# Big Boss is watching you: votre patron va adorer les objets connectés

| | |
|---|---|
|  | Big Boss is watching you: votre patron va adorer les objets connectés |

---

# L’Odre des Médecins souhaite un remboursement des objets connectés

L’Odre des Médecins souhaite un remboursement des objets connectés

**À l'occasion d'un débat et de la publication d'un livre blanc, le Conseil National de l'Ordre des Médecins préconise d'encadrer les objets connectés liés à la santé par une réglementation européenne.**

"Bonjour, il me faudrait une boîte de pastilles pour la gorge et un bracelet connecté s'il vous plaît". Et si bientôt, entendre cette phrase dans une pharmacie devenait banal ? Les objets connectés liés à la santé sont de plus en plus nombreux : mesure du rythme cardiaque, des phases du sommeil, sans compter les applications associées où l'on rentre des données relatives à nos habitudes alimentaires ou autres. Partant de ce constat, le CNOM (Conseil National de l'Ordre des Médecins) a débattu sur la question, avant de publier un livre blanc détaillant six recommandations.

Parmi elles, on note le souhait d'encadrer les objets connectés par une réglementation européenne : "Afin que la mise sur le marché des outils de m-santé [santé mobile, ndlr] comporte des garanties, le CNOM estime qu'ils devraient faire l'objet d'une déclaration de conformité à un certain nombre de standards. Cette déclaration devrait comporter 3 volets : la confidentialité et la protection des données recueillies, la sécurité informatique, logicielle et matérielle, la sûreté sanitaire".
Il paraît en effet logique que, tout comme ce qu'il se dit lors d'une consultation médicale, les données sanitaires recueillies par des objets connectés et/où des applications restent confidentielles.

Le CNOM estime aussi que ces outils devraient faire l'objet d'une évaluation scientifique systématique, par des experts indépendants. Si l'on devait arriver à la conclusion que l'objet connecté/l'application est bénéfique pour la santé individuelle/collective, "il serait cohérent d'envisager qu'ils soient pris en charge par la collectivité". Autrement dit : l'achat d'un objet connecté ou d'une application pourrait faire l'objet d'un remboursement au même titre que certains médicaments.

Quand on sait que 3 millions d'objets connectés se sont vendus en France en 2013 (étude GFK) et que 11 % des détenteurs déclarent les utiliser dans le contexte de la santé / du bien-être, on comprend la nécessité d'établir une réglementation. Dans les faits, celle-ci risque d'être difficile à mettre en œuvre, surtout au niveau de la confidentialité des données recueillies : pour la grande majorité des applications, le modèle économique repose justement sur la vente des données à diverses entreprises. Il s'agirait alors pour les développeurs d'applis estampillées "santé" de repenser totalement leur stratégie financière.

Et avant même d'envisager une réglementation, le livre blanc du CNOM rappelle qu'il est encore difficile d'évaluer le véritable impact (positif ou négatif) des objets connectés/applications liés à la santé. Selon l'OMS, sur 114 pays interrogés en 2011, seuls 12 % se sont penchés sur cette question.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.android-mt.com/news/lodre-medecins-souhaite-remboursement-objets-connectes-35850

# Voitures connectées faciles à hacker

Voitures connectées faciles à hacker

**Les promesses de la voiture connectée font rêver : sans conducteur, intelligente,… mais visiblement, elle est aussi facile à pirater. Un hackeur en prend ici le contrôle, faisant du véhicule un danger pour ses passagers.**Dans son émission « 60 minutes », CBS News consacre un dossier aux voitures connectées et à leurs failles de sécurité. Kathleen Fisher, experte de la DARPA (Defense Advanced Research Projects Agency) présente la voiture connectée comme un « ordinateur sur roues », soulignant de fait la possibilité de hacker le véhicule.

Démonstration à l'appui : il est en effet possible de contrôler la voiture à distance, à l'aide d'un simple ordinateur portable. Si déclencher les essuie-glaces ou le klaxon peut sembler « inoffensif », quand le hackeur prend contrôle des freins, c'est tout de suite plus inquiétant. Ici, il ne s'agit que de plots en plastique, mais on imagine rapidement les dégâts si une voiture connectée perdait les pédales « dans la vraie vie ».

