RFID quelques réflexions introductives à un débat de société

Darquennes, Denis; Poullet, Yves

Published in:
Revue du Droit des Technologies de l'information

Publication date:
2006

Document Version
le PDF de l'éditeur

DOCTRINE

RFID: quelques réflexions introductives à un débat de société

Denis DARQUENNES et Yves POULLET[1]

I. Réflexions introductives

A. Définition

1. La **RFID**, «*Radio Frequency IDentification*», est une puce fonctionnant comme un terminal et qui, grâce à un dispositif technologique, permet le marquage et la lecture sans contact des marchandises ou du corps des individus, auxquels cette puce est intégré.

La structure technique de ces dispositifs est la suivante:

- une mémoire qui peut atteindre une grande capacité, organisée autour d'un microprocesseur;
- un dispositif de communication sans contact, grâce à une antenne d'émission à distance reliée au microprocesseur; au plus l'antenne est grande, au plus loin pourra s'effectuer la lecture;
- un mécanisme de production d'énergie, assuré soit par une pile interne, soit par les réactions du bobinage de l'antenne à la traversée d'un champ électromagnétique, ce qui dispense de piles et assure un usage illimité.

Ces éléments sont regroupés pour constituer des puces miniatures, appelées de façon synonyme «RFID», «smart tag», «radio-tag» ou «*transponder*» (*transmitter/responder*). Ces puces peuvent être lues à distance par un dispositif de lecture (mobile ou stationnaire), qui est également appelé «*transceiver*» (*transmitter/receiver*).

Ces éléments n'ont de sens qu'à l'intérieur d'un **système RFID**, qui combine les RFID tags, les lecteurs, les bases de données et les réseaux qui, en interaction, permettent la collecte, la transmission, le traitement et le stockage des données générées par le RFID ou liées à la possession de celui-ci. Ce système doit être considéré comme un tout.

B. Typologies

2. La définition elle-même autorise la distinction entre trois types de RFID ou tags et ce, selon la passivité ou non du dispositif mis en place:

- les tags *actifs*, qui sont équipés d'une source d'énergie autonome (pile ou capteur solaire) et

1. Denis DARQUENNES est informaticien, physicien et DGTIcien. Il est chercheur au CRID (FUNDP/Namur) (Denis.darquennes@fundp.ac.be). Yves POULLET est juriste et philosophe. Il est professeur aux Facultés de droit de Namur et de Liège et directeur du CRID (FUNDP/Namur) (Yves.poullet@fundp.ac.be).

d'une puce ; ils sont capables de se signaler seuls et/ou d'établir des dialogues plus construits avec le dispositif de lecture, qui se contente de recevoir le signal radio émis par un tag ; le coût de ces tags est élevé (20 $), même s'il est en diminution constante, et leur durée de vie limitée par la batterie ;

– les tags *semi-passifs* n'initient pas de communication avec le lecteur, mais sont quand même équipés de batteries qui permettent à la puce de stocker des valeurs de type physique, comme la température, la pression ... Ce type de tag est donc en général couplé à des capteurs physiques, constituant des petits détecteurs sans fils pouvant servir à contrôler des facteurs environnementaux (p. ex. le contrôle d'une consommation énergétique). Leur coût peut aller de 10 à 100 $ par pièce ;
– les tags *passifs*, qui sont les plus répandus, sont excités par induction électromagnétique (en l'occurrence par l'onde émise par le lecteur – *forward channel*) et émettent en retour, selon des fréquences radio bien définies, une suite alphanumérique fixe (*backward channel*). Comme ces tags ne renferment aucune batterie, leur durée de vie est illimitée. Leur coût est réduit (de 20 cents à quelques dollars) ; ce coût est fonction de la sophistication de la puce (taille de la mémoire ou capacité d'encryptage).

3. À cette première distinction, on ajoute celle relative au « niveau d'intelligence » des différentes RFID. Ainsi, on distingue selon ce critère, par ordre croissant :

– les tags passifs, qui retournent un identifiant fixe ;
– les tags dits « *Read/Write* », qui retournent un identifiant qui peut être réinscrit par le lecteur ;
– enfin, les tags intelligents, qui peuvent entretenir un dialogue soutenu avec le lecteur, comprenant une variété d'échange de données.

C. Éléments

4. Trois éléments constituent le dispositif du RFID. Le premier est la façon dont on décrit l'objet animé ou non porteur du RFID ; le deuxième a trait aux modalités de transmission des données de la RFID (RFID passifs) ou générées par ce dernier (RFID actifs ou semi-actifs) ; le troisième envisage les bases de données vers lesquelles sont dirigées les transmissions ainsi opérées.

a) L'identifiant de l'objet

5. Depuis 25 ans, le code UPC (pour « *Universal Product Code* » – ou « *bar code* ») est le principal moyen utilisé pour identifier les produits. Cette technique a fait ses preuves et a grandement aidé à réduire les coûts et à accroître l'efficacité et les rendements des activités liées à la manutention des produits et leur contrôle de qualité. Elle souffre cependant de certains handicaps (comme l'impossibilité de lire plus d'un produit à la fois, la nécessité pour le lecteur de voir le code-barres à courte distance, une identification limitée aux catégories de produits) qui poussent les acteurs économiques à la remplacer par le code EPC (*Electronic Product Code*).

L'EPC est encodé sur les tags RFID précédemment décrits. La structure du code EPC est la suivante : il s'agit d'un code de 96 bits comprenant un en-tête de description (*header*) sur 8 bits, un

préfixe identifiant de l'entreprise (*EPC Manager Number*) sur 34 bits, une référence du produit (*Object Class*) sur 20 bits et un numéro de série du produit sur 34 bits (*Serial Number).*

Exemple de structure du code EPC

016.37000.123456.100000000			
Header	EPC Manager	Object Class	Serial Number

Un RFID-tag peut également renfermer d'autres informations qu'un code EPC, comme des données biométriques (p. ex. une image digitalisée, une empreinte digitale ou une photographie) ou des données destinées à empêcher le vol d'articles dans les magasins. On parle alors d'EAS (*Electronic Article Surveillance Systems*).

Grâce à la technologie RFID, ce n'est plus un type de produit qui est identifié (comme c'est le cas avec un code-barres), mais chaque article individuellement. Pour tout produit, il sera alors possible de connaître à son propos une foule de renseignements, comme la date à laquelle il a été fabriqué, comment il a été transporté, quand il a été mis en rayon, vendu, jeté, recyclé.

