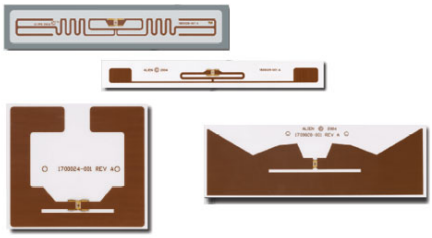
Projet co-financé

par l'Union Européenne



Quelques modèles de tags RFID pour l'identification des objets.

ETUDE DE CAS :

Risques liés à la RFID[1] pour la protection des données à caractère personnel et encadrement juridique.

Etude sous l'angle des 4 pièges tel que proposé par Philippe Lemoine, commissaire de la CNIL[2] lors de sa communication du 30 octobre 2003.

ci-dessus, Implant sous-cutané

ci-contre, injection humaine

[1] : Radio Frequency Identification

[2] : Commission Nationale Informatique et Liberté

La mondialisation de l'économie, cumulée à l'impact des nouveaux modes de commerce est porteuse de défis logistiques qui se posent tout au long de la « supply chain ». Le code-barre s'est imposé depuis longtemps comme outil incontournable de la gestion des stocks et des flux. Mais on se heurte aujourd'hui à ses limites physiques : l'identification doit obligatoirement passer par une lecture optique. Une technologie, qualifiée d'intelligente, permet pourtant de contourner cet écueil. En plus de permettre une lecture en aveugle puisque basée sur les ondes radio, elle peut contenir une large quantité d'information : c'est la RFID, pour Radio Frequency Identification. Elle porte en elle les prémisses de progrès insoupçonnés et l'avènement d'un « Internet des objets » mais également de nouveaux risques pour notre vie privée.

La technologie RFID n'est pas récente. Durant la Seconde Guerre mondiale, la Royal Air Force l'utilisait déjà afin de différencier ses avions de ceux des ennemis.

La miniaturisation et la normalisation[3] aidant, c'est son adoption dans des applications innovantes et notamment dans la distribution, le transport ou l'industrie qui fait beaucoup parler d'elle. Il s'agit, en effet, d'une technologie de pointe visant à assurer l'identification détaillée d'objets de tous types. La RFID permet de procéder à une saisie de données rapide et automatique grâce aux ondes radio. Elle est ainsi de plus en plus utilisée, notamment là où d'autres technologies d'identification, comme celle du code-barre se heurtent à leurs propres limites.

La RFID est en proie depuis quelques mois à de vives critiques en rapport aux risques qu'elle comporterait pour le respect de notre vie privée. Cet outil de traçabilité génial peut il se muer en œil indiscret et inquisiteur ? La presse décrit cette technologie comme une menace angoissante pour nos vies privées … Le danger est il réel ? Et si oui, comment y faire face ?

---

[3] : nombreuses normes ISO à ce sujet

D'ailleurs, un ensemble de textes législatifs, destinés à réglementer les droits et obligations de chacune des parties intéressées, commence à voir le jour, dans le but de prévenir les abus potentiels. Ces lois répondent à différents aspects juridiques illustrant autant d'abus potentiels.

Tâchons d'y voir un peu plus clair …

Considérons que les tags RFID sont des ordinateurs très particuliers : ils sont discrets par leur taille, sans aucun périphérique ni interface. De plus, ils sont capables de s'activer seuls, lors du passage au travers du champ émis par un lecteur et leur état de fonctionnement n'est nullement visible. Dès lors, il est normal que la CNIL s'y intéresse de très près. Etudions les.

Selon le professeur Philippe Lemoine, membre de la CNIL, quatre pièges peuvent masquer les enjeux cruciaux de cette technologie quant au respect de la vie privée des consommateurs.

L'insignifiance des données

Qui peut être intéressé par le numéro d'identifiant unique EPC[4] des conserves entreposées dans vos placards ou des céréales que mangent vos enfants ? Les quantités d'informations contenues dans les tags des produits possédés par une personne, peuvent cependant être récoltées et croisées grâce à un maillage très dense des données. Cette

« *Dans le monde du futur, on s'interrogera sur l'époque où les hommes avaient des bibliothèques où les livres ne parlaient pas entre eux* »
- Minsky

[4] : Electronic Product Code

analyse des informations émises par les biens disposant d'un tag, permettrait ainsi de profiler le consommateur afin de lui proposer un ensemble de produits correspondant à ses habitudes de consommation et à ses envies, réelles ou supposées.

