommes. Rue89, 11 mars 2013 [en ligne] (consulté le 3 janvier 2014) <http://rue89.nouvelobs.com/2013/03/11/le-transhumanisme-francais-que-des-surhommes-pas-de-sous-hommes-240310>

WIRED MAGAZINE, (2012). Personal Drone's Secret Ingredient: iPhone. *Wired Magazine*, juin 2012 [en ligne et en anglais], (page consultée le 26 février 2014) http://www.wired.com/dangerroom/2012/06/ff_flyingsmartphone

LISTE DES EXPERTS INTERVIEWÉS

Les propos recueillis lors des entretiens sont des points de vue personnels, ils n'engagent pas les organismes pour lesquels travaillent les experts.

Dr. Laurent ALEXANDRE,

PDG de DNAVision. Auteur de "La mort de la mort : comment la technomédecine va bouleverser l'humanité" paru aux Editions JC Lattès (2011). Co-fondateur de Doctissimo.

Laurence ALLARD,

Sociologue. Co-fondatrice de l'association Citoyens Capteurs et maître de conférences, IRCAV-Paris 3/Lille 3.

Bernard BENHAMOU,

Délégué aux usages de l'internet au Ministère de la Recherche et de l'Enseignement Supérieur.

Pierre DESMARAIS,

Avocat spécialisé dans la santé.

Céline DESWARTE,

Chargée de mission eSanté à l'Unité Santé et Bien-être de la Direction générale CONNECT, Commission Européenne.

Emmanuel GADENNE,

Consultant. Auteur du "Guide pratique du Quantified Self. Mieux gérer sa vie, sa santé, sa productivité" paru chez Fyp éditions (2012).

Hubert GUILLAUD,

Journaliste. Rédacteur en chef d'InternetActu.net au sein de la Fondation Internet Nouvelle Génération (FING).

Cédric HUTCHINGS,

PDG de Withings.

Julien GUEZ,

Directeur de la stratégie, du marketing et des affaires publiques chez Malakoff Médéric.

Norbert PAQUEL,

Consultant. Délégué général EDISANTE.

Robert PICARD,

Ingénieur général des Mines. Référent Santé du CGEJET.

Dr Nicolas POSTEL-VINAY,

Unité d'hypertension à l'Hôpital Georges Pompidou. Directeur du site www.automesure.com

Antoinette ROUVROY,

Chercheur qualifié du FRS-FNRS en philosophie du droit, associée au centre de recherche en Information, Droit et Société (CRIDS) de l'Université de Namur. Membre du comité de la prospective de la CNIL.

Dr Denise SILBER,

Fondatrice du congrès Doctors 2.0 & You. Co-fondatrice et Présidente de l'AQIS (Association Qualité Internet Santé).

Des représentants des sociétés Be Patient, DMD Santé, MedAppCare, Mobile Health, Humetrix ont également été rencontrés.



MAI 2014

Commission Nationale de
l'Informatique et des Libertés

8, rue Vivienne - CS 30223
75083 Paris CEDEX 02
tél. : 01 53 73 22 22
fax : 01 53 73 22 00
deip@cnil.fr
www.cnil.fr