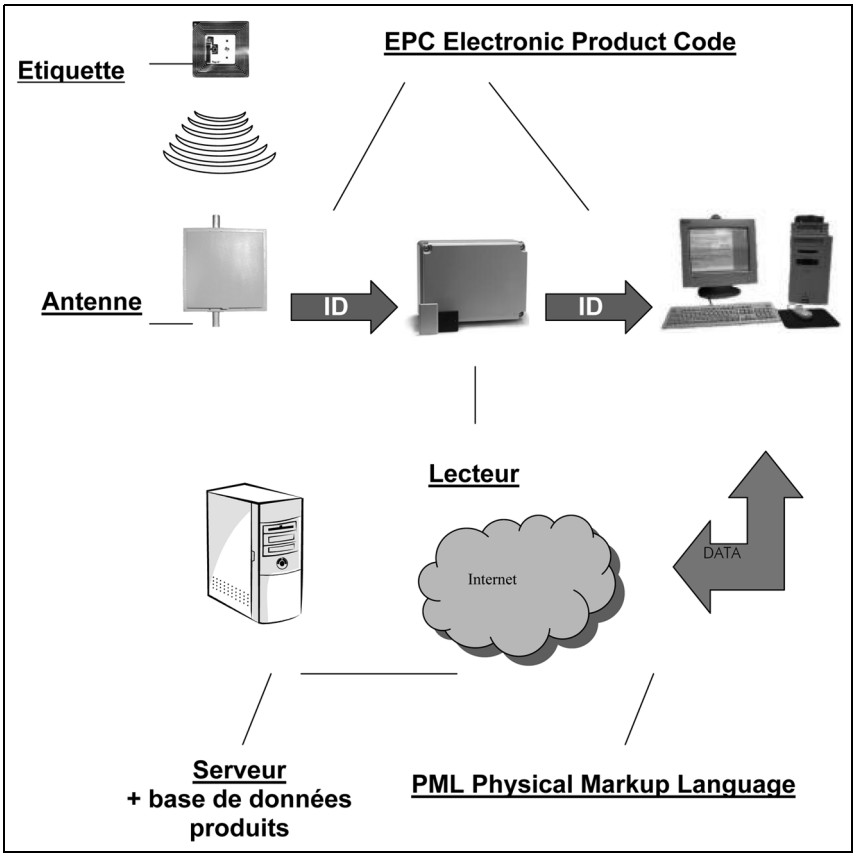
b) La transmission

6. La technologie RFID est intimement liée à l'internet. Les données concernant un objet ne sont pas nécessairement stockées sur sa puce, cette dernière reprenant surtout un identifiant. Comme l'adresse IP permet d'identifier un nom de domaine, et donc un site internet, l'identifiant, dont on a souligné la précision, va lier un objet aux données qui le concernent et qui sont stockées sur un serveur. On ajoute que la comparaison ne s'arrête pas là, mais de la même manière que la correspondance entre les adresses IP et les noms de domaine s'appelle le DNS (*Domain Name System*), on utilisera pour le monde des objets l'acronyme d'ONS (*Object Name System*) pour signifier cette même correspondance (voy. le schéma p. 258).

7. Quand un tag RFID est scanné par un lecteur, il renvoie par onde son code unique. Le lecteur utilisera ce code pour découvrir les informations spécifiques à cet objet stockées en mémoire. Les informations seront alors encodées selon le format standard PML (*Product Markup Language*), ce qui permettra aux applications liées au lecteur d'interagir intelligemment avec le produit. Un *Object Naming Service* (ONS) renseigne les systèmes informatiques sur la localisation de l'information relative à tout objet portant un tag RFID. En bout de chaîne, se trouvent les bases de données «produits» (ou autres systèmes logistiques terminaux), qui stockent les informations relatives aux objets marqués par des radio-tags. L'accès au lecteur et à sa base de données correspondante est nécessaire avant que l'information stockée sur un radio-tag puisse être obtenue et comprise.

La technique RFID permet d'éviter les limitations rencontrées par la technique des codes-barres. En particulier, la lecture (d'un ou plusieurs tags simultanément !) peut se faire sans que la puce ne soit placée à proximité immédiate du lecteur comme en matière de codes-barres (*remote reading)*. Par ailleurs, chaque produit est identifiable individuellement, et on peut même lui ajouter des informations durant son cycle de vie.

Schéma de la chaîne objet – base de données produits via internet



8. En ce qui concerne la transmission elle-même, elle s'opère suivant l'une des quatre plages de fréquence utilisées par la technique RFID.

Tableau

Caractéristiques/ Fréquences	125 à 135 kHz	13,56 MHz	860 à 960 MHz	2,45 GHz
Types de fréquence	Basse	Haute	UHF	Hyper
Distance de lecture et d'écriture	10 cm	0,5 mètre	De 2 à 5 mètres	Une dizaine de mètres
Vitesse de transfert des données	Lente (60 bits)	Rapide (2 K bits)	Rapide	Très rapide (plus de 512 K octets)

De façon générale, plus la fréquence est basse, moins le débit des données transmises est important et moins la distance de lecture est grande.

Dans la conception technique des tags, il est également nécessaire de tenir compte, lors de cette transmission, de deux types de réglementations :

– celles qui interdisent certaines plages de fréquence pour ne pas perturber d'autres types de transmissions ;
– celles qui visent à protéger l'individu des rayonnements électromagnétiques.

9. Les normes ISO liées aux différentes fréquences sont:

Bande	Protocole électromagnétique « air »
125-135 kHz	ISO 18000-2
13,56 MHz	ISO 14443 (A/B) & ISO 15693 (ISO 18000-3 en devenir)
860-960 MHz	ISO 18000-6 en devenir (GEN 2)
2,45 GHz	ISO 18000-4 en devenir

– la norme ISO 11784: identification des animaux par radiofréquence;
– les normes ISO 10536 et ISO 14443 (A & B): norme générale pour les cartes d'identification (cartes de proximité);
– les normes ISO 10536 et ISO 15693: pour les cartes de voisinage;
– les normes ISO 18000: pour les tags RFID.

Il faut noter que d'un point de vue strictement technique, l'émission radio peut être atténuée par la présence de certains matériaux.

Tableau de l'incidence des matériaux sur la transmission du signal radio

Caractéristiques/ Fréquences	125 à 135 kHz	13,56 MHz	860 à 960 MHz	2,45 GHz
Influence du métal	Perturbation	Perturbation	Atténuation	Atténuation
Influence de l'eau	Aucune	Atténuation	Atténuation	Perturbation
Influence du corps humain	Aucune	Atténuation	Atténuation	Perturbation

Récents développements en matière de transmission: le protocole GEN 2 développé par l'EPC

10. Toujours à propos de la transmission, il est important de tenir compte de certains développements récents en matière de transmission, fruit du travail d'organisations privées ayant dans un premier temps travaillé en dehors du cadre de la normalisation de l'ISO, en particulier le protocole GEN 2 développé par l'EPC. EPCglobal est une joint venture entre EAN International (*European Article Numbering*) et l'UCC (*Uniform Code Council*). Elle est l'organisation internationale chargée de promouvoir le développement des technologies EPC. Nous reviendrons amplement (*infra*, n° 23) sur cette organisation, dont le rôle dans la définition des normes RFID et la régulation des dispositifs est essentiel.

Cette organisation a ratifié le protocole GEN 2 (protocole UHF génération 2), standard unique adapté à l'ensemble des réglementations régionales des fréquences (notamment celles de l'Europe et des USA) et qui garantit aux entreprises une interopérabilité optimale des produits RFID.