Plus tôt cette semaine, le sénateur américain Edward J. Markey a sorti un rapport sur les dangers des voitures connectées. Il y compile les données fournies par 16 constructeurs automobiles dont BMW, Fiat Chrysler, Ford, General Motors, Nissan, Mitsubishi ou Mercedes-Benz après qu'il leur ait adressé une lettre et un questionnaire en décembre 2013. Certains constructeurs dont Tesla ont cependant refusé de lui répondre… Selon ses résultats, aucune mesure ne serait mise en place pour détecter et empêcher les tentatives de piratage ou les vols de données. Par ailleurs, outre la sécurité, le rapport revient aussi sur les problèmes de confidentialité des données : les propriétaires de voitures connectés ne seraient pas au courant de tout ce qui est enregistré à leur propos… De quoi faire réfléchir avant d'investir dans la voiture du futur.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.ladn.eu/actualites/pop-insight,voitures-connectees-faciles-hacker,74,24953.html

# Objets de santé connectés : l’Ordre des médecins appelle à une régulation

| | |
|---|---|
| | Objets de santé connectés : l’Ordre des médecins appelle à une régulation |

**Bracelets capteurs d'activité physique, pèse-personnes connectés ou tensiomètres reliés à un smartphone: le développement « exponentiel » des objets de santé connectés rend nécessaire une « régulation » de ce secteur, a estimé mardi l'Ordre des médecins.**

Le Conseil national de l'ordre des médecins (CNOM) a diffusé un « livre blanc » sur la santé connectée, à l'occasion d'un colloque à Paris sur « les enjeux de la santé connectée ».
« Le CNOM se prononce pour une régulation qui impose d'informer l'usager afin qu'il conserve sa liberté dans ce monde connecté et qui assure la fiabilité des technologies et la protection des données personnelles », selon ce livre blanc.
Les objets de santé connectés sont des objets munis de capteurs pour mesurer des paramètres du corps comme le poids, la fréquence cardiaque ou la pression artérielle et qui sont capables de transmettre ces données à une application mobile sur téléphone portable ou à un service web spécifique pour y être stockées et analysées.
Certains de ces objets connectés comme des tensiomètres (pour prendre la tension) ou des glucomètres (pour prendre la glycémie) sont conseillés par des médecins à leurs patients pour leur permettre de suivre plus efficacement des paramètres essentiels à leur santé.
Avec ce livre blanc, l'Ordre des médecins « exprime la nécessité d'une régulation » mais pas nécessairement celle « d'épaissir les volumes du Dalloz sur le droit de la santé », a indiqué le Dr Jacques Lucas, vice-président du CNOM lors du colloque.
L'Ordre fait des propositions pour « définir un cadre du bon usage » de ces outils, alors que les patients sont précisément « en attente de conseils de la part de leurs médecins » sur ces nouveaux objets.
Autre proposition de l'Ordre, l'instauration d'une régulation « adaptée, graduée et européenne » pour ces outils avec comme « minimum » l'obligation d'une « déclaration de conformité à un certain nombre de standards ».
Une telle déclaration devrait porter au moins sur la confidentialité des données recueillies, sur la sécurité informatique et sur la sûreté sanitaire de l'outil en question, selon l'Ordre.
La sécurité et la confidentialité des données sont un point clé dans le domaine de la santé connectée puisque ces outils sont capables de dialoguer avec un téléphone portable ou un site internet dédié.
En France, il est interdit de collecter des données personnelles comme celles liées à la santé, sans l'accord de la personne concernée. La vente de données de santé nominatives est également prohibée.
L'Ordre « appelle à un usage responsable et pragmatique de la santé connectée » et « souhaite que les questions éthiques soulevées par ces technologies donnent lieu à des débats publics ».

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.notretemps.com/internet/objets-de-sante-connectes-l-ordre-des,i78194

---

# 2020 : 1% des objets connectés seront des…voitures

## 2020 : 1% des objets connectés seront des…voitures

**Les équipements sans fil s'immiscent dans les véhicules. En 2020, 250 millions de voitures seront connectées au réseau avertit le Gartner. Un véritable écosystème est en train de se créer sur ce mouvement.**

En 2020, 250 millions de voitures connectées parcourront les routes du monde avertit le Gartner. Dans les 5 années qui viennent, les nouveaux véhicules équipés de capacités de conduite automatique vont devenir un segment majeur de l'Internet des objets, assure le cabinet d'étude.
Cette année, le Gartner prévoit unparc de 4,9 milliards d'objets connectés, en croissance de 30% par rapport à 2014. En 2020, il devrait y avoir 25 milliards d'objets connectés. Les voitures connectées devraient donc représenter 1% des objets connectés dans 5 ans.