Qu'est-ce qui techniquement empêcherait, à terme, un vendeur de voir s'afficher sur son écran le « profil marketing » de la cliente ou du client qui est en face de lui, profil déduit à partir des étiquettes de ses vêtements, ses accessoires de maroquinerie, des objets contenus dans ses poches, son sac à main ou son porte-documents ? Rien, a priori.

Sauf que la directive du Parlement Européen et du Conseil du 12 juillet 2002[5] limite ce type d'intrusions dans la vie privée des consommateurs. Cette directive exige dans son premier article que « les Etats membres protègent les droits et les libertés des personnes physiques à l'égard du traitement des données à caractère personnel et notamment le droit au respect de leur vie privée ».

Mais les informations contenues dans les tags RFID constituent-elles des informations relevant du caractère personnel ?

Selon la loi luxembourgeoise du 13 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, peut être considéré comme donnée à caractère personnel « toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable ; une personne physique ou morale est réputée identifiable si elle peut être identifiée directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique. ».

[5] : 2002/58/CE

On peut en tirer les conclusions suivantes :

- Les produits achetés par une personne sont de l'ordre de la sphère privée de cette personne.
- Les informations contenues dans les tags RFID accolés à ces produits sont des données à caractère personnel.
- La loi régit l'utilisation et le traitement de ces données puisque celles-ci sont à caractère personnel.

Il est dès lors illégal et illégitime de tenter de récupérer les données à caractère personnel que constituent les informations contenues dans les tags RFID figurant sur les produits en la possession d'une personne privée.

D'un point de vue technique, l'utilisation de lecteurs permettant l'identification à grande distance de tags RFID est pour l'instant impossible. En effet, les modèles d'étiquettes actuels ne permettent pas une distance de lecture supérieure à quelques mètres, dans des conditions idéales, au maximum.

Il est donc impossible que l'on puisse lire depuis l'extérieur de la maison les informations contenues sur les étiquettes RFID présentes dans un placard. De plus, la convention sur la cybercriminalité du 23 novembre 2003 précise que doit être érigé en « infraction pénale (…) l'accès intentionnel et sans droit à tout ou partie d'un système informatique », les tags RFID étant dans le texte considérés comme un système informatique puisque permettant « un traitement automatisé de données ».

Le deuxième piège est **la priorité donnée aux objets.** Les applications actuelles de traçabilité des produits font perdre de vue que les futures applications iront au-delà et seront plus intrusives dans la vie des personnes. En effet, tous les objets qui entourent une personne établissent sa

biographie. Par exemple, un ticket de caisse ou un titre de transport permettent de localiser une personne et de connaître ses activités dans les moindres détails.

De nombreux cas, mettant en œuvre la RFID à des fins de marquage humains ont d'ors et déjà été remarqués. L'autorisation donnée aux USA par la Food and Drug Administration d'utiliser des tags sous-cutanés pour des implantations humaines à fait grand bruit. Bien sûr, au départ, les applications apparaissent fort légitimes. Le but avoué est de permettre à des secouristes d'accéder grâce à cet identifiant aux dossiers médicaux des patients afin de leur administrer au plus vite les traitements adaptés même s'ils sont trouvés inconscients. Tâchons d'imaginer les dérives possibles de cette application en nous situant dans le cas d'une catastrophe de grande ampleur. Sans forcément avoir les conséquences des attentats du 9/11, un accident impliquant de nombreuses victimes réclame des soins en urgence et il faut alors que les secouristes gèrent les priorités. Est-ce que la culture américaine n'autoriserait pas de privilégier les blessés assurés sociaux ?

Un autre cas de figure qui se passe au Japon est choquant pour notre culture européenne. Les japonais sont friands de technologies et adorent leurs GSM. Evidement, ils aiment aussi leurs enfants ! Alors, certains écoliers se sont vus marqués avec ces tags sous-cutanés pour permettre à leurs parents d'être avertis par SMS lorsqu'ils arrivent dans l'établissement.

Mais revenons aux objets. Le plus important, ce n'est pas tant l'objet mais les informations véhiculées par celui-ci qu'il faut prendre en compte.

