

1

NANOMONDE – VIVAGORA

CR débat du 6 avril 2006

Communication, transport, sécurité : quels usages des nanoproducts au quotidien ?

Étapes de la séance

I – Nano or not nano ?

II --Explication technique. C'est quoi la RFID ? Quelle lecture ? À quelle distance ? Où vont les infos ? Comparaison Etats-Unis / Europe

III - Le système EPC (Electronic Product Code)

IV – Les logiques d'acteurs. Qui a intérêt à quoi ? Localiser ou délocaliser l'info ?

Architecture des systèmes d'information

V - Le risque de rupture avec les consommateurs

Introduction - Dorothée Benoit Browaey

Nous arrivons à notre quatrième débat et VivAgora subit le feu des critiques et les accusations, tantôt de ceux qui considèrent que les « nanos » sont utilisées comme prétexte à remettre en cause un système, tantôt par ceux qui veulent mettre en pièces le système d'innovation vu comme non réformable. VivAgora refuse ces visions défaitistes et croit en la capacité de nos sociétés à infléchir les règles, à coopérer pour comprendre et décider des caps non « prédéterminés ».

Nous abordons ce soir les nanotechnologies sous l'angle de notre quotidien. Nous allons voir ensemble comment les nano-objets, nanodispositifs sont en mesure de transformer nos modes de vie, nos systèmes de sécurité, nos communications, nos relations sociales. Les puces d'identification par radiofréquence (RFID) - dont le marché atteint 2 milliards de dollars - servent à la gestion des stocks des chaînes de distribution (WalMart, Tesco, Metro, Carrefour...) ou des éleveurs (marquage des animaux par les puces d'Allflex ou de Mérieux) ou facilitent le contrôle d'accès dans les transport (Navigo à Paris) ou l'identification des personnes (la firme Verichip a implanté plus de 2000 personnes dans le monde pour les hôpitaux, l'entrée dans les entreprises ou les lieux ludiques). Le développement de ces puces (RFID), la généralisation et miniaturisation des capteurs constituent des bases de données dont l'usage n'est pas maîtrisé.

Sommes nous maîtres des informations nous concernant ? A qui appartiennent les données ? Qui en tire profit ? Quelles connexions sont-elles possibles entre les informations de sécurité (passeports biométriques), de santé (dossier médical, carte vitale), de consommation (habitudes d'achats, goûts, rythmes, déplacements) ? Beaucoup de groupes (CASPIAN, LDH, DELIS, Observatoire des droits et des usages, Collectif Georges Orwell, Association Privacy International) mais aussi des institutions (Conseil général des technologies de l'information, CGTI, le groupe 29 de représentants des « CNIL » européennes) se sont déjà mobilisés pour s'opposer à des usages abusifs. Nous nous attacherons à identifier quelles sont les capacités techniques actuelles et futures et quels sont les outils, les instances pour protéger les personnes ?

I – NANO OR NOT NANO ?

Claude Henry (sociologue, président de l'association VECAM, qui travaille sur la société de l'information et de la connaissance)

Les questions sur les libertés publiques confrontées aux réseaux d'information sont déjà anciennes. Aujourd'hui, la question à explorer me semble être : Quelle nouveauté

2

apportent les nanotechnologies ? Comment les nanotechnologies sont-elles en mesure de renforcer les problèmes ?

Philippe Marcel

Les RFID sont de la taille « micro », de plusieurs millimètres à plusieurs centimètres. Il n'y a pas de nouveauté. Particulièrement au niveau des antennes, on est loin des nanos. Le problème est celui de l'information et de la gestion de l'information. Et je m'appuierai

sur mon collègue de la CNIL pour les questions de protection des données personnelles.

DBB

La réduction de l'échelle n'introduit-elle pas une diminution des coûts, entraînant une inflation du phénomène ?

PM

On peut aller jusqu'à la taille nano pour la gravure, mais pour la partie analogique, il faut au moins un millimètre pour avoir assez de puissance. Et la partie antenne est mille fois plus grande que la puce.

Pour avoir une liaison sans fil de type radio-fréquence avec un rendement correct, il faut que la géométrie de l'antenne respecte certains critères. Pour les antennes les plus simples, la longueur de l'antenne doit être de l'ordre du quart de la longueur d'onde de la fréquence de fonctionnement. Par exemple, si l'on considère la bande de fréquence de Wifi (liaison sans fil), cela correspond à une longueur d'antenne de l'ordre de 2,5 cm. Par ailleurs s'il l'on considère des longueurs d'ondes de l'ordre de quelques centaines de nanomètres, on est alors dans le domaine optique et non plus radio-fréquence. Si toutefois l'antenne reste à des dimensions faibles de quelques millimètres ou quelques microns, alors la distance de lecture devient très très faible (quelques millimètres).