Ce standard présente comme propriétés la possibilité de crypter les communications, un accroissement significatif des vitesses de lecture et d'écriture des étiquettes radiofréquences, ainsi qu'une moindre vulnérabilité des signaux aux interférences.

EPCglobal a annoncé en décembre 2004 la publication du protocole GEN 2, standard unique pour les RFID, qui, jusqu'alors, étaient l'objet de trois standards techniques différents et incompatibles entre eux. Le standard unique choisi était indispensable pour produire des RFID en gros volume, à des prix réduits, frein principal au développement de cette technologie.

Le GEN 2 est ainsi la véritable pierre angulaire du système EPC. Il a été établi à partir des besoins des utilisateurs, a bénéficié du soutien des entreprises expertes de la RFID et a nécessité onze mois de collaboration au sein des groupes de travail réunis sous l'égide d'EPCglobal.

Ce protocole est actuellement soumis au processus de ratification de l'ISO, qui devrait l'incorporer aux standards ISO 18000 et ce, pour le milieu de l'année 2006.

c) Les bases de données associées aux réseaux RFID

11. Grâce à l'EPC, la technologie RFID est ainsi associée à un réseau de bases de données, réseau et bases accessibles par l'internet. Ces bases de données constituent, avec la puce, l'antenne et le lecteur, un quatrième élément des systèmes technologiques fondés sur la technologie des RFID. Elles permettent de collecter les données en provenance des RFID ou des lecteurs et celles associées à la possession du RFID (p. ex., la localisation de la personne), de les associer à d'autres données déjà stockées (p. ex. : les données sur le porteur du RFID et les données déjà reçues à son propos via le système), de les traiter et de générer des actions (p. ex. : lui présenter telle publicité) ou décisions vis-à-vis de la personne (déclencher un signal d'alarme lorsque le RFID non désactivé placé sur un objet laisse présumer un vol dans un magasin) ou du RFID lui-même s'il s'agit d'un RFID dit intelligent (*supra*, n° 3).

II. Les applications 2

12. À quoi sert et surtout peut servir cette technologie qui combine miniaturisation et lecture à distance ? Sans hésiter, on peut affirmer que la technologie de radio-identification devient pour beaucoup de secteurs d'activités un enjeu économique majeur. Sans doute, songe-t-on à la distribution et au transport, pour lesquels les premières applications ont été développées, mais beaucoup d'autres secteurs économiques sont également concernés. On les passe rapidement en revue non sans un œil sur le futur.

A. RFID et secteur de la distribution ou des services

13. Les libres-services et, de manière générale, le secteur de la grande distribution utilisent volontiers aujourd'hui la technologie du code-barres. Comme déjà expliqué, le passage à des codes EPC permet d'identifier les objets industriels à un niveau individualisé bien plus élevé, et surtout, grâce à la lecture à distance, de pouvoir les suivre à l'intérieur mais également à l'extérieur du magasin. Cette caractéristique des RFID permet à cette technologie de répondre à quatre problèmes rencontrés par le secteur de la distribution.

- Le commerce sans stock (*Supply-chain*) : un produit reçoit dès sa fabrication un identifiant qui va le suivre à travers toute la chaîne logistique du commerce. Les opérations de fabrication et de transport peuvent être déclenchées automatiquement à partir des données ainsi recueillies.
- Le magasin sans caissière et sans vol (*Billing*) : un chariot muni

d'une puce passe sous une arche ou la carte de fidélité du consommateur est munie d'une puce RFID. Le déplacement du consommateur au sein de la grande surface peut être enregistré à distance, et dans la mesure où le chariot dispose d'un équipement terminal visuel, on peut imaginer l'envoi, sur l'écran installé sur le chariot du consommateur, de publicités ciblées et ce, en fonction de la connaissance que l'on a de l'endroit où circule le consommateur qui conduit le chariot tagé et de la consommation opérée par ce dernier à ce moment-là, voire sur une plus longue durée. Le tag peut en outre être lu et inspecté pour éviter la sortie sans paiement ou la sortie d'un article sous couvert de l'étiquette d'un autre article. On ajoute que des déplacements suspects dans certaines zones du magasin pourront être détectés.

– Le développement de service en magasin (*cross-selling*) : lors d'un essayage de vêtements, la reconnaissance des articles permet de proposer immédiatement d'autres articles assortis.
– L'accompagnement d'un client ou de l'objet dans le temps, dans la mesure où la lecture du RFID à partir de la maison du possesseur de celui-ci permettra de lui envoyer via son terminal des suggestions ou de la publicité liées à l'achat du produit.

De manière générale, on note que les données accumulées par le système lors des passages du consommateur dans l'entreprise de distribution permettent de mieux connaître ses habitudes de consommation, et dès lors de lui proposer des produits ou services appropriés (maintenance, renouvellement, fidélisation). On peut concevoir que certains équipements ménagers au sein de la maison du consommateur soient équipés de RFID permettant de connaître l'état, par exemple, du contenu du frigo, permettant le déclenchement à distance d'une commande.

14. Actuellement au stade de l'expérimentation dans certaines chaînes de grands magasins comme Metro ou Wal-Mart, la phase de généralisation de l'utilisation des RFID dans le secteur de la grande distribution est attendue pour 2010.

Il est clair que c'est dans ce secteur que l'on attend – et espère – les plus grandes retombées économiques (sachant qu'aux USA, les pertes subies par l'industrie, à cause d'une mauvaise visibilité de la chaîne de production, évoluent entre $ 180 et $ 300 milliards par an). Il est clair que la technologie RFID permettra une gestion plus précise du niveau des stocks, une réduction des vols à l'étalage, une lecture plus rapide (tout en étant plus précise) des volumes de marchandise, une localisation plus rapide des produits dans la chaîne, permettant un retrait plus rapide de ces derniers, et un suivi des clients tant pour des raisons de sécurité que de marketing. Dans le secteur des services, on cite, à titre d'exemple, ces discothèques espagnoles[2] qui proposent à leurs clients de se faire inoculer une puce, ce qui leur permet de ne pas devoir subir les queues d'attente pour les vérifications d'usage aux entrées et de pouvoir, sans devoir sortir un franc pendant toute la durée de leur soirée, se voir présenter un relevé de toutes les consommations opérées.

2. *Cf.* le célèbre cas de la discothèque Baja Beach Club implantée aux Pays-Bas et en Espagne (http://www.baja.nl).

B. RFID et secteur de la santé

15. La Food and Drug Administration américaine (FDA) a lancé un programme de lutte contre la contrefaçon de médicaments reposant sur l'utilisation de RFID dans les emballages (*Food Drug Administration & Counterfeit Program*).

On étudie également l'implant de radio-tags sur les humains (la société Applied Digital Solutions et sa puce Verichip). Ces solutions peuvent être très utiles pour certaines catégories de patients à risque (Alzheimer ou souffrant de problèmes cardio-vasculaires, ou encore de diabète), dans la mesure où on pourrait insérer dans la puce les données médicales dites d'urgence, ce qui permettrait, en cas de besoin d'intervention vis-à-vis d'un patient incapable de s'exprimer, de lire à distance la puce et de connaître les contre-indications que révèlent ces données d'urgence. Le récent rapport du Groupe Européen d'Éthique de la Santé[3] développe nombre d'applications dont l'intérêt est évident. Ainsi un implant dans le corps d'un patient à maladie chronique comme le diabète permet de contrôler à distance, via le téléphone, l'état du patient diabétique, voire, dans le cadre d'un RFID interactif, de lui envoyer les impulsions nécessaires à un rétablissement de la situation compromise.

