Note numéro 2
mars 2014

Note du CREOGN

Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale

Observatoire FIC (CREOGN – CEIS)

« Quelle sécurité pour les objets connectés »

Mercredi 5 mars 2014 – Quartier des Célestins

Les objets connectés s'installent progressivement dans notre vie courante. Au nombre de 4 milliards actuellement, ils seront, selon certaines estimations, 50 milliards en 2020. Leur utilisation croissante dans la vie courante des individus aura des implications en matière de sécurité et de confidentialité des données échangées.

Objets connectés : expansion et menaces

Aujourd'hui, le grand public plébiscite les objets connectés dès lors qu'ils participent à des activités de loisir. Le « *fun* » est la motivation première des acheteurs d'objets high tech. La sécurité devient cependant un élément différenciant pour le consommateur. Cette dimension est désormais prise en compte par les concepteurs d'éléments électroniques qui, à l'instar de Intel, s'efforcent de l'intégrer dès le stade de la conception.

Cinq risques liés à la sécurité peuvent être identifiés. Le premier risque est économique. En effet, tout objet dont la sécurité prête à caution perd instantanément la confiance du public et, par la même occasion, ne se vend plus. Le second risque est un risque médical. Les appareils de santé connectés peuvent être la cible d'attaques malveillantes ou de bugs provoqués par des informations erronées reçues. Les appareils concernés peuvent alors mettre en péril la santé de leurs utilisateurs, voire même leur vie (par exemple s'agissant de stimulateurs cardiaques ou de pompes à insuline). Les données personnelles constituent la cible du troisième risque puisqu'un très grand nombre d'informations portant sur les activités des individus circuleront *de facto* sur les réseaux, les objets ne sollicitant pas forcément l'accord de leur propriétaire pour communiquer entre eux. Pourront ainsi être interceptées et exploitées des informations relatives aux déplacements, aux habitudes de consommation, à la santé... Le quatrième risque est celui des logiciels malveillants. Il se trouve amplifié car beaucoup d'objets utiliseront ou communiqueront avec un OS[1] embarqué et se trouveront exposés aux attaques de hackers. Enfin, le dernier risque est lié aux utilisateurs. Actuellement sous-éduqués sur les questions de sécurité informatique, ils ont des habitudes qui mettent en péril leur sécurité informatique, donc l'intégrité de leurs données personnelles.

Tous ces risques peuvent se concrétiser de manières diverses. Un logiciel espion, introduit dans le système d'exploitation d'une paire de lunettes connectée, peut permettre à un tiers d'accéder aux images capturées par celles-ci. Les télévisions connectées sont susceptibles d'être l'objet du même type de piratage (de manière discrète si le pirate prend soin d'éteindre le témoin de fonctionnement...). Les objets connectés pourront également recevoir des spams, comme nos boîtes mail actuelles. Les possibilités sont déclinables à l'infini.

1 OS : Operating system, ensemble des programmes qui dirigent les capacités d'un ordinateur. Par exemple, Linux, Android, Windows 8 sont des OS.

Les menaces sont d'autant plus prégnantes que, dès à présent, il est possible de trouver facilement par un moteur de recherche les objets connectés[2]. Sont ainsi accessibles des caméras de surveillance mais aussi des systèmes aussi divers que des centres de crémation ou des installations électriques.
Compte tenu de ces éléments, la société Mc Affee, propriété d'Intel, estime avoir quatre défis à relever. Le premier consiste à intégrer dès la conception des éléments de sécurité dans les composants produits par Intel. L'objectif est de sortir des lignes de fabrication des composants proposant d'emblée un haut niveau de sécurité. Le deuxième défi consiste à intervenir sur le partage d'informations. Il s'agit de donner aux objets une capacité à filtrer les demandes d'accès de manière à limiter les risques de piratage. Le troisième challenge est celui de la standardisation destinée à permettre à l'ensemble des objets connectés de se transmettre des informations de sécurité. Il s'agit de réagir le plus vite possible aux attaques identifiées avant qu'elles ne se propagent. Dans l'idéal, l'alerte doit se répandre plus vite que la menace. Enfin, le dernier défi est celui de l'éducation des consommateurs. Les comportements à risque doivent disparaître pour que les menaces diminuent. Ainsi, le consommateur doit comprendre qu'en téléchargeant des applications sur des sites peu sûrs, par exemple pour débloquer une console de jeux ou un téléphone portable, il n'est jamais certain de ce qu'il installe sur son ordinateur et les appareils périphériques.