DBB

Comment se fait-il que le rapport rédigé par Philippe Lemoine, de la CNIL, considère que ce secteur des technologies de l'information représente 55 à 60 % du marché des nanotechnologies.

Yann Le Hégarat

Philippe Lemoine se réfère à la National Science Foundation (NSF) américaine qui estime que d'ici 10 ans, 60 % des nanotechnologies seront dans le domaine des technologies de l'information, et qu'il y en aura 10 % pour les nano-bio et 30 % pour les nanomatériaux.

DBB

L'introduction des nanos dans le traitement de l'information peut-il en changer la nature ?

YLH

Oui, la diminution de taille implique la même histoire que dans la technologie de l'électronique : la loi de Moore. Dans ce cas, on change régulièrement les usines qui construisent les microprocesseurs. Mais avec les nanos, il y a le mouvement inverse de la miniaturisation qui est la reconstruction à partir de constituants élémentaires. Qu'est-ce que cela va permettre ? On va pouvoir faire des nano-ordinateurs, marquer des atomes, utiliser les effets quantiques pour le chiffrement (cryptage). Mais il n'y a pas d'application tangible, pour l'instant. Les perspectives restent encore du domaine de la conjecture. Peut-être que le chiffrement sera bouleversé par des ordinateurs quantiques.

DBB

Si je résume : ce qui est nano, c'est pour l'avenir, aujourd'hui, on a du micro ?

PM

Ce qui existe aujourd'hui, ce sont des nanotraceurs lisibles de façon optique. Pour simplifier, il s'agit d'utiliser les propriétés optiques de nanoparticules stables qui peuvent

être fonctionnalisées en vue de répondre de façon optique à une onde les éclairant. On peut ainsi par combinaison avoir un équivalent de « code à barres » optique directement dans un faible épaisseur d'un substrat donné.

Frédéric Levy

Les perspectives à long terme des nanotechnologies sont de mettre de l'information dans tous les objets.

YLH

Il s'agit du concept d'informatique omniprésente ou « ubiquitous computing ». Les RFID ne sont qu'une première étape et ne sont jamais que l'un des modèles informationnels. On va vers une multiplication d'objets qui intègrent de l'information (de l'identifiant, de la

mémoire) et qui en échantent, créant un environnement physico-informationnel complètement nouveau. Le concept d' « *ubiquitous computing* » est flou car sa définition n'a pas encore de consensus ; de nombreux termes et concepts y sont liés comme ambiance intelligente, réseaux de capteurs exploitant les phénomènes d'émergence etc.

Michel Alberganti (journaliste au *Monde*) se dit consterné par les thèmes abordés. Selon lui, les RFID n'ont rien à voir avec les nanos. La question qu'il souhaite voir aborder est : Quand les nanos deviennent-elles un problème ?

II --EXPLICATION TECHNIQUE. C'EST QUOI LA RFID ? QUELLE LECTURE ? À QUELLE DISTANCE ? OÙ VONT LES INFOS ? COMPARAISON ETATS-UNIS / EUROPE

Philippe Marcel

Les RFID ne sont pas à l'échelle nano mais leur réduction à l'état invisible (que peuvent permettre les progrès de la micro-électronique et de la nano-électronique) fait peur. Les RFID ont été introduites vers 1986 et fonctionnent soit en basses fréquences (125 khertz à 13 MégaHertz), ce qui implique un champ proche. Elle n'ont pas d'énergie propre et répondent seulement dès lors qu'elles sont activées par un lecteur qui ne peut agir qu'à proximité. Ainsi, le système Navigo permet de lire les puces dans un champ de 30 centimètres à 80 cm dans le meilleur des cas. L'autre technologie est celles des UHF et SHF, qui utilise un champ lointain ; dans ce cas et pour l'heure, on peut envisager d'accéder à une information si le lecteur est à moins de 3 ou 4 mètres de la puce. Peut-être arrivera-t-on au maximum à 10 mètres en hautes fréquences, si l'on respecte les valeurs d'émission.

Les Américains ont des puissances embarquées bien plus grandes pour la partie hautes fréquences (par exemple pour bluetooth). Si l'on augmente les puissances, on augmente la pollution électro-magnétique, qui en Europe est parfaitement bordée par les normes. Les Américains prétendent pouvoir faire un inventaire sur 600 m². En fait cela n'a pas de sens dans la mesure où la seule présence d'un article sur une telle surface n'a d'intérêt que si l'on peut localiser ce dernier. Ce qui n'est pas le cas. Il en est de même dans une foule. Par ailleurs, si ce que l'on lit dans la presse donne l'impression qu'il est possible de repérer des gens par satellite grâce à la RFID implantée en sous-cutané (fonctionnement en basse fréquence), il faut savoir que c'est totalement impossible : cela nécessite un système relais (téléphone portable avec GPS ou équivalent). Donc c'est seulement en croisant des « identifiants » et informations de géo-localisation que l'on peut repérer une personne. Au même titre que les téléphones portables.