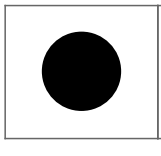
**Un levier de croissance économique**
« La voiture connectée est déjà une réalité, et la connectivité sans fil dans les véhicules est en expansion rapide, des modèles de luxe et des marques haut de gamme, au modèles de milieu de gamme » explique James F. Hines, du Gartner. L'Idate confirmait déjà cette tendance en juin dernier.
Par ailleurs, la prolifération de la connectivité automobile doit avoir des implications majeures sur des secteurs tels que la télématique, la conduite automatique, ou encore la mobilité, assure le Gartner.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/2020-1-des-objets-connectes-seront-desvoitures-39813698.htm

---

# Les données de santé et les objets connectés seront dans la ligne de mire des cybercriminels en 2015



Les données de santé et les objets connectés seront dans la ligne de mire des cybercriminels en 2015

**« 2014 a été une année riche en innovations. L'apparition des vêtements connectés et le développement de l'Internet des objets retiennent bien sûr toutes les attentions et promettent une année 2015 tout aussi riche. Il reste pourtant toujours une ombre au tableau : la cybercriminalité. Nos données personnelles sont plus exposées que jamais et les gouvernements ne semblent pas décidés à mettre en vigueur les lois pour y remédier. »**

**2014, une année faite de hauts…**

« En 2014, Le Cloud et les technologies mobiles ont contribué à rendre nos vies plus faciles, plus productives et plus agréables. Quant aux appareils mobiles, ils représentent aujourd'hui plus de 30 % du trafic Internet, soit deux fois plus qu'il y a 18 mois.

Les technologies mobiles elles-mêmes continuent d'évoluer. Je pense notamment aux vêtements et aux accessoires connectés, comme les Google Glass ou les montres. Mais aussi tendance soient-elles, ces technologies ne sont rien comparé au Cloud. Plus de 90% des entreprises et 90% des internautes comptent désormais sur le Cloud pour disposer d'un accès facile, abordable et permanent à leurs données et leurs services favoris. Internet n'est plus un moyen de connexion à l'information, mais bien le lieu où on la stocke. »

**… Et de bas !**

« Malheureusement, innovations et risques sont indissociables. On a pu s'en rendre compte avec la succession d'attaques informatiques de grande envergure qui ont touché les entreprises de tous les secteurs cette année.

Nos adversaires ne sont plus seulement des criminels et des hacktivistes. La sophistication et le nombre croissants d'attaques sont autant d'indices qui pointent du doigt les Etats, nouveaux acteurs de la cyberguerre. Et ces pratiques douteuses ont commencé à provoquer des crises diplomatiques dans le monde réel. Je pense notamment aux tensions qui se sont accentuées entre les États-Unis et la Chine.

Quelques gouvernements à travers le monde tentent d'endiguer le phénomène mais rares sont les progrès qui valent la peine d'être mentionnés. Les révélations d'Edward Snowden en 2013 ont continué de polariser le débat sur la vie privée et de freiner les efforts législatifs, pourtant nécessaires. Dans ce contexte, que pouvons-nous prévoir en 2015 ? »

Les cyber-attaques au niveau national continueront d'évoluer et d'augmenter, mais les dommages seront davantage supportés par le secteur privé

« En 2014, des états du monde entier ont repoussé les limites acceptables de la cyber-attaque pour contrôler leurs propres populations et espionner d'autres états. Parce que personne ne s'est attelé activement au développement de normes de comportement numérique acceptables – une Convention de la Haye ou de Genève du numérique pour ainsi dire – nous pouvons nous attendre à ce que cette guerre numérique secrète se poursuive. Cependant, les sociétés du secteur privé seront de plus en plus souvent entraînées dans cette guerre soit en tant que victime visée soit en tant qu'instrument involontaire d'une attaque contre d'autres sociétés. »

**Le débat sur la vie privée va mûrir**

« Nous commençons à constater un assouplissement de l'actuel environnement polarisé aux États-Unis et en Europe au fur et à mesure que les gens comprennent que leur vie privée est attaquée et défendue par un ensemble d'acteurs plus varié et complexe que les débats actuels ne le porteraient à croire. L'idée s'impose que la vie privée n'est pas un concept monolithique et qu'elle ne peut pas survivre indépendamment de la sécurité. Un débat plus pragmatique et équilibré sur la manière de sécuriser notre vie privée se poursuivra en 2015 et les perspectives de voir une politique de protection de la vie privée et une législation sur le partage du renseignement susceptibles de mieux nous protéger pourraient s'éclaircir. Cette prédiction se vérifiera si la Réglementation générale sur la protection des données de l'EU, qui devrait être finalisée 2015, entre en vigueur. »

