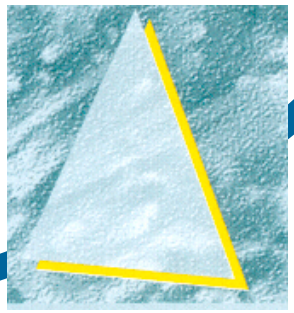
NOTES ÉDUCATION PERMANENTE
N° 23 - DÉCEMBRE 2006

ASSOCIATION POUR UNE
FONDATION TRAVAIL-UNIVERSITÉ
CHAUSSÉE DE HAECHT, 579 – B-1031 BRUXELLES
RUE DE L'ARSENAL, 5 – B-5000 NAMUR
ÉDITEUR RESPONSABLE : PIERRE GEORIS

HTTP ://WWW.FTU.BE



L'INVASION DES PUCES COMMUNICANTES

Enjeux sociétaux des technologies RFID

On en trouve dans des clés de voiture, des étiquettes de produits, des cartes de parking, de bibliothèque ou de centre sportif, des marqueurs pour animaux, bientôt dans les passeports. Appelées RFID, ces puces électroniques de nouvelle génération ont la particularité de communiquer à distance avec des détecteurs. Porteuses de données tantôt anodines, tantôt sensibles, elles envahissent notre vie quotidienne, souvent à notre insu. Quels sont les enjeux de société liés à la diffusion de cette nouvelle technologie ?

Les termes étiquettes communicantes, tags ou puces émettrices désignent des dispositifs d'identification à radiofréquence (*RFID, radiofrequency identification device*). Ces nouveaux objets techniques consistent en une puce munie d'un processeur, d'une mémoire et d'un émetteur radio (voir fiche technique en fin de document). Souvent miniaturisés, les dispositifs RFID sont destinés à s'intégrer dans d'autres objets ou dans des êtres vivants, pour interagir avec leur environnement. Quatre grandes catégories d'usages peuvent être distinguées : l'étiquette communicante; l'identifiant personnel; le traceur; le capteur d'informations.

A
ÉTIQUETER

L'étiquette communicante est actuellement l'usage le plus prometteur sur le plan économique, notamment dans la logistique et la grande distribution. L'étiquette RFID succède ici au code à barres, avec des performances accrues. L'étiquette identifie chaque produit individuellement, alors que le code à barres n'identifiait que la catégorie. Quand un magasinier passe une palette ou le consommateur un caddie sous un portail de détection, toutes les étiquettes sont scannées en une fraction de seconde et les bases de données sur les produits sont mises à jour. Les étiquettes RFID peuvent également servir à la sécurisation d'objets (antivol) ou au suivi d'animaux domestiques ou d'élevage.

C'est d'abord dans la logistique que les étiquettes RFID ont été mises au banc d'essai, car elles permettent des gains de productivité considérables dans la gestion des flux et des stocks, à condition que les logiciels de gestion des données soient capables de suivre les performances du matériel. Les applications dans la grande distribution n'ont pas encore atteint le seuil de maturité qui permettrait leur diffusion à grande échelle; elles restent limitées à quelques points de vente expérimentaux – bien que Wall-Mart, le leader américain des hypermarchés, utilise intensivement la RFID. Les difficultés de normalisation et d'interopérabilité constituent encore un frein à la diffusion de l'étiquette communicante. L'acceptabilité de ce changement technologique par les consommateurs ne semble pas problématique tant que les étiquettes RFID

n'enregistrent que les produits, sans couplage avec un identifiant personnel.

B

IDENTIFIER

L'identifiant personnel RFID présente en effet un profil plus critique. Dans le cas de l'hypermarché, le couplage entre une carte RFID du consommateur et les étiquettes communicantes peut déboucher sur le profilage, le ciblage des publicités, le contrôle des situations d'endettement. Wall-Mart a ainsi expérimenté un audioguide qui suggère au consommateur les achats à faire en fonction de ses préférences, de son budget et du stock disponible.

Une puce RFID identifiante permet également de stocker des données biométriques, comme des photos ou des empreintes digitales. C'est le cas du passeport biométrique, ou encore de certains systèmes de sécurité qui sélectionnent l'accès individuel à des locaux ou à des équipements.

Lorsque des données personnelles sont incorporées dans une puce RFID communicante, elles relèvent de la législation sur la protection des données et de la vie privée, sous deux aspects : le respect du caractère privé des données d'une part, la sécurité d'accès par rapport à des tiers, éventuellement malveillants, d'autre part. Les questions de sécurité, de fiabilité et de transparence des identifiants RFID requièrent une évaluation approfondie du point de vue juridique, éthique, politique et social, comme on le verra plus loin.