À propos des passeports biométriques, les informations sur les données personnelles (empreintes digitales, iris...) seront portées par une puce RFID de façon cryptée.

Stéphanie Lacour (juriste au CNRS) demande si, en fin de compte, ce qu'apportent les nanos, ce n'est pas la possibilité de la convergence ? On voit se développer des capteurs corporels (prise de température, de tension...) pour les personnes âgées qui pourraient être mis en connexion avec des bases de données...

4

Bernard Bartolien indique que l'on peut faire des labos sur puces, séquencer l'ADN, faire du tri en masse.

DBB

Vous avez insisté sur la différence du développement avec les Etats-Unis. Est-ce du fait de limitations par des structures comme la CNIL en France ou d'autres cadres normatifs ?

PM

Il existe différents cadres normatifs : en Europe, on part du principe qu'on ne doit pas polluer son voisin, et donc on limite la pollution électromagnétique. Outre-Atlantique, c'est un tout autre état d'esprit : si mon voisin parle fort, je parle plus fort que lui.

Les grandes surfaces qui veulent utiliser ces étiquettes sont sur une logique à bas coût. Mais au lieu des trois centimes d'euros visés, on est plutôt à cinq centimes, sans compter l'antenne ; donc, si l'on arrive à huit, voire dix centimes, ce ne sera déjà pas mal ! Mettre une puce sur une bouteille d'Evian sera sans intérêt, donc on est revenu en arrière et on

se contente pour l'instant de la logistique interne, c'est-à-dire que l'on ne s'intéresse pas aux données unitaires mais seulement aux grands stocks.

DBB

Du point de vue industriel, quels sont les atouts américains ?

PM

Les Américains disposent du labo Auto-ID du Massachusetts Institute of Technology (MIT), laboratoire auquel sont associés des industriels (Gillette, Procter & Gamble, Nestlé, Coca, Carrefour) et le Département de la défense américain qui correspond au Pôle de traçabilité de Valence et à la CNOR avec des budgets multipliés par dix mille. Dans notre laboratoire, nous sommes quatre ou cinq ; eux ils sont cinquante !

III - LE SYSTÈME EPC (ELECTRONIC PRODUCT CODE)

Philippe Marcel évoque la possibilité de la constitution d'une Banque de Données Mondiale Electronic Product Code (EPC), sorte d'internet des objets (où chacun d'eux est identifié par un code avec 96 éléments binaires) qui centraliserait les informations, avec le risque d'un monopole et de possibilités incontrôlables de connexions de données. Malgré ces divergences, on arrive à harmoniser les fréquences allouées et les puissances autorisées. Il n'empêche que les Américains sont dans une démarche complètement différente. Il existe un problème au niveau d'une certaine harmonisation concernant les normes ISO. Nous avons l'obligation de défendre la position française et européenne face à la position américaine dont la puissance financière est phénoménale.

Colette Lartigue

Dans le contexte des échanges économiques que nous avons actuellement, est-il viable d'avoir ces deux systèmes ? L'un des deux ne va-t-il pas prendre le pas sur l'autre dans un avenir plus ou moins proche ?

PM

Les deux vont rester en place. On essaie de suivre, car on s'est un peu harmonisé avec les Américains sur certains domaines. Donc on est obligés de faire contre-poids. Donc, sur la notion d'EPC, on est présent. La traçabilité globale d'EPC est mondiale. On essaie de proposer des normes ; et c'est toujours utile d'utiliser des RFID non normalisées pour des raisons de confidentialité.

Par exemple le système bancaire ne souhaite pas que tout soit complètement compatible avec tout le monde. On se bat là-dessus dans les entreprises pour que la RFID soit réellement un outil de traçabilité et de gestion et non une dépendance à un système.

5

YLH

Il y a d'autres dimensions à la normalisation. La normalisation logique des identifiants et de leur signification, la normalisation physique avec ses puissances et ses fréquences. Il y a aussi un système d'information dans le cadre d'EPC qui a vocation à normaliser l'ensemble des codes barres des produits commercialisables. Et identifier un objet par un autre, c'est coûteux comme une bouteille d'eau individuelle par rapport à une autre bouteille d'eau du même paquet.

