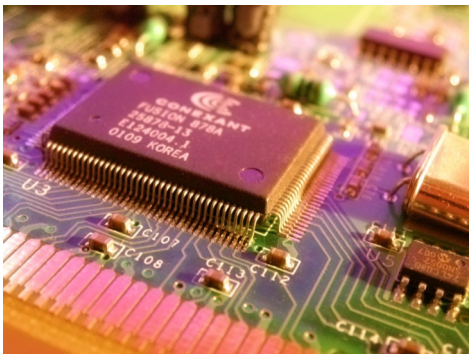
Une invasion de puces… électroniques
RFID : libertés individuelles menacées

Chats, chiens, chevaux, cartes bancaires, cartes Vitale, badges, passeports, cartes d'accès aux transports, livres de bibliothèque, télépéage, forfaits de ski, gestion de vélo ou auto-partage, bientôt le permis… La puce, non pas l'ectoparasite mais bien l'électronique, fait partie du quotidien depuis un moment déjà. Son utilisation s'intensifie et se banalise. Le fait qu'elle facilite la vie est indéniable, mais… sans risques ?



La puce « Radio Frequency IDentification » ou RFID (en français, Identification par radiofréquence) est presque « magique », et à plusieurs niveaux. Comme elle est munie d'un microprocesseur et d'une antenne, les informations qui y sont contenues peuvent être lues à distance par fréquence, grâce à une antenne. Pour les industriels, la puce placée sur les produits permet de suivre ceux-ci, de leur fabrication jusqu'à leur vente, et offre une protection antivol plus efficace qu'un code-barre : économique. Pour le consommateur, les badges et pass de métro ou autre transport dit « sans contact » font gagner du temps : pratique.

On imagine déjà munir les vêtements de ce type de puce : une machine à laver révèlerait alors sa composition textile et recommanderait un certain degré et temps de lavage. De même qu'un réfrigérateur pourrait indiquer que tel ou tel produit a dépassé sa date de péremption.

Bientôt, plus besoin de vider son chariot aux caisses, un lecteur analysera automatiquement les RFID des produits choisis et en fera la facture. Les débuts de cette prouesse technologique remontent aux années 1940 : les avions amis ou ennemis étaient ainsi repérés durant la guerre. La puce a ensuite servi pour suivre le bétail, les voitures. Puis les aliments, les médicaments, les livres de bibliothèque, les animaux domestiques... Bientôt les humains ?

Voulons-nous être « RFIDisés » ?

Déjà, la ville de Mexico en a implanté sous la peau de ses officiers de police, pour contrôler l'accès aux bases de données et mieux les localiser en cas de kidnapping. À Barcelone, Conrad Chase, directeur de la boîte de nuit du Baja Beach Club, offrait à ses clients VIP ces mêmes puces, avec une fonction porte-monnaie. Des puces de la taille d'un grain de riz, dans lesquelles on peut mettre des informations, en retirer, en ajouter, en modifier. Des puces de plus en plus indétectables qui suivent, pistent, détectent, contrôlent, surveillent leur propriétaire. Des puces qui inquiètent les défenseurs des droits de l'Homme et des libertés individuelles.

Jean-Claude Vitran, membre du Comité central de la Ligue des Droits de l'Homme et du citoyen (LDH) et responsable du groupe de travail « Libertés et technologies de l'information et de la communication », mettait en garde contre l'utilisation des puces RFID dans un article paru fin 2009 [(1)], au commencement de la campagne « Urgence pour les libertés ! Urgence pour les droits ! » : « *À l'évidence, cette révolution technologique, croisée avec les nanotechnologies dont les scientifiques disent qu'elles seront la prochaine révolution industrielle et bouleverseront notre environnement, pose la question du respect de la vie privée et des droits fondamentaux. En effet, le citoyen est en droit de s'imaginer que, porteur de vêtements et de chaussures " RFIDisés ", il pourrait ensuite être tracé en permanence par des lecteurs judicieusement placés dans des lieux de passages obligés – transports publics, notamment* ».