Le secteur de la distribution est la cible actuelle et les renseignements personnels sur la santé (RPS) sont dans le collimateur

« Suite aux nombreuses failles dans le secteur de la distribution et des services financiers en 2014, les entreprises qui gèrent les données des cartes de paiement renforcent leurs défenses et réduisent la fenêtre d'opportunité pour les cybercriminels, ce qui les rend moins lucratives en tant que cibles. Malheureusement, le secteur de la distribution est massif et d'envergure mondiale, et il continuera à être un environnement riche en cibles. En 2015, toutefois, les cybercriminels bien organisés se tourneront de plus en plus vers le vol d'un autre type de données moins bien sécurisées, très lucratives à monétiser dans l'économie du cyber-crime, et largement détenues par des entreprises ne disposant pas de moyens de défense contre les attaques sophistiquées : les informations personnelles détenues par les prestataires de services de santé. Hélas, il est probable que nous assistions à une autre série de hacks tant que les fournisseurs n'auront pas renforcé leur sécurité pour lutter efficacement contre ces menaces. »

L'identité des objets (connectés)

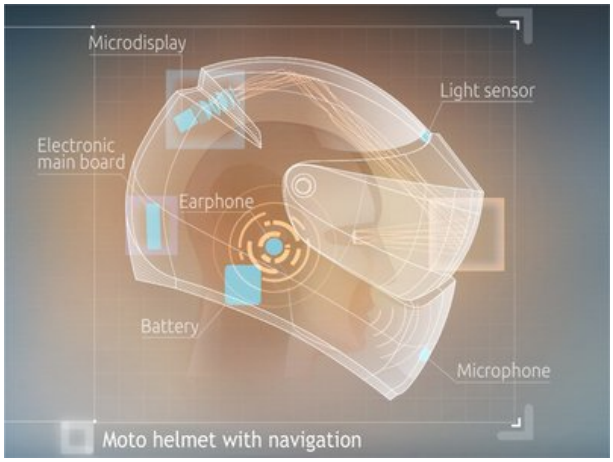
« Malgré le battage autour des vulnérabilités des logiciels et des systèmes, elles deviennent moins lucratives pour les criminels que l'ingénierie sociale et d'autres « trust exploits » plus faciles à exécuter. J'ai lu cet année un tweet qui disait à peu près ceci : « pas besoin de Zero Days quand on a la stupidité ». L'accentuation de l'interaction homme-machine et machine-machine ne fera qu'aggraver cette situation. De ce fait, l'authentification et la gestion des identités des personnes et des objets connectés qui accèdent à nos réseaux et nos données, seront un élément de sécurité de plus en plus critique en 2015. Tenez-vous prêt pour le Botnet des objets. Si l'on considère cette tendance, la forte croissance de l'Internet des objets dans le secteur de la santé, et ma prédiction sur les renseignements personnels sur la santé (RPS), les ramifications sont vraiment effrayantes.

Bien que nous ayons assisté à un changement à la présidence du Sénat de États-Unis, je ne suis pas optimiste quant aux chances de voir évoluer les projets de législation sur la cyber-sécurité en 2015. Bien que cette question soit d'une importance critique pour l'avenir de toutes les nations, elle est complexe et les avancées seront difficiles dans le climat géopolitique actuel. En l'absence de législation complète, les régulateurs de l'industrie interviendront pour combler le vide en créant une mosaïque de nouvelles exigences de conformité potentiellement incompatibles (hélas…) »

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.globalsecuritymag.fr/Art-Coviello-Executive-Chairman-de,20150107,49869.html

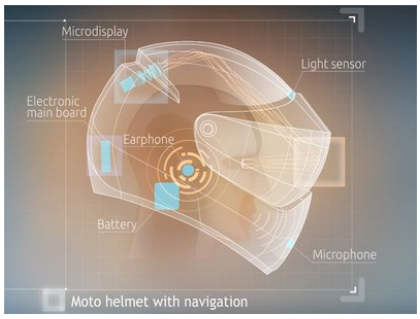
# Un casque moto connecté à réalité augmentée prévu pour cet été




Un casque moto connecté à réalité augmentée, prévu pour cet été

**La société russe Livemap annonce avoir levé 300 000 dollars pour commercialiser son produit phare. La sortie de son casque de moto affichant des éléments visuels sur la visière du conducteur est prévue pour cet été.**

La société russe Livemap développe un produit très particulier pour les conducteurs de deux-roues. Il s'agit d'un casque intégrant plusieurs technologies comme la réalité augmentée ou encore, le contrôle de services grâce à la voix. Le dispositif peut se relier au GPS et afficher un itinéraire sur la visière du conducteur.