La normalisation est mondiale. Elle pose du point de vue de la CNIL beaucoup plus de problèmes de finalité de la collecte de données qui apparaissent personnelles et de l'interopérabilité des bases, y compris bien sûr dans ses aspects de traçage et de localisation des objets.

DBB demande des précisions par rapport au problème posé à la CNIL.

YLH

Les problèmes éthiques de ces bases de données sont multiples. À qui appartiennent les données ? Qui peut les tracer ? Exemple : la puce elle-même est inerte, n'a pas d'énergie propre, ne fait rien par défaut. Mais en présence d'un lecteur, elle va s'activer, ce qui entraîne une **trace**, l'identification de la puce d'une part, et, (liée au lecteur) **la localisation de l'objet**. C'est l'intérêt de pouvoir tracer les objets notamment pour les chaînes logistiques. Cette traçabilité, y compris dans son aspect géographique, est gérée

par un système d'information, de la même façon qu'un téléphone mobile est tracé par un opérateur. Ce système est peut-être dérivable en « **concierge électronique** », il peut être public ou privé, prendra la même forme que les systèmes antivol des magasins. On peut imaginer de la même manière, que le lecteur non seulement active ce qui passe dans son champ, mais aussi enregistre les identifiants. **Ce que ces identifiants deviennent dans le système d'information interconnecté entre différents acteurs** pose un véritable problème.

DBB

Les vigilances à avoir portent donc sur deux points : **À qui appartiennent les informations et peut-on maîtriser leur devenir, leur usage ?**

PM

Pour compléter, il faut parler de la notion de traçabilité globale. Actuellement, on a une chaîne de traçabilité. Une entreprise qui a un fournisseur va fournir un certain nombre d'informations utiles pour la traçabilité globale du produit, mais elle garde ses informations. Si on pousse à l'extrême le système EPC, toute entreprise va mettre toutes ses informations de production et son savoir-faire sur une base de données mondiale. Ainsi, on pourra mettre à chaque fois en corrélation, l'identifiant et sa base de données. Il faut noter un point non négligeable dans le système actuel : l'étiquette est à bas coût, mais l'accès à la base de donnée est payant ; chaque fois qu'il y a action sur la base de donnée mondiale, tout est payant, l'écriture comme la lecture.

Dominique Pestre

1) Nous tournons autour de la question de ce qui est véritablement nano dans le débat de ce soir sur les informations diffuses et connectées. C'est un vrai et un faux débat, récurrent dans nos rencontres. Je ne crois pas que l'on puisse éviter la cacophonie. Parfois, les acteurs ont intérêt à la cacophonie. Une fois, ils disent que leurs objets sont « nano » pour avoir de l'argent. Puis quand on leur demande de confirmer que c'est bien nano, ils disent qu'ils n'ont jamais prétendu que ça l'était !

En fait, la réduction en taille fait que **l'on appelle nano, par anticipation**, des choses qui n'en sont pas mais qui sont susceptibles, quand elles émergeront, de déplacer les repères. Donc c'est vrai que ce n'est pas la question pertinente, mais il faut se la poser régulièrement parce qu'il n'y a pas de solution simple à cette question.

6

2) Je pense qu'il est important que nous ayons le maximum **d'épaisseur dans la description**. (S'adressant à Philippe Marcel) Et vous êtes tellement « dedans » que vous ne savez pas ce que vous devez dire, ce que nous ne savons pas. Or nous ne savons rien, et cela vous ne le savez pas. Et finalement plus on avance dans l'explication - et c'est cela l'intérêt de l'explication technique - plus c'est mystérieux. Et il y a un tas de choses que l'on voudrait demander, et à chacune de vos phrases, on voudrait vous arrêter, mais on ne peut pas. Je pense qu'il faut continuer dans cette direction, et ne pas hésiter à vous demander des choses.

3) Il y a une autre manière d'aborder l'épaisseur des objets, c'est de les **aborder par les usages**. On constate des rejets du côté de la CNIL, qui considère les techniques en situation, à travers les usages. Sous cet angle pratique, émergent des aspects techniques que les techniciens ne pensent pas à nous dire, parce que pour eux, ce n'est pas pertinent. Les usages sont importants car ils peuvent **réinventer la technique**.

4) Qu'est-ce qui pousse à développer les étiquettes et informations partout ?

La réponse doit être extrêmement différenciée parce qu'elle passe par une série d'acteurs différents qui peuvent être d'accord à un moment donné pour développer quelque chose en commun avec des stratégies qui sont très différentes. Aux Etats-Unis, vous disiez que les pratiques étaient différentes. Si l'on veut comprendre pourquoi, il faut sans doute s'intéresser aux acteurs, les grandes entreprises, le département de la défense, les ONG.... Pour repérer le « pourquoi » de ces projets, on peut regarder les usages et leurs conséquences.