Le 30 octobre 2005, soit quatre ans auparavant, Philippe Lemoine, commissaire de la Commission nationale de l'informatique et des libertés (CNIL), alertait déjà sur les pièges qui concourent à minorer le risque que présente la radio-identification : « *L'insignifiance [apparente] des données, la priorité donnée aux objets [en apparence toujours vis-à-vis des personnes], la logique de mondialisation [normalisation technologique basée sur un concept américain de " privacy " sans prise en compte des prin-*

[(1)] – « RFID : vers un traçage généralisé ? », Ligue des Droits et l'Homme et du citoyen (LDH), *Hommes & Libertés* n° 148 d'octobre, novembre et décembre 2009.

cipes européens de protection de la vie privée] et enfin le risque de " non-vigilance " individuelle [présence et activation invisibles] ».

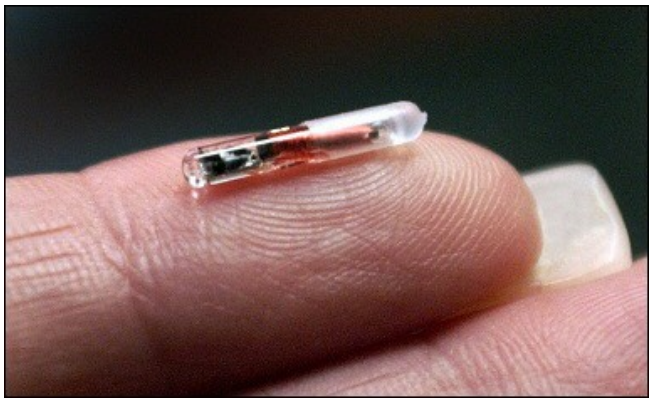
La solution du micro-ondes

Car si des sociétés comme Applied Digital Solutions, laquelle produit et commercialise les puces de la marque Verichip, présentent la puce électronique comme l'outil bientôt indispensable non seulement à la médecine, aux entreprises, mais bientôt à tout être humain, le revers de la médaille pour les libertés individuelles est sérieux. Dans son article, Jean-Claude Vitran rapporte les inquiétudes de la CNIL qui estime que *« ces technologies de radio-identification permettent le profilage des individus et font, par conséquent, peser un risque particulier sur les libertés »*. Selon la CNIL, « *la solution consisterait à neutraliser la puce RFID une fois l'objet acheté* ». Neutraliser une puce électronique ? Possible grâce au « RFID Zapper » qu'on peut trouver sur Internet ou dans des boutiques spécialisées : en générant un champ électromagnétique puissant de courte portée, il désactive de façon permanente la puce qui a alors reçu un choc électrique. Possible également en faisant cuire la puce quelques minutes au micro-ondes, mais cette seconde solution paraît peu recommandée si la puce se trouve sur des chaussures ou sous la peau !

Pourtant, les dangers sont réels : les puces peuvent facilement devenir la cible des hackers [(2)]. Adam Laurie, chercheur indépendant britannique spécialisé dans les systèmes de sécurité, l'a démontré lors de la ShmooCon Convention [(3)] de Whashington en 2007. Il a pu pirater la puce RFID d'un membre de l'assistance que ce dernier utilisait pour déverrouiller son ordinateur portable. Adam Laurie a ainsi accédé au contenu de l'ordinateur en question et a pu en fournir les identifiant et mot de passe à l'assemblée. Son objectif était de mettre en garde des responsables scolaires californiens qui souhaitaient que leurs étudiants soient munis de ces mêmes puces placées sous la peau.

Cheval de Troie ou virus

De la même façon, un autre hacker préventif, Jonathan Wasthues, a piraté l'accès au siège des députés en Californie en septembre 2010. Joe Simitian, sénateur démocrate de Californie à l'origine de cette intervention, déclarait : « *Si vous pouvez lire les informations d'une personne à distance de quelques mètres, puis en l'espace d'une poignée de secondes cloner sa carte et vous faire passer pour lui, imaginez un peu les méfaits possibles* ». Et d'autres hackers d'informer que pour moins de 200 dollars US, soit moins de 145 euros, il est possible d'acquérir le matériel nécessaire pour pirater ces puces.



