DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

GÉNIAL! NOS OBJETS SONT CONNECTÉS!

Publié le 26 janvier 2017

Montres intelligentes, compteurs intelligents, lampes intelligentes… Même les emballages deviennent intelligents. « En réalité, il s'agit de ceux qui sont équipés de puces RFID, destinées à les localiser. Une technologie qui n'est pas vraiment récente », souligne le Pr Bruno Dumas, de l'Université de Namur.

Ce spécialiste des interactions homme-machine et de la manière dont l'expansion de l'informatique dans la vie courante influe sur nos usages, jette un regard à la fois technique, mais aussi plutôt philosophique sur cette évolution de la technologie « branchée ». « Je suis un informaticien qui applique des méthodes de la psychologie aux interfaces homme-machine », souligne-t-il.

Donner une intelligibilité aux objets connectés

Avec quatre milliards d'objets connectés dans le monde qui pourraient être 13,5 milliards d'ici 2020, faut-il craindre leur intrusion dans notre vie?

« Le problème ne se pose pas en ces termes, souligne le scientifique du Centre de recherche sur l'ingénierie des systèmes d'information de l'UNamur. "Ce qui compte aujourd'hui, c'est de comprendre et de faire comprendre à chaque utilisateur de ces objets comment ils fonctionnent et ce qu'ils peuvent réellement nous apporter comme avantages ou comme inconvénients. C'est d'abord une question d'éducation, de compréhension du système ».

« Avec les objets connectés, la complexité est particulièrement grande », précise le scientifique. « Ce qui peut être une source de frustrations pour l'utilisateur. La priorité est donc de donner à ces objets une certaine intelligibilité ».

DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

Une éducation à l'informatique à envisager dès l'école

Sans doute. Mais comment éduquer aux objets connectés, à leur système d'exploitation, aux réseaux, à la sécurité qui est liée à leur usage?

« L'effort devrait se situer au niveau de l'école », estime le Dr Dumas. Mais ici se pose alors la question du cours où ces matières devraient être abordées. L'informatique, est-ce des mathématiques, de l'histoire, de la géographie, de la philosophie? Sans doute un peu de tout cela. "Ce qui compte aujourd'hui, c'est de pouvoir instiller une véritable culture de l'informatique, afin de pouvoir effectivement en comprendre les enjeux et les grands modes de fonctionnement", dit-il.

Sans verser dans la paranoïa et l'éventuelle crainte d'une « révolte » des appareils connectés (« on en est loin", souligne Bruno Dumas, qui pointe les gigantesques problèmes d'interconnexion qui se posent à ces machines), il ne faut pas éluder les problèmes de sécurité de ces systèmes.

La sécurité, un maillon faible

« Les objets connectés posent en effet la question de la sécurité », souligne de son côté le Commissaire Bogaert, de la Police fédérale, auteur de « Surfons tranquille ».

« Prenons certaines caméras de surveillance qui transmettent leurs images par wifi par exemple. Leurs logiciels sont souvent obsolètes et rarement mis à jour. Elles constituent dès lors des portes d'entrée moins bien sécurisées aux systèmes informatiques que les ordinateurs qui les gèrent » indique le commissaire du Computer Crime Unit. « Des cas de piratages des réseaux, via les protocoles désuets des caméras de surveillance, ont défrayé la chronique ces derniers mois ».

Protection des données privées

Faut-il dès lors craindre les faiblesses de la connexion de notre brosse à dents intelligente? Va-t-elle ouvrir toute grande la porte de notre vie privée à la planète entière?

C'est toute la question de la protection des données privée qui est ici en jeu. « De nombreux appareils informatisés captent et conservent en effet une foule de données privées nous concernant : relations, emploi du temps, données médicales, etc. », note de son côté le Dr Pascal Francq, du Paul Otlet Institute

« Nos données se retrouvent d'abord sur nos appareils domestiques (ordinateurs, smartphones, domotique, etc.). Ces derniers sont généralement vulnérables. Leurs usagers et leurs concepteurs ne suivent que trop rarement les consignes de sécurité les plus élémentaires" .

DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

Des risques démultipliés par l'incompétence… des entreprises

« Les risques purement technologiques suffiraient déjà à alimenter les craintes les plus cauchemardesques. Mais la légèreté avec laquelle les différents acteurs s'emparent du sujet de la cybersécurité amplifie les dégâts potentiels ».

« Bien entendu le risque zéro n'existe pas. Cependant, je m'inquiète pour les entreprises produisant tous ces appareils connectés ou concevant ces nouvelles applications en ligne qui envahissent nos vies. Elles ne disposent en effet que très rarement de réels experts en sécurité informatique, un profil excessivement rare aujourd'hui. »

« Ce sont d'abord les entreprises «traditionnelles» qui se lancent dans les objets connectés. L'exemple de la voiture piratée l'illustre parfaitement. De plus en plus d'attaques par déni de service sont menées via des appareils ménagers comme des frigos connectés ».

« Mais je suis également préoccupé par les nombreuses startups numériques qui se créent chaque jour. Non seulement on y retrouve rarement des experts en cybersécurité, mais elles ne disposent généralement pas non plus des fonds nécessaires pour faire de cette dernière une priorité ».

« En fait, même pour les géants du numérique, il n'est pas certain que la sécurité soit forcément la priorité absolue. Leurs revenus, et donc leur développement potentiel, semblent plus liés aujourd'hui à l'exploitation des données disponibles plutôt qu'à la sécurisation de celles collectées ».

Reprendre en main son destin numérique

Pour contrer cette tendance, et tout comme le Pr Dumas, le Dr Francq propose de mettre l'accent sur l'éducation. « Un travail d'information m'apparaît ici comme essentiel. De nombreuses cyberattaques profitent en effet des lacunes des utilisateurs lambda : absence de logiciels antivirus, oubli de mises à jour, téléchargement de fichiers infectés, mots de passe faciles à découvrir, mauvaises configurations, etc. »

« Des internautes mieux conscientisés seraient aussi plus exigeants vis-à-vis des fournisseurs de services en ligne et d'objets connectés. En nous montrant intraitables en matière de cybersécurité, ces derniers seraient obligés, sous notre pression, à la prendre en considération dès la conception de nouveaux produits ».