Par exemple, dans le débat sur **EPC**, les questions seraient : qu'est-ce qui pousse, et qui, à mettre tout en commun dans une grande banque de données centralisée ? Quels sont les acteurs précis qui promeuvent cela ? Qui finance ?

Rien ne dit que, pour la logistique des produits, on ait intérêt à une banque commune, qui peut être favorable pour certains aspects, pas pour d'autres.

IV – LES LOGIQUES D'ACTEURS.

DBB

Sur la question des usages que posait Dominique Pestre, et en regardant cette dynamique d'EPC, est-ce que l'on peut repérer quels sont les intérêts en jeu ?

YLH

On va regarder ce qui se passe pour Internet. On a exagérément qualifié EPC d'« Internet des objets », entre autres, la fameuse banque de données qui est derrière les objets avec les informations qui sont reliées, et cela correspond en grande partie à ce que l'on trouve dans la gouvernance d'Internet, ce que l'on appelle le DNS, et il se trouve que le principal acteur américain (Verisign) qui se pose comme étant le garant de la racine des autorités de signatures électroniques et également le garant de la racine des noms dans le domaine des sites Internet.

Or, celui qui contrôle la racine contrôle à priori toute la fonction stratégique d'intégrité de l'ensemble.

Ensuite, il y a les normes techniques, quand elles sont figées, s'il y a des conséquences fâcheuses diverses, économiques, visant les libertés individuelles et collectives, cela va poser de gros problèmes de faire un retour en arrière.

Donc, l'analogie entre le principal acteur d'Internet (Verisign) qui est emblématique de la vision stratégique des Américains dans ce genre de système, on l'a retrouvé sur l'Internet des objets, sur le code EPC.

PM

WalMart est le leader mondial de la distribution. Il y a en France une tentative de la grande distribution qui demandait aux sous-traitants de mettre ce que l'on appelle « les

7

recettes », leur savoir-faire à disposition des grandes surfaces pour qu'elles contrôlent la traçabilité. Cela a échoué, et ne s'est fait que pour des sous-marques des magasins. Ce sont des logiques industrielles soutenues par des subventions d'État. Le code RFID est vu comme une possibilité d'élargissement des codes-barres. Il y a les collègues de GenCod qui sont à l'origine des codes barres « payants », pour utiliser certains codes normalisés il faut être adhérent et cotisé. S'ils n'étaient pas rentrés dans le système, ils perdraient leur marché et une partie de leurs finances. Donc, ils sont rentrés dans le système et l'objectif de GenCod, c'est faire en sorte de réaliser que les codes RFID soient un élargissement des codes actuels. Ainsi, ils ne perdent pas leurs bases de données ni leur place financière, mais ils l'élargissent.

Jean-Paul Karsenty

Nous n'avons pas vu assez tôt que les adresses Internet sont des éléments stratégiques, des lieux de passage obligés. Il est utile de relier comment se construisent les bases de données, l'architecture des bases de données et les acteurs qui prennent pouvoir sur l'orientation de ces bases et leurs régulations extérieures. On peut prendre un point de comparaison avec la génomique et la post-génomique : l'agrégation des bases de données s'est faite selon une architecture qui permettait d'avoir la main sur le développement du secteur.

Il s'agit de dégager l'enjeu, à savoir : on se bat pour éviter de se faire imposer des standards par la puissance des industriels du secteur, et qui ne nous permettront absolument plus d'être des acteurs offensifs dans la construction mutuelle de ces bases de données.

DBB

Avez-vous des éléments d'éclairage sur la stratégie qui structure ces projets EPC, qui

donnent du poids à certains, et moins à d'autres ?

Patrice Senn

Pour qu'un code EPC soit acceptable, il faut que chacun puisse le lire. Prenons l'exemple des portables ; on les a numérotés pour éviter le vol. Mais cela permet de repérer son détenteur ! Est-ce un bon ou un mauvais usage ?

Au départ, cela s'est mis en place grâce à la micro-électronique. Par exemple, les puces dans les objets peuvent protéger contre la contrefaçon. Il n'y a pas au départ une stratégie. Il s'agit simplement d'industriels qui veulent se protéger.

DBB

Dans ce processus-là, qu'est-ce qui fait la loi ?

PS

Les standards se font dans des forums internationaux. La question est de se dire que ça n'a de sens que s'il y a un standard mondial. Pour être capable, pour identifier un produit dans le monde, il faut être d'accord sur un code unique. Cela ne se passe pas au niveau des Etats, mais au niveau des forums, dans les organismes internationaux de normalisation.