Toutefois, de nombreux usages actuels des identifiants RFID sont moins complexes et moins risqués: les cartes de parking, les skipass, l'accès à des installations sportives ou à des bibliothèques, etc.

C

SUIVRE À LA TRACE

Une troisième catégorie d'usages concerne le traçage des déplacements, pour autant que les puces émettrices aient une portée suffisante. Les systèmes les plus élémentaires concernent le suivi des colis ou des bagages, la localisation d'objets ou de véhicules, le télépéage sur autoroute. Des logiciels peuvent assurer une sorte de communication directe entre objets, par exemple entre un colis, sa palette, son camion et sa destination. Par ailleurs, la combinaison de l'identification et du traçage peut permettre d'effectuer des contrôles individualisés, par exemple en suivant à la trace les déplacements et les contacts des employés dans une entreprise. Ici encore, c'est la combinaison de données sur les objets et de données sur les personnes qui soulève de nombreuses incertitudes juridiques et comporte des risques pour la vie en société.

D

CAPTER L'INFORMATION À LA SOURCE

Enfin, les dispositifs RFID constituent de puissants capteurs d'information, car ils peuvent être incorporés dans des instruments techniques, des vêtements, des objets domestiques ou des tissus humains. Des logiciels permettent de mettre en réseau des capteurs, des machines et des objets, de les faire interagir, de manière à constituer un "internet des objets".

Des puces RFID peuvent également être implantés dans le corps humain. Elles servent alors à mesurer certains paramètres biologiques, à des fins de diagnostic ou de prévention (par exemple, pour des personnes diabétiques ou cardiaques). Mais certains projets vont plus loin : il s'agit de suppléer à des fonctions biologiques déficientes, par exemple au niveau de l'audition ou de la vision. Le cas des implants RFID humains soulève des questions médicales et éthiques qui doivent faire l'objet d'une approche préventive approfondie.

E

LE CAS DE LA BIOMÉTRIE

Le cas de la biométrie révèle une tendance inquiétante à organiser le développement technologique autour d'objectifs de contrôle et de surveillance. La RFID serait victime d'une dérive

sécuritaire. Divers groupes de pression se sont constitués pour s'opposer à certains projets, notamment dans le domaine de la collecte et de l'utilisation de données biométriques à des fins de contrôle d'identité.

Ce n'est pas un hasard si les inquiétudes se cristallisent sur la biométrie et ses applications en cours de développement: le passeport biométrique, les contrôles d'accès basés sur les empreintes biologiques numérisées, les implants biométriques, etc. Le principe est simple: chaque individu peut être caractérisé par une série de paramètres biologiques (empreinte digitale, visage, iris, voix, échantillons d'ADN), qui forment une combinaison unique et qui peuvent aujourd'hui être numérisés. Une fois numérisés, ils peuvent être stockés dans des bases de données, comparés, analysés, communiqués. L'enjeu éthique est tout aussi évident: les caractéristiques biométriques font partie du corps d'un individu, dans quelle mesure peut-on les stocker, les communiquer, les vérifier à l'insu ou sans l'assentiment de la personne concernée ?

À la demande du Parlement européen, l'Institut de prospective technologique (IPTS) a évalué les différents impacts du développement de la biométrie, dans le cadre des technologies convergentes.

Cette étude repose sur deux postulats. D'une part, la diffusion des applications biométriques dépend de leur acceptabilité sociale, qui sera facilitée par leur usage dans les passeports et autres systèmes d'identification; les applications commerciales suivront, à condition que les cadres législatifs s'adaptent. C'est pourquoi l'IPTS recommande que les objectifs précis de chaque application biométrique soient clairement définis, de façon à favoriser la confiance des citoyens. D'autre part, il faut reconnaître les limites de ces technologies: leur fiabilité n'est pas absolue, elles sont vulnérables, elles ne resteront pas inviolables. Des procédures alternatives doivent toujours être prévues en cas de panne ou de dysfonctionnement des systèmes – mais l'IPTS ne soulève pas l'hypothèse d'un refus ou d'un boycott.

Aux yeux des opposants à la biométrie, il est peu probable que ces conclusions éloignent le spectre d'une société de la surveillance.

LE SPECTRE D'UNE SOCIÉTÉ SOUS SURVEILLANCE

Selon un rapport rédigé pour la conférence européenne des commissaires nationaux à la protection des données, cette société de la surveillance existe déjà et elle repose largement sur la technologie: bases de données, RFID, biométrie, traçage, tri social, marketing ciblé, etc.

Les législations de protection des citoyens sont souvent réactives, elles suivent la technologie mais ne l'anticipent pas, si bien que les nouveautés se développent toujours dans un contexte peu encadré. Les progrès technologiques requièrent une nouvelle approche du concept de vie privée, qui devrait être basé sur une évaluation continue des facteurs constitutifs de la vie privée et de leur évolution.