Ainsi, l'ancien secrétaire de la Santé du Président Bush, Tommy Thompson, propose d'implanter une micro-puce d'identification par radiofréquence (RFID) sous la peau des citoyens américains. Ces micro-puces seraient liées à une base de données informatisée créée par le département de la Santé des USA afin de stocker et contrôler les registres de santé de la Nation. La compagnie Applied Digital Solutions, qui fabrique les micro-puces, et dont Mr Thompson est un des directeurs, fait également pression sur les autorités britanniques de la santé pour lancer un projet semblable au Royaume-Uni. Les avantages médicaux sont évidents quand il s'agit d'accéder au dossier médical de personnes incapables de décrire leur état de santé.

C. RFID et secteur des transports

16. Les applications dans ce domaine sont multiples tant dans le domaine de la sécurité privée que publique. Par exemple, la surveillance de l'état des pneus d'une automobile (Michelin et Nokian Tyres) peut se faire grâce à une puce électronique relevant pression et température, la transmission se faisant via un téléphone portable. La gestion des bagages dans un aéroport est également à l'étude (projet développé en commun par l'aéroport d'Orlando avec Delta Airlines et l'US Department of Homeland Security). Enfin, le système E-Zpass permet de franchir les péages autoroutiers sans s'arrêter.

D. RFID et sécurité

17. Outre la détection des vols dans les magasins déjà évoquée (*supra*, n° 13), une étude est en cours sur la sécurisation des billets d'euros à la Banque centrale européenne. On songe également à introduire des radio-tags dans les badges d'accès aux zones contrôlées; ainsi en Australie, certains personnels de banque se voient implanter un RFID de manière à tracer leurs parcours au sein de l'entreprise et ce, pour des raisons de sécurité.

3. «Aspects éthiques des implants TIC dans le corps humain», Avis n° 20 du Groupe Européen d'Éthique des Sciences et des Nouvelles Technologies auprès de la Commission européenne, 16 mars 2005.

À propos de la sécurité publique, on sait que les passeports européens de nouvelle génération doivent incorporer une puce lisible sans contact. Suite aux attentats du 11 septembre 2001, les Américains ont imposé une échéance très courte pour l'entrée en vigueur de ces nouveaux documents (26 octobre 2005, reportée au 26 août 2006 par les Européens). Le choix technologique veillera cependant à ce qu'il ne soit pas possible de tracer les individus à leur insu. Par ailleurs, certains s'inquiètent de l'absence de sécurité ou de la faible sécurité qui entoure ces cartes à puces, dans la mesure où des lecteurs en possession de personnes autorisées pourraient facilement, vu le peu de protection de l'accès aux puces, lire à distance le contenu du passeport, voire le télédécharger.

Par ailleurs, l'« US Department of Homeland Security » développe un programme « US-VISIT » (*US Visitor and Immigrant Status Indicator Technology*), dont le but est de contrôler les 330 millions de personnes pénétrant chaque année aux USA par un des 55 points de passage frontières les plus importants, en obtenant « *the appropriate level of information to the right people at the right time …* ».

Les associations de défense des droits civils, comme CASPIAN, retiennent surtout l'effet « marketing » déloyal de la déclaration de Monsieur Thompson (*cf. supra*, n° 15) de se faire lui-même implanter une puce.

Elles redoutent également qu'un tel accès au dossier médical ne donne la latitude aux services médicaux de privilégier les blessés assurés sociaux.

Elles dénoncent également l'effet catalyseur des attaques terroristes pour encourager un usage plus répandu de la micro-puce d'identification.

Enfin, cette technique d'implant – dans son utilisation bancaire – soulève des problèmes de sécurité spécifiques (l'ID de l'implant étant diffusé en permanence, il pourrait être récupéré et réutilisé à des fins de vol).

Les RFID intéressent également les autorités publiques vu leurs soucis sécuritaires et leur lutte contre le terrorisme. Ainsi apprend-on l'existence du « Snorting Door Project », auquel la société SAP est partie prenante, qui viserait à détecter les comportements atypiques en surveillant les RFID disséminés dans la nature.

On cite également le projet d'IBM, appelé « *Person Tracking Unit* », visant à scanner les tags RFID sur les éléments d'une foule afin de suivre leurs mouvements à travers les lieux publics.

Récemment en Belgique, le Sénateur Brotchi proposait[4] d'inoculer une puce aux délinquants sexuels et ce, afin de prévenir des récidives. Il est clair que d'autres projets de suivi des délinquants seront certainement mis sur la table dans ces moments d'obsession sécuritaire.

E. RFID et paiements

18. Le but est de concevoir des cartes de paiement pouvant être reconnues à distance au moment d'un paiement. Ainsi Mastercard propose le principe du Pay Pass, une carte équipée d'une puce RFID permettant au client-porteur,

4. Proposition de loi visant à introduire la possibilité de recourir à un dispositif de surveillance électronique et à un traitement pharmacologique hormonal des agresseurs sexuels remis en liberté, *Doc. parl.*, Sén., sess. 2005-2006, n° 3-1816 du 13 juillet 2006.

sur présentation de cette dernière à proximité d'un lecteur, d'automatiquement valider l'achat. Ce système n'est cependant envisagé que pour les petites transactions. Le système américain Speedpass permet aux automobilistes d'acheter selon cette technique du carburant ou des fournitures dans le réseau des stations Exxon Mobil.

La société Applied Digital Solutions propose également une identification automatique, grâce à la puce implantée dans leur corps, de toute personne se préparant à utiliser sa carte de crédit. Bien sûr, cette proposition relance le débat sur l'acceptation par toute personne de l'implant d'une puce.

F. RFID et le secteur public

19. Le département de la Défense aux USA soutient un projet permettant de localiser et tracer les livres des bibliothèques locales. La US Food and Drug Administration (FDA) veut promouvoir l'usage (pour 2007) des RFID-tags dans la chaîne de production pharmaceutique, pour enrayer la contrefaçon dans ce secteur.

G. RFID et emploi

20. Le suivi des employés marqués par une puce RFID permet aux employeurs de détecter automatiquement les circuits anormaux ou les séjours prolongés de leurs employés.

Autre application : le ministre de la Justice du Land de Hesse en Allemagne a suggéré, en mars 2005, que les chômeurs de longue durée portent au pied un bracelet électronique, surveillance qui devrait les contraindre à davantage de discipline en vue de retrouver un travail. Il faut préciser que le tollé suscité par cette déclaration a contraint le ministère de la Justice de ce Land à publier une nouvelle communication rejetant cette réflexion, qualifiée d'absurde.