La CNIL a mis en avant deux priorités fondamentales lors de sa séance du 30 octobre 2003:

- Les données traitées sont bien des données personnelles, même s'il s'agit de données ne portant que sur des objets, dès

lors que la technologie RFID permet d'instituer un maillage dense d'analyse[6] des milliers d'objets qui entourent une personne;

- Il faut imposer la mise en place de mécanismes de désactivation[7] des « smart tags » dans certaines situations et avec le libre choix des personnes.

Contrairement aux législations européennes et nationales, la CNIL pose donc le principe selon lequel les données contenues dans les tags RFID entourant une personne, constituent des données à caractère personnel. En effet, le maillage de ces informations permet de véritablement tracer la vie des consommateurs. Dès lors, la classification de ces informations en données à caractère personnel devra être effectuée par le législateur. A moins que jurisprudence ne fasse loi…

Le troisième piège concerne **la logique de mondialisation :** les principaux centres de recherches sont basés aux Etats Unis. Or, à la différence des pays membres de l'Union Européenne, il n'y existe pas là-bas d'instance de contrôle en charge de la protection des consommateurs par rapport aux atteintes des libertés. Les autorités américaines sont en effet beaucoup moins vigilantes que les autorités européennes en matière de respect de la vie privée alors qu'il s'agit d'un des points fondateur de la Constitution américaine.

Il n'y a que quelques associations citoyennes américaines qui s'érigent contre le manque de vigilance du législateur américain à ce sujet. Ainsi,

---

[6] : on parle aussi de "smart environement"

[7] : la prochaine norme (EPC Gen 2) décrit une commande de désactivation du tag (kill command) qui pourra le désactiver en totalité ou en partie et pouvoir ainsi continuer à utiliser les seules informations utiles à son porteur.

l'association CASPIAN[8] a organisé un boycott massif de produits contenant la technologie RFID. Ses principaux griefs portent sur l'absence de marquage annonçant la présence d'étiquettes RFID dans les produits et l'absence de transparence dans l'utilisation qui en est faite par le distributeur. Ils se fondent également sur l'impossibilité de déceler qu'une étiquette RFID reste active, au-delà de l'acte d'achat, et puisse ainsi potentiellement être lue, à l'insu de son porteur, par d'autres personnes ou organismes, violant ainsi le respect de la vie privée.

Les standards relatifs à la RFID sont donc développés par ces centres de recherche américains sans qu'un quelconque contrôle ne soit effectué ou qu'une réflexion sur les futures utilisations de ces standards ne soient menée. Etant donné l'importance des enjeux économiques, il est certain que les standards mis en place aux Etats Unis seront amenés à s'étendre à l'ensemble des économies concernées par la technologie RFID. Le dialogue est mené avec les organismes mondiaux de standardisation tels que l'ISO ou GS1[9]. Ceux-ci devraient être confortés dans leur capacité d'influence, permettant ainsi aux futurs standards d'être acceptables, du point du vue culturel, sur les différents continents.

De manière très opportune, le sujet a été abordé lors de la conférence internationale des commissaires à la protection des données (Sidney, Septembre 2003) et a fait l'objet d'une résolution[10] qui vise à créer un organisme indépendant de contrôle du respect de la vie privée au niveau européen. Cet organisme, appelé groupe 29, est composé de représentants des différentes commissions nationales de protection des données personnelles des pays membres de l'UE. Il s'agit d'un organisme consultatif et

---

[8] Consumers Against Supermarket Privacy Invasion and Numbering

[9] : GS1 : regroupement de EAN (European Article Number) et UCC (Uniform Code Council), effectif au 1er avril 2005

[10] : voir http://www.privacyconference2003.org/

indépendant qui a proposé en janvier 2005 un document de travail[11] repris à l'article 29 de la directive 95/46/CE. Ces tâches sont décrites à l'article 30 de cette même directive ainsi qu'à l'article 15 de la directive 2002/58/CE. Ces directives européennes concernent la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Elles représentent déjà une barrière à certaines dérives que nous avons évoquées.

Les directives européennes et les lois de chaque Etat de l'Union restent strictes sur ce point : la convention sur la cybercriminalité du 23 novembre 2003 précise que sera érigée « en infraction pénale, (…) l'interception intentionnelle et sans droit, effectuée par des moyens techniques de données informatiques ». Dans la mesure où les informations transmises par RFID sont des données informatiques, cette convention européenne sera applicable. Elle est un signe de coopération internationale : « les parties coopèrent les unes avec les autres » afin de mettre un terme à la cybercriminalité.