Après avoir développé de premiers concepts, la start-up indique que son produit est désormais prêt à être commercialisé. Elle précise au site américain Techcrunch avoir levé la somme de 300 000 dollars auprès du ministère des Sciences de Russie, afin de procéder à la mise sur le marché de son dispositif.
Grâce à ces fonds, Livemap indique s'être notamment concentrée sur le dispositif permettant de projeter des images sur la visière. Son dernier prototype devrait être présenté au printemps prochain, pour une commercialisation au trimestre suivant.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://pro.clubic.com/actualite-e-business/investissement/actualite-746953-casque-moto-realite-augmentee-levee-fonds.html
Par Olivier Robillart

# BYOD : la surveillance de l’employé peut mener à un licenciement

BYOD : la surveillance de l’employé peut mener à un licenciement

**Dans le Bring Your Own Device (BYOD), le respect de la vie privée est un point majeur. Néanmoins, l'employé doit aussi comprendre qu'utiliser son propre appareil peut avoir des conséquences importantes.**

**Des licenciements aux raisons diverses mais toutes liées au BYOD**

Nous ne cessons de le répéter ces dernières années : si le BYOD consiste à apporter son appareil personnel au travail, cela implique aussi que le travail s'introduit dans l'appareil personnel. Outre des applications ou encore des données professionnelles, on retrouve aussi des systèmes de surveillance. Qui plus est, certaines politiques de BYOD sont très strictes et impose de s'y conformer à la lettre, sans quoi les répercutions peuvent être irréversibles.

Prenons quelques exemples concrets. Selon CIO, une banque située à New York a dû licencier plusieurs de ses cadres pour une raison d'une grande simplicité : ils n'avaient pas signalé la perte de leur smartphone dans les 24 heures. La politique de BYOD de la firme était pourtant claire sur ce point…

Autre exemple, un responsable des technologies de l'information et de la communication d'un cabinet d'avocats californien savait systématiquement qu'un des employés filait en douce pour aller… jouer au golf. Malheureusement pour lui, cet avocat joueur était surveillé par la géolocalisation de son smartphone contrôlée par son entreprise.

**Le contrôle de l'appareil en question**

Dans les 12 points à traiter pour une bonne politique de BYOD, la question des données personnelles s'était posée. La séparation entre données privées et professionnelles est en effet capitale pour éviter tous malentendus. Néanmoins, cela n'empêche pas que quoi qu'il arrive, l'entreprise peut avoir des informations sur ses employés. Et c'est bien normal. Dès lors que l'employé utilise son appareil au travail, la direction se doit de disposer d'un minimum de contrôle sur cet appareil. Mais quelle est la limite à cette mainmise ?

En février dernier, ZDNet avait publié un article centré sur la réticence des employés à ce que leur direction contrôle tout. Une hésitation elle aussi légitime, car le fait d'apporter son appareil personnel au travail ne signifie pas que l'on souhaite que tout le monde sache que l'on a une maladie, des vices cachés et autre jardin secret. Tant que cela n'influe pas sur la qualité du travail, cela va sans dire.

La problématique de la surveillance n'en reste pas moins réelle, et plus aujourd'hui encore qu'hier. La généralisation du paiement sans contact, via Apple Pay notamment, est un bon exemple. De nombreux employés aux États-Unis se demandent si ce système de paiement n'est pas trop intrusif du fait du BYOD, dès lors que la compagnie pourrait savoir tout ce que le salarié achète. Du papier toilette aux céréales, en passant par le sex toy…

**Un équilibre à trouver entre Big Brother et liberté totale**

Savoir où l'on va partout et tout le temps, savoir ce que l'on télécharge, voire savoir ce qu'on achète. Le BYOD rimerait-il avec Big Brother ? Non, bien entendu, tout du moins, pas forcément. Tout dépend déjà de la politique de BYOD mise en place par l'entreprise. À l'employé de la consulter attentivement afin de connaître les limites ou non de cette politique. À lui de vérifier quelles sont les informations connues et inconnues. À lui de se renseigner sur ce qui est partagé ou non, et avec qui précisément.