DBB

Donc, c'est dans une vaste guerre industrielle que l'on sort des armes industrielles. Dans tout ça, qui a des intérêts ? Plus de sécurité, plus de traçabilité, est-ce vraiment au service des consommateurs ?

Dominique Pestre

Il y a une sorte d'évidence du technicien qui fabrique. Ce qu'il fait est absolument naturel, et en plus on comprend sa logique : cela évite que l'on vole le portable ! cela évite la contrefaçon ! cela permet, pour les médicaments que vous n'avez pas le mauvais lot ! Tout cela on le fait au nom de la sécurité ; il n'y aura plus de vol, on saura

8

exactement où vous êtes, vous serez soignés par le bon médicament, il n'y aura plus de problème, car nous allons fabriquer la société absolument idéale !

Le problème, c'est que ça peut s'écrire à l'envers. Cette même société peut se décrire comme une société dans laquelle vous n'avez plus d'autonomie, qui est liberticide. C'est « Big Brother ». Donc, le problème est réel. Si on regarde les choses différemment, l'image peut être terriblement noire, ou terriblement rose, mais le noir, n'est pas séparable du rose. Et le problème des sociétés humaines, à mon sens, c'est que nous devons anticiper la face noire du rose.

V - LE RISQUE DE RUPTURE AVEC LES CONSOMMATEURS

Patrice Senn

Je partage tout à fait cet avis. C'est-à-dire que l'on est toujours conscient qu'une technologie peut toujours être détournée de l'usage pour lequel elle a été faite. Mais en même temps, je pense que c'est la société qui doit, justement, mettre les garde-fous et avoir un système de contrôle un peu universel. Cela ne veut pas dire que les bases de données sont au même endroit, ni qu'une personne en détient l'ensemble. Les garde-fous de la société font que l'on peut éviter les débordements.

On ne peut pas non plus dire que s'il y a un détournement possible des RFID, alors, de ce fait, on dit qu'il ne fallait pas le faire. D'abord, c'est un peu tard, parce que selon les prévisions, il y en a déjà deux milliards dans le monde aujourd'hui et il y en aura dix milliards en 2010, et trois cent à quatre cent milliards en 2016. Et ce sont les prévisions qui ne concernent que l'identification et le marquage des stocks.

Maintenant, dire qu'il n'y aura pas de code universel pour EPC, c'est aussi une possibilité. Après tout, on peut envisager que chacun fasse son code. Mais, à ce moment-là, l'utilisateur aura le risque ou l'avantage (on ne le saura jamais) de ne pas savoir ce qu'il y a dans le RFID.

C'est plus frustrant pour vous de ne pas le savoir, parce qu'il y en aura de toute façon. L'industrie va l'utiliser, pour la question des stocks, etc.

Et, du coup, ne pas savoir peut être pire que d'avoir un code général ; et puis, c'est à chacun d'éviter que ce soit entre les mains de personnes plus ou moins malintentionnées. De même, pour les codes Visa, personne ne s'en inquiète aujourd'hui. Mais, c'est tout de même le système bancaire qui contrôle tous les codes Visa. Ce n'est pas pour cela que le système va en abuser. Le système des cartes Visa peut faire des suivis sur tout ce que vous achetez, caractériser votre profil consommateur. Les codes, c'est eux qui les décident, et ce n'est pas pour cela que vous n'utilisez pas votre carte Visa. Parce qu'en fait, vous avez une certaine confiance dans le système bancaire.

Ce qui est important, c'est de travailler sur la confiance, sur les tiers, sur les opérateurs qui vont l'utiliser. C'est uniquement ainsi que l'on peut éviter les craintes, les dérives, et les problèmes que vous pouvez soulever.

YLH

J'ai des critiques à faire. Je suis ingénieur ; l'ingénieur crée un objet social même s'il a l'apparence d'une technologie. Vous parlez de l'usage des bases de données. Pas besoin d'en parler en détail ! En effet, pour utiliser un code RFID, on n'a pas besoin de savoir quelle est la codification de l'entreprise, celle du type d'objet, le numéro de série. Un simple numéro unique suffit lui-même pour que l'objet soit identifié par n'importe qui pour n'importe quelle finalité.

On retrouvera le RFID qui sera lu à un autre endroit avec le même numéro. Vous n'avez aucun accès à la base EPC et vous avez quand même un suivi de traçabilité. Cela pose quand même potentiellement un problème de libertés individuelles et publiques.

PS

C'est peut-être assez vrai. Aujourd'hui, le RFID, n'est qu'une extension. Ce n'est pas une rupture. Simplement, c'est le fait de pouvoir mettre plus d'information qui peut être lue

plus facilement. C'est le même principe que le code-barre, sauf qu'aujourd'hui, quand vous voyez le code barre de quelque chose, avec un numéro, vous êtes incapable de remonter à l'objet.