III. Les acteurs présents dans le débat des RFID et leurs positions

21. Si on trouve au premier chef, interopérabilité oblige, les organes de normalisation sectoriels ou intersectoriels qui veillent, outre à la définition des normes, à leur promotion, l'attitude des pouvoirs publics américains et européens mérite l'attention. Enfin, on élargira notre attention du côté des consommateurs et des organes en charge de leurs intérêts, comme la puissante Federal Trade Commission.

A. Les organes de normalisation

22. L'utilisation des technologies requiert une certaine harmonisation aux niveaux nationaux et internationaux. Cette harmonisation assure la compatibilité et l'interopérabilité entre différents fabricants et applications techniques.

De nombreux acteurs interviennent dans ce processus de standardisation des technologies RFID. Nous trouvons ainsi des organes de normalisation travaillant dans des secteurs bien déterminés particulièrement intéressés par les applications RFID. Ainsi :

– The Automotive Industry Action Group (AIAG), qui a développé les spécifications RFID pour

l'industrie automobile;
- The International Air Transport Association (IATA), qui étudie l'usage des technologies RFID pour la gestion des bagages;
- The International Civil Aviation Organization (ICAO), concernée par la lecture par machine des documents de voyage.

23. Des initiatives intersectorielles existent également. À côté des efforts des organes de normalisation développés par les organisations publiques de normalisation, on trouve des initiatives plus régionales, et surtout l'omniprésence en la matière de l'EPCglobal, organisation privée qui gère l'*Object Naming System*, et dont la constitution et les modes de gestion rappellent étrangement ceux des organisations privées en charge de l'internet (ICANN, W3C en particulier).
- The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC);
- The International Telecommunication Union (ITU), qui est l'agence des Nations unies spécialisée dans les télécommunications (surtout concernée au niveau RFID dans deux secteurs: the Radiocommunication Sector [ITU-R] and the Telecommunication Standardization Sector [ITU-T]);
- The State Driven Standardization Initiatives: organisation visant le regroupement et concordance d'efforts et d'initiatives de pays importants du Sud-Est asiatique (Chine, Japon, Corée) dans le domaine de la standardisation des technologies RFID;
- The European Radiocommunication Office (ERO), qui travaille sur des politiques de radiocommunication et d'allocation de fréquences importantes pour les technologies RFID;
- l'European Article Numbering (EAN) et l'Uniform Code Council (UCC), deux initiatives privées qui sont à la base de l'EPCglobal. L'EPCglobal est le résultat de la collaboration et de l'association (véritable joint-venture) entre EAN International et l'UCC; elle promeut l'EPC (*Electronic Product Code*).

24. À l'origine de la définition des standards de la technologie Auto-ID, se trouve l'Auto-ID Center, un partenariat entre 98 compagnies (parmi lesquelles Sun Microsystems) et six des plus grandes universités, leaders dans le domaine de la recherche.

En 1999, sous l'impulsion de l'Uniform Code Council (UCC), organisation privée de standardisation américaine, et de deux fabricants américains de produits de grande consommation (Gillette et Procter And Gamble), l'Auto-ID Center a démarré la conception d'une infrastructure globale d'identification par fréquence radio (RFID) de produits référencés selon un *Electronic Product Code* (EPC).

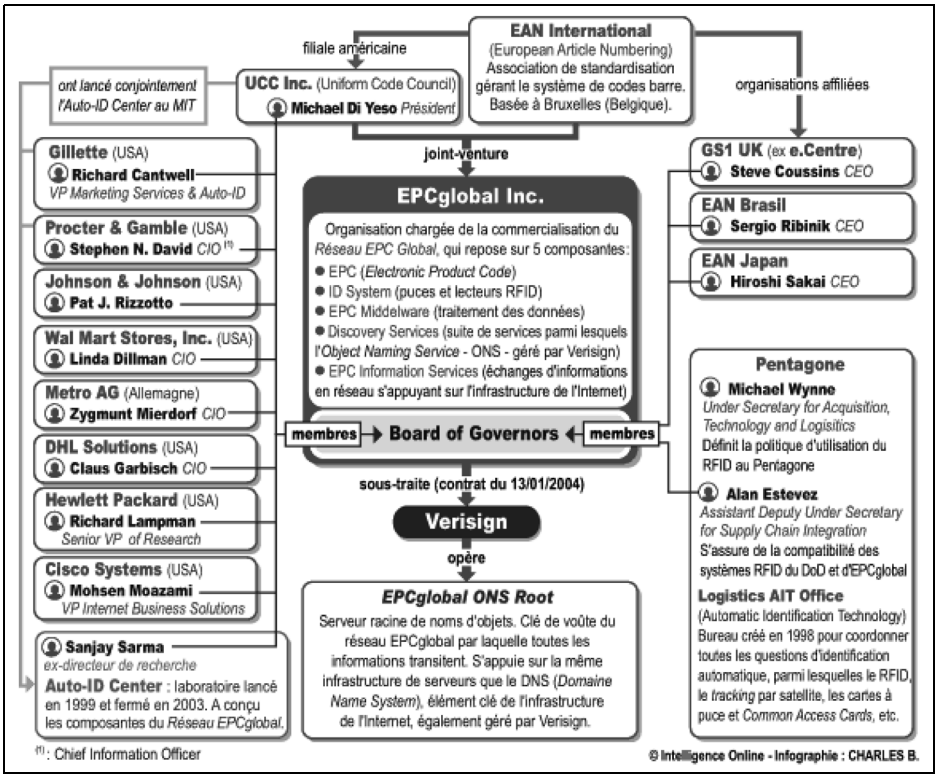
Associant le Massachusetts Institute of Technology (MIT) aux universités de Cambridge (Grande-Bretagne), Adélaïde (Australie), Saint Gallen (Suisse) et Keio (Japon), l'Auto-ID Center a abouti en 2003 au développement du Réseau EPCglobal. Celui-ci est fortement centralisé autour de l'*Object Naming Service* (ONS), dont la gestion a été confiée à l'américain Verisign, qui gère déjà les noms de domaine de l'internet.

L'Auto-ID Center a officiellement cessé ses activités fin octobre 2003 et a transféré ses technologies à l'EPCglobal Inc. (voy. schéma ci-dessous), une joint-venture entre l'association *européenne* de gestion des codes-barres,

EAN International (implantée à Bruxelles), et *sa filiale américaine*, l'UCC.

Dans les faits, l'UCC a nettement pris le pas sur sa maison mère. Lancée en novembre 2003 pour promouvoir l'utilisation du réseau EPCglobal, l'association EPCglobal Inc. est gouvernée par un conseil composé essentiellement de représentants de sociétés américaines, à l'exception de l'allemand Metro AG, et des filiales britannique, japonaise et brésilienne de l'EAN.

Schéma représentant la structure d'EPCglobal



La mainmise américaine s'est donc affirmée sur ce secteur stratégique. La société Verisign, déjà fort décriée pour ses abus de position dominante dans le système DNS (*cf.* l'affaire du service Site Finder[5]), se retrouve donc également au centre de l'ONS, ce qui a pour effet d'inquiéter les organismes concernés par la défense de la vie privée, notamment la CNIL française.