Avoir une politique de BYOD rigoureuse mais juste est important pour n'importe quelle entreprise. Dans le cas contraire, cela risque de faire fuir les employés, qui ne supporteront plus d'être dans 1984. Alors que le BYOD pousse déjà les salariés à en faire plus et à travailler les soirs et les fins de semaine (ce qui n'est bon ni pour l'employé ni même pour l'entreprise à long terme), il ne faudrait pas non plus rendre paranoïaque les employés avec une surveillance abusive.

Le BYOD implique un respect mutuel : respect des données professionnelles de la part du salarié, respect de la vie et des données privées de la part de l'entreprise. Cela peut éviter bien des tracas, que ce soit des plaintes pour intrusions dans la vie privée, des situations gênantes suite à la divulgation d'informations personnelles, ou même le burn-out, qui touche un nombre grandissant d'employés stressés et surchargés. Le BYOD doit être avantage, et non un problème.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

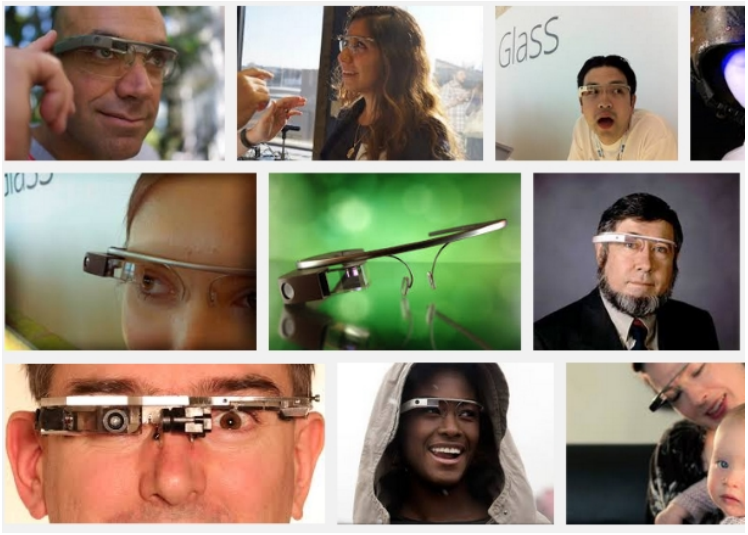
Source : http://www.zdnet.fr/actualites/byod-la-surveillance-de-l-employe-peut-mener-a-un-licenciement-39810793.htm
Par Nil Sanyas

# Objets connectés : le bling-bling, c’est presque fini

| | |
|---|---|
| | Objets connectés : le bling-bling, c’est presque fini |

**Demain, 30% d'entre eux seront camouflés. Lentilles de contact, bijoux, lunettes ; l'objet connecté ira vers plus de sobriété, et pourquoi pas plus de style.**

Et si les objets connectés étaient trop…voyants ? Certes, porter des Google Glass permet pour beaucoup d'affirmer de leur technophilie, et leur singularité. Et ils sont nombreux ; communicants, journalistes IT, évangélistes et autres gourous à se prêter au jeu.
Mais sérieusement, qui pourrait endurer le port ostensible d'objets connectés au quotidien ? C'est pour cette raison qu'en 2017, 30% des objets connectés seront camouflés avertit le Gartner.




Source : Google images

« Les lentilles de contact sont un des projets en développement » explique Annette Zimmermann, directeur de recherche au Gartner. « Un autre objet intéressant qui émerge est la joaillerie intelligente. Il existe presque une douzaine de projets de financement collaboratifs en compétition dès à présent sur ce secteur, avec des capteurs placés dans les bijoux pour des alertes de communication ou des alarmes d'urgence ».