YLH

Attention, Le code barre actuel européen (EAN13) ne donne que des types, pas des numéros dans la série du type. Le code EPC va identifier cette bouteille là, et va la différencier de sa voisine du même lot ou d'un autre lot quelconque. C'est là la première différenciation. Et, ce qu'il y a de plus grave, en dehors du monde des objets manufacturés, c'est le fait que la lecture, l'activation RFID se fait de façon invisible. Or quand vous activez le code-barre, vous avez une lecture d'opérations quelconques qui est visible ; le RFID lu, lui est invisible.

PS

En tout cas, dans les deux cas, la lecture ne peut se faire qu'à faible distance.

PM

Il y a une grande différence. Dans le cas d'une lecture d'un code-barre, s'il y a une anomalie, on sera obligé de jeter tout le lot. Alors qu'avec les RFID, l'information recueillie permettra de n'en jeter qu'une partie. Et puis, il existe toujours la possibilité de détruire la puce. Evidemment, il n'y a alors plus de traçabilité possible. Enfin, les comités de normalisation sont organisés par des industriels. Dans ce cadre, chacun défend son marché.

DBB : Qu'en est-il des définitions de la norme ?

PM : Les normes EPC ne sont pas des normes obligatoires.

YLH

En ce qui concerne l'effaçabilité des puces et des codes, on a certes, la possibilité d'« endormir » la puce. Celle-ci peut être ainsi sous le contrôle des individus. Ainsi, dans le cas d'un linge étiqueté, la machine à laver lit le code et choisit le type de lavage. Mais si je veux avoir la possibilité de neutraliser cette lecture, c'est à dire d'« endormir » la puce, c'est plus cher et doit être prévu par le manufacturier !

Alain Lombard

J'aimerais d'autres infos que celles concernant les RFID. J'aimerais savoir à quoi tout cela sert exactement. Est-ce que Minatech travaille strictement sur l'industrie de l'information, mais aussi sur le militaire ? J'aurais aimé que l'on ait une réflexion sur ces phénomènes et leurs impacts.

PS

France Telecom R&D a créé avec le CEA un laboratoire, MINATEC IDEAs Laboratory, dont le but est de travailler sur les usages des nanos. En fait les phénomènes sur lesquels on travaille aujourd'hui sont surtout dans le secteur micro. On est relativement loin des nanos, mais on est intéressé par le débat sur les nanos. On organise des débats publics, mais nous avons encore peu d'objets pour réfléchir sur les nouveaux usages. On n'a pas le sentiment qu'il y ai rupture au niveau des objets. On voit cela plutôt comme des façons d'améliorer des objets. Par exemple, face au problème des portables dont les batteries se vident, on se demande si les nanos ne pourraient pas servir ?

Hélène Milet

La peur naît des méconnaissances. Les codes-barres, les RFID, sont des outils. Les outils peuvent être nuisibles selon la façon dont on s'en sert. Le problème posé ce soir n'est pas dans la puce, mais dans qui la lit. De plus, l'inquiétude vient de la possibilité de stocker en un point toute la vie d'une personne.

10

Un intervenant dans la salle regrette que l'on n'ait pas abordé la question de fond de la place de la technique dans la société.

Alain Weber

Au niveau de l'Etat, la tendance qui prévaut est de créer des bases de données cumulatives ? Mais, pour l'instant, le ministère de l'Intérieur ne sait pas quelle orientation donner à ces bases de données. Les Européens communiquent des infos dont on ne sait pas qui les traite. Les données biométriques devraient être utilisées dans le cadre de l'espace de Schengen, mais, il n'y a pas d'uniformité au niveau des enregistrements, et tous les pays n'ont pas signé les accords.

Il faudrait brider ces informations, et éviter qu'il y ai interconnexion entre ces données et, par exemple, la carte vitale. Quand on rentre dans le détail du dossier de l'INES (la carte d'identité biométrique), on prend conscience qu'il n'y a aucune raison de passer à ce type de carte d'identité.

Yann Le Hégarat explique ce qu'est le groupe de l'article 29. Il explique que le passeport biométrique est aussi RFID. Mais u fait que certaines données de la puce ne sont pas lisibles par tout le monde, cela autorise une certaine confidentialité.

La puce contient :

- Les données du passeport,
- Une photo numérisée du visage,
- optionnellement deux photos numérisées d'empreintes digitales,
- optionnellement Les données de l'iris.

La carte d'identité nationale française sera sûrement biométrique. Et il y aura une base de données centralisée pour l'Europe.