La domination américaine en terme de standards et le manque de préoccupation pour la vie privée des consommateurs est ainsi mise en sursis… Les associations de citoyens, y compris américaines restent donc vigilantes et exercent une pression forte pour faire évoluer les standards vers une meilleure protection de la vie privée des consommateurs.

La non-vigilance individuelle : la technologie RFID repose sur le principe de la lecture automatique et à distance des tags. Dès lors, la communication entre le tag et le lecteur peut être initiée à tout moment. Le tag est toujours activable, subrepticement , à chaque fois qu'un signal est

[11] : 10107/05/EN – WP 105

émis par l'antenne d'un lecteur, le tag réagit en communicant les données qu'il contient. Le contenu du tag est ainsi décrypté par le lecteur, à chaque passage près de celui-ci, automatiquement. Les informations contenues dans le tag peuvent donc être transférées via Internet[12] aux intéressés qui se chargent du traitement des données.

Le rayonnement d'un tag RFID est donc potentiellement illimité dans le temps. La lecture du tag peut donc se faire sans que son « propriétaire » en soit informé ni ne puisse donner son consentement. De plus, le porteur du dit tag n'a donc aucun geste particulier à effectuer et par la même, ne démontre en aucun cas son intention évidente de permettre la lecture du tag en question.

Par exemple, un titre de transport équipé d'un tag RFID permettra une lecture et une vérification de la validité de celui-ci. Il contient toutes les informations personnelles concernant le porteur du titre de transport. L'organisation en charge du traitement des données peut ainsi savoir où est le détenteur du titre de transport et à quel moment il utilise le réseau de transport en commun. Il serait dès lors aussi possible à une tierce personne de lire les informations concernant l'utilisateur du réseau de transport en commun à l'aide d'un lecteur compatible. Dans ce cas précis, il est même possible d'accéder, en plus de données personnelles à des données sensibles. Le type de titre de transport est souvent lié à des particularités de son porteur. Un abonnement gratuit peut signifier un handicap de son porteur ou encore donner des renseignement sur son age.

Comme nous l'avons déjà vu, il commence à se profiler une solution pour prendre en compte ces problématiques. Ainsi, les futurs tags RFID seront munis, dans le secteur de la distribution, d'un système permettant de

[12] : Selon le principe de l'EPC, à partir de l'identifiant RFID il est possible d'accéder à une base de données relative à l'objet en question.

neutraliser en partie le signal concernant les données à caractère personnel après le passage du portique de sécurité du magasin.

Concernant les données personnelles, les données seront cryptées et leur intégrité sera garantie ou encore, les tags renverront à une base de données, de manière à empêcher une lecture directe et « en clair » des informations stockées sur un tag RFID comme précisé dans les articles 6.1 et 17 de la directive 2002/58/CE.

Enfin, la loi luxembourgeoise du 13 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel stipule que le responsable du traitement doit s'assurer que les données qu'il traite le sont loyalement et licitement, et notamment que ces données sont:

- collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités;
- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement;
- exactes et, si nécessaire, mises à jour; toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées
- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées.

Quiconque effectue un traitement en violation des dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende pouvant aller jusqu'à 125.000 euros ou d'une de ces peines seulement. La

juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction. Ainsi, le législateur protége les porteurs potentiels de la technologie RFID.

La technologie RFID a désormais atteint sa maturité technique, lui assurant ainsi une pérennité certaine. Il reste cependant à l'intégrer à un plus grand nombre d'infrastructures afin que les économies d'échelle réalisées permettent son développement, sa démocratisation et son accès au plus grand nombre d'entreprises.

Il apparaît cependant que l'adoption d'une technologie telle que la RFID comporte des risques d'atteintes plus ou moins graves à la vie privée des consommateurs. Les législateurs européens, mais aussi les associations de consommateurs, notamment américaines, luttent activement et en permanence afin d'éviter de tels débordements. Cette technologie ne pourra ainsi pleinement offrir ses avantages potentiels que si tous les acteurs ont une pleine confiance en elle. On estime pour l'instant que seuls 5 à 10% des applications potentielles de la RFID ont été imaginées. Il subsiste donc un espace important pour la créativité et l'innovation en termes d'applications RFID. Avec, sans doute, de nouveaux risques associés à gérer.