B. L'attitude des pouvoirs publics américains

25. Initialement, ce sont le département de la Défense des États-Unis ainsi que le secteur des grandes chaînes de distribution (Wal-Mart) qui ont donné à cette technologie un grand coup d'accélérateur. Ils ont ainsi demandé à leurs principaux fournisseurs de se préparer

5. Dans cette affaire, la société Verisign redirigeait les adresses internet en «.com» et en «.net» incorrectement orthographiées vers un site créé spécifiquement par elle. La société récupérait, au passage, de nombreuses informations concernant l'internaute à l'origine de l'URL erronée.

à incorporer cette technologie, leur laissant deux ans pour être opérationnels, à défaut de quoi leur contrat pourrait être résilié[6].

Au niveau du Sénat américain, un groupe influent de sénateurs républicains, membres de la «Senate Republican High Tech Task Force», prône un déploiement non réglementé des RFID. Ils ont le large soutien des organismes de technologie et de vente au détail de RFID. Leur argument central s'exprime comme suit: «*The Republican Senators would protect exciting new technologies from premature regulation or legislation in search of a problem. RFID holds tremendous promise for our economy, including military logistics and commercial inventory efficiencies, and should not be saddled prematurely with regulation*». Comme on le voit, les arguments économiques et militaires en constituent le poids principal.

Le Sénateur John Ensign, *Task Force's chairman* de ce groupe de sénateurs, le précise dans les termes suivants: «*Our policy platform reflects our desire to keep America at the forefront of technological advancement, and to encourage our country's most creative entrepreneurs*».

Ainsi, comme en matière de l'internet, l'autorégulation par le secteur sans intervention de l'État apparaît, aux yeux de certains politiciens américains, comme une manière de prolonger l'avance technologique et industrielle américaine dans le secteur et de conserver, nonobstant la mondialisation souhaitée des technologies en cause, la mainmise américaine sur la gestion du développement de ces technologies dans la mesure où les organes de normalisation et de gestion de l'ONS seront dans les faits contrôlés par les entreprises américaines.

C. La réaction des pouvoirs publics européens

26. La technologie RFID est une affaire essentiellement américaine et son développement est mené essentiellement par la demande du secteur privé, en vue d'apporter une réponse à des problèmes économiques concrets. La régulation, comme nous l'avons vu, repose sur l'initiative de regroupements d'industries et d'organismes internationaux des Nations unies; elle concerne les standards techniques permettant une harmonisation et une interopérabilité des systèmes RFID. En ce qui concerne l'usage de ces derniers, ce sont les industriels eux-mêmes qui fixent les règles de conduite, notamment en matière de protection des données personnelles et de la vie privée.

Cette dynamique s'impose également en Europe, où l'on s'attend à ce que cette technologie y fasse son entrée de façon affirmée dans les toutes prochaines années. Ce fait a incité la Commission européenne à prendre les devants et à mettre sur pied (depuis avril 2005) un «groupe de travail RFID», présidé par Monsieur Gérald Santucci.

Bien que l'on estime que l'identification RFID par produit ne sera pas possible avant 2008 (en raison des coûts encore trop élevés et de l'incapacité technique de l'infrastructure informatique actuelle d'absorber la quantité de données générées – identification de

6. Dans le cas de Wal-Mart, cette stratégie de l'ultimatum et du diktat avait cependant peu de chances d'aboutir, car elle n'était pas accompagnée d'investissements réels et d'études d'impact sur les systèmes de distribution, les processus métier et la logistique de l'entreprise américaine. En d'autres mots, elle aurait dû assumer sa part de responsabilité dans le changement qu'elle impose et apporter aide et conseils à ses fournisseurs. La conséquence est qu'elle subit maintenant des retards et problèmes logistiques.

plus de 268 millions de fabricants, ayant chacun plus d'un million de produits, soit de l'ordre de 100.000 milliards d'objets au total !), sa capacité potentielle à tracer, «géolocaliser» et profiler les individus, ainsi que leurs actions, incite la Commission à lancer dès à présent une réflexion sur ce sujet.

Le groupe de travail devra ainsi rassembler les informations ayant trait aux technologies et applications RFID, actuellement dispersées dans les différents services de la Commission. Il devra également analyser l'état des réglementations couvrant les RFID en vigueur dans les différents États membres de l'Union. Ce travail sera le prélude à un débat sur la réalisation progressive d'une réglementation européenne des RFID. Cette attitude en faveur d'une réglementation publique des RFID s'écarte de celle prônée outre-Atlantique.

27. La Commission a également pour but d'ouvrir le débat au niveau européen, avant la survenance d'une crise. Sa crainte (justifiée) est de voir l'Europe être sous-représentée dans les séances de travail tenues au niveau mondial, en général à Washington, séances où se décident les développements de la technologie RFID[7].

Cette volonté d'être présent dans le développement de la technologie RFID justifie le soutien par la Commission d'une dizaine de projets RFID qui concernent tous des applications industrielles innovantes de ces étiquettes intelligentes, le secteur le plus important étant celui de la chaîne d'approvisionnement. La granularité de l'identification n'atteint pas le stade ultime des produits pris individuellement, qui ne sera atteint qu'en 2008. Parmi les autres secteurs concernés, nous trouvons l'industrie des transports (avec SMMART pour «*System for Mobile Maintenance and Accessible in Real Time*»), et en dehors du domaine de la chaîne d'approvisionnement, l'environnement (traçage des produits polluants), le transport aérien (étiquetage électronique des bagages et enregistrement automatique des passagers), l'agriculture (programme Idea de marquage électronique des animaux).

D. Les consommateurs et les entreprises

28. L'étude des applications RFID témoigne des enjeux pour la société et les citoyens des utilisations des RFID. Le traçage qu'il permet des objets, et au-delà des personnes qui les portent, peut constituer une atteinte à la vie privée et, en tout cas, rend le consommateur plus vulnérable aux actions promotionnelles des entreprises, l'employé plus contrôlé par son employeur et le citoyen plus surveillé. Plusieurs groupes se sont ainsi constitués pour lancer le débat au niveau citoyen et dénoncer les risques d'abus de telles technologies, ainsi on cite principalement l'organisation américaine EPIC (Electronic Privacy Information Center), de même que le groupe anglais CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) fondé par Katherine Albrecht.

Ces organismes se sont montrés très attentifs et vigilants face aux «expériences» menées dans le do-

7. À titre d'exemple, le workshop sur les RFID qui s'est tenu à Washington en juin dernier regroupait les acteurs suivants: les développeurs en RFID, les consultants Philips Semiconductors, Texas Instruments, Intel, Sun Microsystems, Accenture et CapGemini, EPCglobal, les Grocery Manufacturers of America, la National Retail Federation, certains groupes de défense comme l'Electronic Frontier Foundation, l'Electronic Privacy Information Center, ainsi que le groupe Caspian (Consumers Against Supermarket Privacy Invasion and Numbering), et, finalement, les utilisateurs des RFID comme Marks & Spencer, Procter & Gamble et Wal-Mart.

maine des RFID par certaines entreprises, comme le fabricant de rasoir Gillette (photographie du client déclenchée automatiquement par la puce associée au produit acheté) et la chaîne de supermarchés Tesco. Ces organismes ont prôné un boycott de ces firmes.