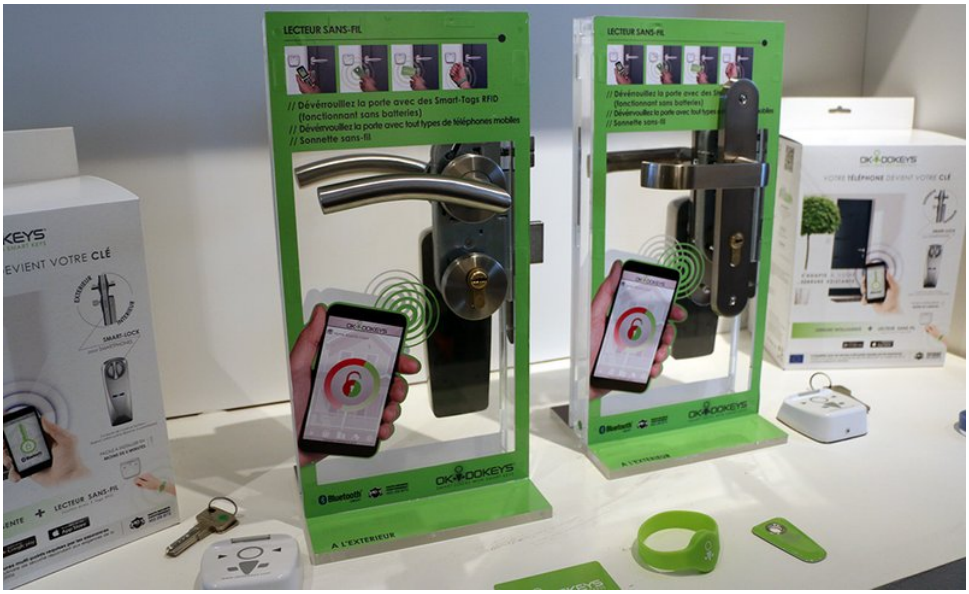
**« Le meilleur style est celui qui se fait oublier» Stendhal**
Certes, l'écrivain parlait littérature. Mais cela pourrait s'appliquer aussi aux objets connectés. Car au delà des nouveautés citées plus haut, les produits connectés déjà connus vont eux aussi aller vers une banalisation de leur apparence assure le cabinet d'étude. « Les objets connectés voyants qui sont déjà sur le marché, comme les lunettes intelligentes, vont évoluer vers de nouveaux designs qui camouflent totalement leurs composants technologiques » assure Annette Zimmermann.
A ce propos, Google a déjà amorcé la tendance en déposant un brevet de Google Glass plus discrète que la première version.

Reste que selon les estimations du Gartner, 70% des objets connectés continueront à être voyants. Parmi eux, les HMD (Head-Mounted Displays), de type Oculus Rift, dont plus de 25 millions d'unités devraient avoir été écoulés d'ici à 2018, toujours selon le Gartner.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/objets-connectes-le-bling-bling-c-est-presque-fini-39811115.htm
Par Guillaume Serries

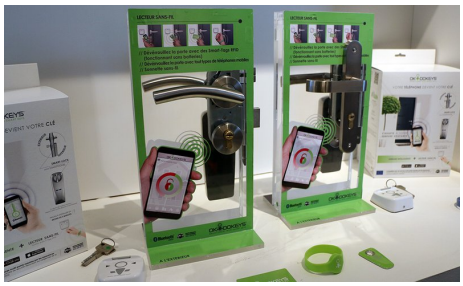
# Okidokeys : la serrure connectée à la française bientôt disponible




Okidokeys : la serrure connectée à la française bientôt disponible

**En vente depuis 6 mois aux Etats-Unis, la serrure connectée de l'entreprise française Okidokeys s'apprête à être commercialisée en Europe. Que se cache-t-il vraiment derrière ce produit, destiné à être installé très rapidement sur n'importe quelle porte ?**

Assez peu connue du grand public, l'entreprise française Okidokeys est pourtant l'une des pionnières en matière de serrure connectée. Il s'agit d'une filiale d'OpenWays, dont le cœur de métier cible, à la base, les hotels, dont certains utilisent depuis longtemps déjà des systèmes de clés électroniques pour l'ouverture des portes des chambres.
Okidokeys cible de son côté les particuliers désireux d'utiliser la ou les serrures de leur logement d'une autre manière, principalement avec un smartphone, mais pas seulement. Car la serrure connectée, si elle se présente sous une unique forme de base, peut être complétée par différents éléments qui permettent d'en renforcer l'usage.
La serrure en elle-même s'installe à l'intérieur du logement, sur une serrure déjà existante. La mise en place n'est censée prendre que quelques minutes, et tout le nécessaire, jusqu'au tournevis, est inclus dans la boîte. Certains impératifs doivent être vérifiés avant l'achat : la serrure de base doit notamment disposer impérativement d'un cylindre européen pour être compatible. L'épaisseur de la porte doit également être contrôlée.