Possible aussi d'y introduire un cheval de Troie ou un virus – informatique – [(4)], comme l'a fait en mai 2010 Mark Gasson, chercheur du groupe de recherche d'intelligence cybernétique, laboratoire de l'université de Reading au Royaume-Uni. Après s'être implanté une puce en 2009 avec laquelle il pouvait ouvrir des portes soi-disant sécurisées, il y a importé un virus et contaminé les ordinateurs de l'université. « *Nos recherches montrent que les technologies implantables se sont développées au point que ces implants sont désormais capables d'échanger des données, de les stocker et de les manipuler* ». Une généralisation cependant inévitable, et selon lui bénéfique, d'un point de vue médical notamment, puisque la puce pourrait fournir toutes les indications de santé d'un patient sans exception, permettant alors de pouvoir mieux le soigner.

L'Union européenne réagit

La technologie RFID est donc une avancée certaine, indéniablement spectaculaire. Mais son utilisation possible reste une menace liberticide non négligeable, malheureusement peu prise en compte malgré les alertes lancées par des spécialistes. Bien sûr, il existe des lois pour éviter ce type de dérives : au niveau européen, les informations collectées ou stockées via des solutions RFID sont soumises aux règles d'une directive datant de 1995, selon laquelle la collecte de données personnelles doit avoir un objet précis et ne doit concerner que les informations pertinentes ; en outre, la durée de conservation des données doit être justifiée par rapport à la réalisation de cet objet. Mais cette directive ne précise pas le « champ » des données personnelles ni qui peut contrôler ces données, ce qui laisse libre cours aux interprétations que peut en faire chaque pays membre de l'Union européenne, et crée des zones d'ombre dommageables. La Commission européenne a donné ses recommandations sur l'utilisation du RFID le 12 mai 2009. Des études sont lancées, mais les

[(2)] – De l'anglais signifiant « bricoleur, bidouilleur ». Employé en informatique pour désigner les programmeurs astucieux et débrouillards, possesseurs de connaissances techniques poussées qu'ils utilisent pour améliorer des systèmes, innover dans le domaine des nouvelles technologies. Différent du « cracker » (pirate), qui utilise ses capacités pour nuire.
[(3)] – Convention du piratage connue des hackers de la côte Est américaine.
[(4)] – Un cheval de Troie est un logiciel d'apparence légitime conçu pour exécuter subrepticement des actions à l'insu de l'utilisateur. Un virus est un logiciel conçu pour se propager en s'insérant dans des programmes légitimes appelés « hôtes », et qui perturbe le fonctionnement de l'ordinateur infecté.

décisions politiques restent assez peu efficaces et prises à un rythme dérisoirement lent comparé à la vitesse exponentielle à laquelle se développe l'industrie de la RFID.

Il faut dire que si les libertés individuelles paient le prix fort face à la banalisation de ces puces, le marché, lui, ne connaît pas la crise et se porte même à merveille. D'après une étude [(5)], soutenue par le ministère de l'Enseignement supérieur et de la Recherche, intitulée « L'Internet des Objets : quels enjeux pour les Européens ? », parue en octobre 2008, « *les estimations du marché des solutions RFID varient (…) de quelques centaines de millions à plusieurs milliards d'euros* ». Selon Vandagraf International, société américaine d'études de marché, la valeur du marché des étiquettes RFID devrait même dépasser les 36 milliards de dollars US, soit plus de 26 milliards d'euros, en 2015 (les chiffres incluant également les lecteurs et le matériel, logiciels et services intégrés). En termes de volume, la société estime qu'on pourrait trouver 1 000 milliards de puces RFID sur le marché d'ici quatre ans. Difficile de freiner un marché si fructueux. Plus facile, par contre, d'outrepasser les libertés individuelles.

[(5)] – « Gouvernance Internet : la construction démocratique des normes », étude menée par Pierre-Jean Benghozi, directeur de recherche au Centre national de la recherche scientifique (CNRS), Sylvain Bureau, chercheur associé au Pôle de recherche en Économie et gestion du CNRS, et Françoise Massit-Folléa, responsable scientique du programme Vox Internet II.