La CNIL défend le principe selon lequel, les moyens mis en oeuvre doivent être proportionnés aux fins.

Patrice Senn : Il faut toujours se rappeler qu'il n'y aura jamais d'objet nano lisible sans une antenne très grosse pour la lire.

Un **sociologue** intervient

On distingue deux tendances. Si on regarde les usages, il y a la mise en oeuvre de la biométrie. Par exemple, pour entrer dans une école, il faudra être porteur d'une puce. En revanche, on n'évoque jamais la nécessité de la protection des données. On ne sait pas ce que deviennent ces données. Et cela implique le risque de développer une certaine ignorance.

Il y a une contradiction entre d'une part un fantasme d'homogénéité (qui consiste à penser que lorsque l'on aura tout marqué, tout ira pour le mieux) et d'autre part, l'hétérogénéité des motivations. Ainsi, la puce que porte l'élève peut permettre de prévenir ses parents lorsqu'il est absent, mais elle peut aussi permettre de récupérer éventuellement, les dettes des parents.

Roger Moret, physicien, souhaite revenir sur ce qu'a dit **Hélène Millet** à propos de la peur. On a l'impression que si l'on dit nano, ceci induit la peur, alors que si l'on parle du niveau micro, les gens sont rassurés. Or, il faut prendre conscience que l'on est dans un processus de miniaturisation, et qu'il y a simplement continuité entre le micro et le nano.

DBB

Je souhaiterais que l'on revienne aux perspectives constructives. Nous sommes devant un processus d'ingénieur. Il y a d'un côté, la science à l'oeuvre, d'autre part, des résistances en face. Que faire ?

PS

Je ne suis pas favorable aux bases de données mondiales. Il faut être capable de lire l'information en local, sans être obligé d'aller chercher dans une base de données mondiale. Cela dit, il serait dommage de se priver d'un progrès.

11

Colette Lartigues

La peur est liée à l'importance donnée au phénomène, importance qui apparaît à la fois dans les investissements énormes effectués sur les nanos et dans la communication et les discours. Côté recherche, il y a énormément de projets labellisés « nanos ». La question éthique peut se poser individuellement, mais elle est extrêmement difficile à poser au niveau du groupe. Pour une activité qui impose l'interdisciplinarité, on aurait pu attendre une réflexion sociétale un peu plus structurée. De plus, on constate que dans les formulaires de réponse aux appels à projets « nanos », il n'y a pas encore de place pour un critère d'impact sociétal, alors que cela existe pour les projets à caractère bio ou biotechnologies.

PM

Une remarque en conclusion et aussi une question d'éthique plus large : quel est l'impact d'une dépendance de l'individu à un environnement « intelligent » lui donnant toutes les informations ? Ne va pas t-on perdre en réflexion et qu'arrivera-t-il quand nous serons sortis de ce cadre ? Cette question de société m'interpelle fortement.

Gérard Toulouse

Dans ces questions de fuite en avant technologique, il y a des résistances. Il n'y a pas de raison de désespérer, elles peuvent se structurer et aboutir. Dans d'autres secteurs, on voit que les résistances fonctionnent. Je pense par exemple au développement du commerce équitable, au fait que l'on voit des gens qui arrêtent l'utilisation de la voiture.

Dominique Pestre (synthèse)

J'ai un problème avec quelques interventions. Celle du sociologue qui a enquêté sur les cartes biométriques au lycée, par exemple. « L'ordinaire est hétérogène », dites-vous, et les questions et élucubrations des intellectuels manquent cette hétérogénéité, dans leur volonté de bien/mal faire. Vos propos renvoient implicitement à une théorie du complot, ce qui est une mauvaise direction selon moi. De même, Alain Weber, de la LDH, va à la limite dans le même sens quand il nous dit en effet que même l'organisation technocratique la plus puissante et motivée ne peut que rater sa tentative de tout quadriller - puisque les gouvernants sont assez bêtes pour ne pas réussir à s'entendre sur des standards communs (le passeport "Schengen"). Mme Millet nous dit que « la peur vient de la méconnaissance ». Attention ! Il y a aussi des peurs justifiées, qui naissent de la connaissance. En tant qu'historien, je pense en outre que ce qui est techniquement possible se fait, d'une manière générale. Car il y a toujours des acteurs pour trouver un intérêt à telle ou telle innovation.

Les solutions ou garde-fous ? il faut trouver des « garants » dans la société civile : la

LDH peut en être, la CNIL ou d'autres... Et puis il faut inciter les chercheurs à l'autovigilance...
mais bien sûr sous des formes publiques permettant aux profanes de les arrêter s'il le faut.