**Le maître des clés**
« Par rapport aux serrures américaines, qui ont souvent de simples loquets, les serrures européennes ont été un défi » explique Pascal Metivier, le PDG d'Okidokeys. « La principale difficulté a été d'adapter le mécanisme qui ouvre la porte aux serrures 3 ou 5 points. » Les assurances demandent généralement la présence d'une serrure 3 points minimum pour la couverture d'un logement. La serrure d'Okiokeys est compatible avec ce type d'installation.
Concrètement, le « robot », une fois installé, agit sur le cylindre de la porte pour l'ouvrir ou la verrouiller. Le reste est essentiellement l'affaire de la connectique Bluetooth, qui permet de connecter un smartphone pour interagir avec la serrure. Tout est chiffré en 256 bits AES, une mesure de protection très répandue et efficace, assure l'entreprise. La clé de chiffrement est différente pour chaque serrure : pas de risque de voir sa porte ouverte par un voisin qui aurait le même modèle.
Différentes clés peuvent être programmées par le biais d'une interface Web, elle aussi sécurisée. L'administrateur peut autoriser, gratuitement, jusqu'à 10 personnes à accéder à jusqu'à 5 serrures. Des plages horaires et des jours peuvent être délimités, pour, par exemple, autoriser une femme de ménage à entrer seulement à certains moments.
Différents paramètres peuvent également être réalisés par le biais de l'application mobile, disponible sur iOS et Android. On peut, par exemple, autoriser temporairement l'ouverture d'une porte quand le smartphone en est proche : pratique quand on a les bras chargés. La serrure peut également se fermer automatiquement.
Bien évidemment, tout ceci n'empêche pas d'utiliser une bonne vieille clé manuelle, qui garde la priorité sur la serrure à l'extérieur. A l'intérieur, un loquet permet de fermer la porte à la main.


**RFID, NFC et CAC à la rescousse**
La serrure fonctionne à l'aide de 4 piles LR6, pour une autonomie d'un an. Lorsque les piles arrivent en fin de vie, le système le fait savoir 6 semaines à l'avance, et insiste de plus en plus pour qu'on les change, jusqu'à empêcher la fermeture électronique.
Le vrai risque question autonomie concerne davantage le smartphone : si on n'a plus de batterie et pas de vraie clé sur soi, comment faire ? Okidokeys a la réponse : il s'agit d'une sonnette connectée, qui dispose de plusieurs systèmes de lecture. Outre le NFC d'un téléphone, elle peut lire des puces RFID programmées à l'avance pour l'ouverture de la porte. Ces dernières sont disponibles sous la forme de cartes à mettre dans son portefeuille, de porte-clés ou encore de bracelets étanche. Une solution de secours, mais également de nécessité si on ne dispose pas d'un smartphone. En cas de perte, ces éléments peuvent être rapidement désactivés sur le site.
La sonnette connectée intègre également le système CAC, pour « crypto acoustic credential ». Ce dispositif, utilisé dans certains hôtels, permet d'utiliser un téléphone mobile « traditionnel » pour ouvrir une porte à l'aide d'une séquence sonore sécurisée. L'utilisateur reçoit un SMS avec un code, il doit ensuite appeler un numéro vert, qui va jouer un son pour la sonnette. Cette dernière est capable de l'interpréter, de le valider et d'ouvrir la porte si tout est en règle.

**Une ouverture à Internet**
A ce stade, tout se passe en local. Mais Okidokeys propose également un pack incluant un module, appelé Gateway, qui se connecte à une box et relie donc la serrure à Internet. Il est ainsi possible de savoir, en temps réel sur son smartphone, si la porte a été ouverte, et par quel moyen. La serrure intègre également une alarme, qui va retentir en cas d'entrée forcée. Là encore, l'administrateur est prévenu à distance, à condition de disposer de cette extension Internet.

Okidokeys dongle

On se retrouve donc face à trois solutions : la serrure de base, celle avec la sonnette et les tags, et celle qui permet, en plus du reste, de connecter le site à Internet. Tout ceci a un prix non négligeable : le premier pack est proposé au tarif de 250 euros, le second à 350 et le troisième à 450.

La démonstration d'Okidokeys est efficace et le système est convaincant. Néanmoins, il apparaît également destiné à des personnes qui ont un besoin important d'optimiser l'accès à leur logement. Si la démarche commence à avoir du sens dans un environnement familial – où les parents donneront des bracelets RFID aux enfants, par exemple – il en a presque encore plus dans le cadre d'une location mesurée, pour les adeptes de services de type Airbnb. Ce n'est d'ailleurs pas pour rien si l'interface en ligne passe en mode payant – 35 euros par an – si l'on désire enregistrer plus de 10 utilisateurs et plus de 5 serrures.

Les trois packs seront disponibles en France à partir du mois de janvier 2015.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.clubic.com/mag/maison-connectee/actualite-744009-okidokeys-serrure-connectee-francaise-disponible.html?estat_svc=s%3D223023201608%26crmID%3D639453874_775958436