Ainsi, ils dénoncent au travers de leur action les dérives associées à la technologie RFID. Ainsi en est-il du livre « *Spychips: How Major Corporations and Government Plan to Track your Every Move with RFID* », écrit par Katherine Albrecht et Liz McIntyre[8]. Par ailleurs, ils attirent également l'attention sur les stratégies mises en place par les partisans de cette technologie pour progressivement la disséminer dans la société, en commençant par des secteurs clés comme le médical ou l'armée. Les arguments « sécuritaire » et du sauvetage de vies humaines permettent à ces technologies d'acquérir une « force de conviction » la rendant incontournable dans la vie de tous les jours.

En Allemagne, la Foebud, principale association de défense de la vie privée engagée dans le combat contre l'intrusion des RFID-tags et travaillant sur des solutions techniques visant à limiter les effets des puces radio, a obligé la chaîne de supermarchés Metro à faire preuve de transparence dans son expérience grandeur nature d'utilisation de puces à radiofréquence. Le groupe a ainsi reconnu, d'une part, avoir distribué, à l'encontre de ses promesses, 10.000 cartes de fidélité équipées de puces RFID et, d'autre part, que le dispositif technique permettant de désactiver automatiquement les puces à la sortie du magasin n'était pas au point. Sous la pression de la Foebud, le groupe Metro a finalement renoncé à poursuivre cette expérience.

Le groupe CASPIAN a de même dénoncé les tests secrets (observation via webcam de clients achetant certains produits marqués par une radio-puce) des étiquettes intelligentes menés dans certains magasins de la chaîne Wal-Mart, par ailleurs principal promoteur de la technologie RFID. La chaîne de magasins a finalement pris du retard dans l'implantation de cette technologie, mais surtout pour des raisons de coûts non assumés et de problèmes logistiques.

Signalons enfin l'attitude plus positive du grand groupe de distribution Marks & Spencer, qui a annoncé clairement, au vu des critiques ayant frappé ses concurrents, son intention d'être très transparent dans la gestion des tests qu'il effectuera avec les étiquettes électroniques. L'association CASPIAN a salué cette attitude jugée responsable.

29. Ces divers exemples sont la preuve que la vigilance des organisations citoyennes se justifie pleinement : elles exercent un réel pouvoir de contrainte efficace vis-à-vis des grands groupes commerciaux, trop enclins à satisfaire uniquement leurs intérêts économiques. Par leur action, les organisations essayent de sensibiliser les futurs consommateurs et les citoyens en général aux possibles abus de cette technologie naissante de la part des entreprises, des gouvernements ou de pirates.

30. Du côté des entreprises clientes des produits RFID, l'inquiétude s'est également propagée au niveau de certains chefs d'entreprise, ainsi que dans certains milieux professionnels, qui redoutent l'usage pouvant être fait des systèmes RFID dans la concurrence déloyale et l'espionnage industriel.

8. K. ALBRECHT et L. MC INTYRE, *How Major Corporations and Government Plan to Track your Every Move with RFID*, Spychips Collection, Penguin, Nelson Current, octobre 2005.

De même, ils ont contesté le monopole de la société Verisign dans la gestion des codes EPC d'identification des objets, permettant à cette dernière d'en faire profiter de façon privilégiée son réseau de partenaires ou les entreprises de son groupe.

E. La Federal Trade Commission

31. La US Federal Trade Commission (FTC) est une juridiction administrative américaine en charge des litiges de consommation et de la surveillance du respect de pratiques loyales dans les relations entre entreprises et consommateurs. On connaît le rôle important qu'elle joue dans la régulation des technologies de l'information et de la communication, en particulier dans la défense de la protection des données des citoyens face aux entreprises. Dans le débat relatif aux RFID, la FTC entend jouer le même rôle. Ainsi, elle a publié un rapport (« *Workshop Report from de Staff ot the Federal Trade Commission* » – march 2005[9]) un jour après celui du groupe sénatorial américain déjà évoqué (*supra*, n° 25). Ce rapport conclut dans le même sens que les sénateurs. La FTC annonce en effet qu'elle ne publiera pas de directives à l'adresse des compagnies déployant la technologie RFID. Elle justifie cependant son attitude non par une opposition de principe à la réglementation de cette technologie, mais par le fait qu'elle juge prématurée une intervention réglementaire. Ainsi, dans un premier temps, elle laisse aux soins des détaillants ainsi qu'aux industries de la RFID d'éduquer les consommateurs aux usages des collectes de données et d'identification rendus possibles par cette technologie. Son objectif principal est de surveiller l'évolution de l'autorégulation en cours et de n'intervenir que lorsque cela s'avère approprié. Sur base des constats qu'elle pourra opérer, la FTC n'écarte cependant pas, bien au contraire, la possibilité de publier des directives dans le futur.

32. Lors de son « Workshop » de mars 2005[10], la FTC identifie les principaux éléments économiques susceptibles d'entraver le développement ou la progression de l'usage des radio-tags.

Le premier de ces facteurs est le coût de réalisation des tags, qui est encore trop élevé à l'heure actuelle (entre 20 et 40 cents pour les tags passifs) et encore trop éloigné de l'objectif des 5 cents par tag, coût qui ne sera sans doute pas atteint avant 2008.

Les autres coûts incontournables dans le développement de cette technologie concernent le hardware (comptant pour 3 % des dépenses) et surtout le software (comptant pour 75 % (!) des dépenses).

Les autres facteurs inhibiteurs de cette technologie sont le manque de standardisation des fréquences utilisées en RFID, les défis techniques, comme la précision dans la lecture ainsi que l'interférence et l'influence des substances externes, et, enfin, le manque de connaissance par les utilisateurs finaux des principes de fonctionnement de cette technologie.

33. Sur ce dernier point, la FTC tire la sonnette d'alarme. Le défi essentiel à relever est de rassurer le consommateur sur la protection de ses données collectées à travers la technologie RFID. Ainsi, la FTC propose les conclusions suivantes :

9. Disponible sur le site www.ftc.gov/bcp/workshops/rfid/index.htm.
10. *RFID : Radio Frequency Identification : Applications and Implications for Consumers*, A Workshop Report from the Staff of the Federal Trade Commission (March 2005), http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf.

