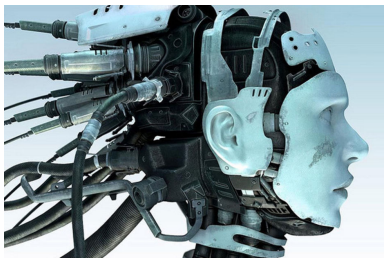
# Hyperconnexion du corps humain : 3 règles pour ne pas faire n’importe quoi | Le Net Expert Informatique

| | |
|---|---|
|  | Hyperconnexion du corps humain : 3 règles pour ne pas faire n’importe quoi |

**Face au déploiement des objets connectés au corps humain, qui permettent de recueillir des données de santé, utilisateurs et industriels doivent être particulièrement vigilants, nous explique Nathalie Dreyfus, conseil en propriété industrielle, Dreyfus & Associés, expert près la cour d'appel de Paris et à l'OMPI.**

Bracelets, montres, balances connectés… la m-santé envahit les magasins spécialisés. Au-delà de leur côté ludique, ces objets permettent aux entreprises de recueillir de très nombreuses données sur leurs utilisateurs : rythme cardiaque, nombre de pas effectués par jour, quantité et qualité du sommeil, taux de sucre dans les larmes, taux d'alcoolémie ou tension artérielle…
Ce mouvement de collecte massive de données – le big data – n'en est qu'à son début, selon la Cnil. En 2017, un utilisateur de smartphone sur deux aura installé au moins une application dédiée à son bien-être et à sa santé.

Les données recueillies sont traitées par de nombreuses entreprises qui les exploitent afin de mieux connaître leurs clients. Une pratique intrusive, qui doit susciter la vigilance des utilisateurs, mais aussi des industriels. En effet, leur responsabilité peut-être engagée. Les données recueillies, liées à la santé, ont un caractère sensible et font l'objet d'une protection renforcée. Ainsi, leur collecte et leur traitement, soumis à un contrôle accru, doivent être autorisés. Mais certaines data -celles se rapportant en général au bien-être-, échappent à une demande d'autorisation préalable grâce aux normes simplifiées. Attention cependant car la frontière entre bien-être et santé est particulièrement ténue.

Pour assurer leur sécurité juridique, les industriels du secteur mettre en place quelques règles.
**1. RESPECTER LE CADRE LÉGAL ET LE RAPPORT DE LA CNIL SUR LA PRATIQUE DU « QUANTIFIED SELF »**
Le rapport de la Cnil, déposé fin mai 2014, intitulé 'Le corps, nouvel objet connecté', traite des problèmes liés aux données personnelles de santé issues des applications et objets de mesure de soi (quantified self). Ces pratiques consistent généralement à mesurer et à comparer avec d'autres, des variables de notre mode de vie (nutrition, exercice physique, sommeil…). La pratique du « quantified self » va continuer à s'imposer, le corps humain étant de plus en plus connecté dans ses fonctions biologiques.

Le « quantified self » constitue donc un marché d'avenir pour les professionnels. Des assureurs américains ont déjà annoncé leur souhait d'utiliser les objets connectés dans le suivi de leurs clients et la prise en compte des données dans l'indemnisation en cas de dommage. La Cnil s'inquiète des nombreux risques potentiels, tels que l'exploitation commerciale abusive des données personnelles et l'intrusion dans la vie privée des utilisateurs. Nul doute pourtant que la Commission, appuyée par le G29 et la Commissaire européenne Viviane Reding, auront à cœur de protéger ces données médicales. Dans l'attente – et face aux lois françaises et européennes très protectrices, particulièrement en ce qui concerne les données sensibles – les industriels développant des produits liés à la santé doivent veiller à rester dans les clous lors de la collecte.

**2. MISER SUR LE « CLIENT EMPOWERMENT » POUR GAGNER LA CONFIANCE DES CONSOMMATEURS**
Ce mouvement donne davantage de pouvoirs de contrôle au client. Il permet de rééquilibrer la relation entre l'entreprise collectrice de données et l'usager qui a souvent l'impression d'être négligé par les professionnels. Cette prise de pouvoir peut aussi permettre la patrimonialisation des données à condition d'obtenir le consentement direct du client. Cela ouvre aux industriels la possibilité de commercialiser les données collectées.

**3. SE CONFORMER AUX PRINCIPES DE « PRIVACY BY DESIGN »**
Le concept de « privacy by design » propose de faire de la protection de la vie privée de l'utilisateur une caractéristique majeure de l'objet afin « d'assurer la protection de la vie privée en l'intégrant dans les normes de conception des technologies, pratiques internes et infrastructures matérielles ». Les données recueillies ne sont alors pas extensivement partagées ou revendues. En intégrant ce concept au cahier des charges de l'objet connecté, l'industriel gagnera la confiance des clients et se démarquera aussi de ses concurrents.

**TOUT N'EST PAS PERMIS**
La pratique du « quantified self » va continuer à s'imposer, le corps humain étant de plus en plus connecté dans ses fonctions biologiques. Elle constitue donc un marché d'avenir pour les professionnels. Des assureurs américains ont ainsi déjà annoncé leur souhait d'utiliser les objets connectés dans le suivi de leurs clients et la prise en compte des données dans l'indemnisation en cas de dommage. La CNIL s'inquiète des nombreux risques potentiels, tels que l'exploitation commerciale abusive des données personnelles et l'intrusion dans la vie privée des utilisateurs. Nul doute pourtant que la Commission, appuyée par le G29 et la Commissaire européenne Viviane Reding, auront à cœur de protéger ces données médicales. Dans l'attente, face aux lois françaises et européennes très protectrices, particulièrement en ce qui concerne les données sensibles, les industriels développant des produits liés à la santé doivent tenir compte du fait que tout n'est pas permis.

---



---



---



Source : http://www.usine-digitale.fr/article/hyperconnexion-du-corps-humain-3-regles-pour-ne-pas-faire-n-importe-quoi.N335953
Par Nathalie Dreyfus, conseil en propriété industrielle, Dreyfus & Associés, expert près la cour d'appel de Paris et à l'OMPI