Les commissaires nationaux soulignent que les systèmes de surveillance invisibles, incontrôlés, incompréhensibles ou excessifs peuvent créer de l'insécurité au lieu de la sécurité. Ils peuvent aussi générer la marginalisation ou l'exclusion. La réglementation de la protection de la vie privée est insuffisante. C'est l'ensemble des dispositifs qui créent et entretiennent la confiance qui doivent être pris en considération pour que surveillance, liberté et démocratie restent compatibles.

LES DÉFIS À RELEVER

À court terme, les principaux défis à relever concernent :

- les normes techniques, qui font toujours l'objet de discussions tendues entre les blocs Europe, Amérique du Nord et Asie ;
- la protection de la vie privée, car les législations en vigueur doivent être adaptées à la nouvelle donne RFID ;
- le développement de logiciels capables de gérer de manière fiable et sécurisée les données collectées,

– la définition d'un cadre juridique et réglementaire approprié, non seulement pour le respect de la vie privée, mais aussi pour les applications dans le domaine de la santé ;
– la prise en compte du contexte social et économique de diffusion des innovations.

À moyen terme, face à une technologie qui est à la fois émergente et générique, c'est-à-dire transversale à de nombreux usages, la capacité politique à anticiper les changements et à prévenir les risques est un enjeu essentiel.

Un développement débridé de la technologie RFID pourrait s'avérer, à long terme, contre-performant.

Gérard Valenduc
Patricia Vendramin
d'après deux articles parus dans La Lettre EMERIT n°48

- AWT, *Fiche technique RFID*, Agence wallonne des télécommunications, Namur (www.awt.be).
- European Commission, *Towards a RFID policy for Europe*, Reports from the European consultation on RFID policy, Brussels, 2006.
- Infopôle, *Dossier de documentation de la conférence "Tracking, tracing et objets communicants"*, Namur, novembre 2006 (www.infopole.be).
- IPTS, *Biometrics at the frontiers: assessing the impact on society*, EUR21585-EN, JRC Institute for prospective technological studies, Sevilla, February 2005.
- Murkami Wood D., Ball K., *Un rapport sur la société de surveillance*, Rapport du *Surveillance Studies Network* pour la 28ème conférence européenne des commissaires à la protection des données et à la vie privée, Londres, novembre 2006.
- Des points d'entrée vers des groupes de pression "anti-puces": www.jameh.org; www.stoppuce.be; www.ines.sgdg.org

FICHE TECHNIQUE : LA TECHNOLOGIE RFID, EN QUELQUES MOTS

Sur le plan technique, les dispositifs RFID se distinguent selon le type d'ondes émises et selon que la puce est active ou passive. Les propriétés techniques influencent le type d'usage qui peut en être fait.

Les puces passives réagissent uniquement au dispositif électromagnétique qui les détecte. C'est le cas de la plupart des étiquettes RFID apposées sur des produits. On peut les assimiler à des codes à barres de deuxième génération. Elles sont aussi utilisées dans le marquage des animaux. Les puces semi-actives sont alimentées en énergie par le dispositif électromagnétique qui les détecte. Elles peuvent être dotées de capteurs, mémoriser les paramètres mesurés et les transmettre en présence d'un dispositif de lecture. Elles sont utilisées à des fins de contrôle à distance ou de diagnostic. Les puces actives sont dotées d'un émetteur récepteur continu et permettent une traçabilité permanente.

Les puces qui émettent dans la gamme des ondes radio ont une faible capacité de mémorisation, mais une longue portée (jusqu'à deux mètres), peu sensible aux obstacles. Les puces de la gamme UHF permettent un meilleur codage, mais leur portée est limitée à moins d'un mètre et les ondes sont facilement absorbées par l'eau ou le métal. Les puces de la gamme des micro-ondes (SHF) sont les plus performantes sur le plan électronique, mais aussi les plus sensibles aux obstacles; leur portée peut s'étendre jusqu'à une dizaine de mètres s'il s'agit de puces actives.

La taille des dispositifs RFID peut varier du centimètre (étiquettes communicantes) au millimètre (implants humains, de la taille d'un grain de riz). Le coût d'une puce RFID est actuellement d'environ 0.25 US$; l'objectif à court terme est de descendre à 0.05 US$, un niveau que les industriels considèrent comme un bon seuil de rentabilité.

La normalisation est un problème non résolu à ce jour. Les plages de fréquences sont différentes en Europe, en Amérique et en Asie. Les normes de codage et d'interopérabilité pour l'échange de données ne sont pas encore universellement établies.

AVEC LE SOUTIEN DU MINISTÈRE DE LA COMMUNAUTÉ FRANÇAISE, SERVICE DE L'ÉDUCATION PERMANENTE