L'enjeu des données personnelles

La protection des données personnelles connaît une véritable révolution en droit avec l'arrivée des objets connectés. En effet, si la loi Informatique et liberté de 1978 a déjà connu des mises à jour, de nouvelles règles européennes devraient voir le jour à l'horizon 2016. Il s'agit de prendre en considération la masse d'informations personnelles collectées par les objets de la vie quotidienne et exportées sur Internet et des serveurs divers. On sait qu'il est déjà possible de dessiner le profil d'un individu en récupérant ici et là les informations qu'il laisse volontairement sur Internet (il suffit de consulter Facebook pour constater cette réalité). Or les objets connectés non seulement collectent en permanence une multitude d'informations mais, de plus, les échangent avec d'autres objets ou des serveurs sans même que l'utilisateur en soit informé. Qui, aujourd'hui, se soucie par exemple de ce que son téléphone peut bien envoyer lorsque telle ou telle application est utilisée ? Demain, les spécialistes du « big data » pourront tirer de cette mine à ciel ouvert des portraits bien plus fins d'un individu. Ils apprendront tout des habitudes de consommation, des déplacements, des problèmes de santé rien qu'en interrogeant leurs moteurs de recherche spécialisés.

Par ailleurs, la loi de 1978 ne s'applique qu'au territoire français. Dès lors que les serveurs sont à l'étranger, il est difficile de connaître le niveau de protection offert par la législation locale aux données personnelles.

D'autre part, l'exception française d'usage personnel autorise l'utilisation domestique de certains systèmes. Dès lors que les objets connectés sont majoritairement utilisés dans un cadre privé, la protection des données par la CNIL ne peut pas s'appliquer... On peut observer également que nombre d'objets naviguent à la lisière du domaine médical, lequel bénéficie d'une forte protection juridique. Que penser en effet des balances connectées, des appareils de sport, des fréquencemètres destinés aux coureurs ou des fourchettes électroniques qui pèsent les denrées et mesurent le temps de mastication entre deux bouchées ? Ces appareils scrutent des données vitales mais échappent actuellement au

2 Voir sur ce point l'article du site vice.com (http://www.vice.com/fr/read/shodan-est-le-moteur-de-recherches-le-plus-dangereux-du-monde).

domaine de la médecine. Ce flou est savamment entretenu par les industriels qui ne veulent évidemment pas tuer la poule aux œufs d'or. En effet, des données de santé ne peuvent être hébergées que sur un serveur agréé, avec des contraintes fortes d'identification pour y accéder. Autant d'obligations qui impliquent des coûts élevés et viennent grignoter les bénéfices. La Food and Drugs Administration[3] américaine a publié un guide sur ces questions, classant les dispositifs connectés en trois catégories. La première regroupe les dispositifs médicaux, la seconde les dispositifs sans lien avec les questions de santé, la troisième recevant quant à elle les appareils sur lesquels la FDA n'a pas d'avis tranché. Ces derniers, qui sont provisoirement considérés comme sans lien avec la santé, peuvent basculer sans préavis dans l'une ou l'autre des deux autres catégories. Sur ces questions, l'administration américaine est donc particulièrement prudente et attend, pour se prononcer, de disposer d'informations complémentaires.

Conclusion

La question de la protection des données personnelles nécessite une attention permanente des autorités. Le droit international en la matière ne donne pas vraiment d'assurances comparables à celles du droit français. Par ailleurs, la mondialisation rend la réflexion complexe. A titre d'illustration, le constructeur de matériel informatique chinois Huawei fait 70 % de chiffre d'affaire à l'étranger. Or le droit chinois est inexistant s'agissant de la protection des données privées. D'autre part, 32 % des composants utilisés viennent des États-Unis, pays qui s'est très récemment illustré dans la collecte internationale et clandestine de données personnelles. Autant d'informations qui invitent pour le moment à considérer avec prudence l'utilisation des moyens connectés, particulièrement pour la conservation d'informations confidentielles et personnelles.

3 Administration des produits alimentaires et médicamenteux.