- les initiatives de l'industrie peuvent jouer un rôle important en réponse aux inquiétudes liées à la vie privée soulevées par la technologie RFID; le but de ces initiatives doit être la transparence;
- plusieurs des problèmes potentiels relatifs à la vie privée sont inextricablement liés à la sécurité des bases de données regroupant les informations collectées via les systèmes RFID; comme dans tout contexte dans lequel des informations à caractère personnel sont collectées auprès de consommateurs, les compagnies utilisant les RFID à des fins de collectes doivent implémenter des mesures raisonnables et appropriées pour protéger les données stockées dans les bases de données reliées aux systèmes RFID;
- l'éducation des consommateurs est indispensable pour protéger leur vie privée; l'industrie, les associations privées de défense et le gouvernement doivent développer des outils de formation expliquant le fonctionnement de la technologie RFID, dans quelles situations elle peut se rencontrer et quels choix sont possibles vis-à-vis de son usage;
- la réalisation de guides de conduite, évoluant avec la technologie et les dispositions légales, est vivement encouragée. Ces guides doivent s'appuyer sur les concepts suivants: «consumer notice», «consumer choice», «consumer education» et information sur les politiques de rétention, utilisation et protection de toutes les données à caractère personnel obtenues via l'usage des EPC code, en respect de toutes les législations applicables.

IV. Les RFID face à la loi

34. Notre propos est limité. Il constitue une simple esquisse des questions soulevées par les RFID au regard de l'application des lois. À cet égard, on songe en particulier à deux types de législations: premièrement (A), celles relatives à la cybercriminalité, dans la mesure où l'installation d'une RFID peut être un outil de collecte d'informations constitutif d'une infraction, et surtout dans la mesure où la collecte d'informations permise par cette technologie peut être captée par des tiers non autorisés lors de leur transmission. L'application des législations de protection des données (B) soulève de nombreuses questions sur le champ d'application de ces législations et, à supposer que ces législations soient applicables, sur les conséquences qu'il faut tirer des dispositions de ces législations. Sur ce point, nous suivrons les réflexions du Groupe dit de l'article 29[11] et du Groupe Européen d'Éthique des Sciences et des Nouvelles Technologies auprès de la Commission européenne[12], qui montrent qu'au-delà de la protection des données, certaines applications des

11. Document de travail sur les questions de protection des données posées par la technologie RFID, document du 19 janvier 2005 WP n° 105, disponible sur le site de la Commission: http://www.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_fr.pdf
12. Disponible sur le site: http://www.ec.europa.eu/european_group_ethics/docs/avis20_fr.pdf.

RFID soulèvent des questions bien plus essentielles de dignité humaine. Sur ce point, il sera intéressant de s'interroger sur la façon dont l'autorégulation (C) et la technologie (D) elle-même peuvent concourir à une meilleure protection des données.

A. Les lois sur la cybercriminalité

35. La Convention européenne sur la cybercriminalité du 23 novembre 2001[13] prévoit un certain nombre de nouvelles infractions, dont certaines sont applicables aux radio-tags. En effet, tenant compte des articles 2 (accès illégal) et 3 (interception illégale) de la section 1 (droit pénal matériel), sont érigés en infraction pénale, d'une part, l'accès intentionnel et sans droit à tout ou partie d'un système informatique (dans la mesure où les radio-tags sont considérés comme un système informatique, puisque permettant un traitement automatisé de données), ainsi que, d'autre part, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques (dans la mesure où les données transmises par radio-tag sont des données informatiques).

Ainsi, l'accès aux données contenues dans une puce RFID par une borne de lecture placée par une personne non autorisée constitue un *hacking*, de même que l'interception des données transmises par une RFID à une borne située à distance est punissable. On insiste sur la nécessité, tant pour les concepteurs des applications de cette technologie que pour ceux qui les utilisent, d'entourer les dispositifs de transmission et les produits RFID d'une sécurité appropriée. Ainsi, le cryptage automatique des transmissions, les contrôles d'accès à la puce sont autant de mesures que les obligations de sécurité déduites des législations de protection des données imposent.

B. Les lois de protection des données

a) Les applications RFID tombent-elles nécessairement sous le champ d'application des lois de «protection des données à caractère personnel» ?

36. La particularité des RFID consiste dans le fait qu'elles introduisent un lien entre un objet et des informations relatives à cet objet (sa chaleur, sa localisation, *etc.*), cet objet fût-il le corps lui-même. Sans doute, et c'est le but, peut-on à partir de là inférer des informations relatives au possesseur de l'objet ou à celui qui le porte et déclencher certaines actions curatives, publicitaires ou autres vis-à-vis de lui. Pour autant, il n'est pas nécessaire de connaître son identité ni même de la rechercher. Ce qui importe, c'est que le sujet X, porteur du RFID, se trouve à tel endroit, ait fait tel achat, soit en possession d'un titre de transport valable.

Peut-on, à leur propos, parler de données à caractère personnel, au sens de l'article 2, a), de la directive 1995/46/CE ? La notion d'identité est au cœur de la définition de ce type de données. Sans doute cette définition est-elle large, dans la mesure où, comme le rappelle le Groupe de l'article 29 à propos des cookies[14] ou des RFID[15] en invoquant le considérant 26,

13. Convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001 (STE, n° 185).
14. Dans le cadre des cookies, les données générées par les cookies se réfèrent à un terminal et une adresse IP, et non à l'individu possesseur du terminal ou de l'adresse IP. Le rapprochement avec le cas des RFID est intéressant, dans la mesure où les personnes qui bénéficient des données générées par les cookies n'ont de même aucun besoin de connaître l'identité exacte de la personne afin d'agir sur elle.
15. «Working document on data protection issues related to RFID technology», 19 janvier 2005, *op. cit.*

l'« identifiabilité » se conçoit en fonction de « *l'ensemble des moyens susceptibles d'être raisonnablement mis en place, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne* ». Outre que, comme le reconnaît le Groupe lui-même, cette approche même large de la notion de données à caractère personnel ne permet pas de couvrir tous les cas[16], elle reste théorique dans la mesure où ceux qui exploitent les données nées des cookies ou des RFID ne cherchent pas à identifier la personne concernée, mais simplement à profiler[17] le détenteur d'un terminal pour décider vis-à-vis de lui de certaines actions.

37. En d'autres termes, les données générées par les RFID ne sont pas nécessairement des données à caractère personnel. Peut-être une autre définition de la donnée à caractère personnel est-elle nécessaire, fondée cette fois sur la notion de « contactibilité »[18], c'est-à-dire le fait que des données permettent ou non de contacter un individu, d'influencer son comportement ou de prendre une décision vis-à-vis de lui, mais en l'état actuel du droit ce critère n'est pas retenu[19].

b) L'application des lois de protection des données : examen de l'avis du Groupe dit de l'article 29

38. Le Groupe de l'article 29 s'est inquiété de la généralisation de l'usage des identifiants électroniques à fréquence radio et des conséquences pour la vie privée des citoyens. Ce Groupe rassemble les différentes autorités de protection des données personnelles des 25 pays membres de l'Union européenne et le Contrôleur européen à la protection des données.

16. Sur ce point, le Groupe de l'article 29 est prudent. Il conclut que la réponse à la question de l'application de la directive sera à donner pour chaque application de la technologie RFID, après examen au cas par cas de la présence ou non d'un traitement de données à caractère personnel, tel que défini par la directive générale « protection des données ». Tout utilisateur des informations collectées au moyen de la technologie RFID devra donc au préalable évaluer si cette dernière est effectivement considérée comme « donnée à caractère personnel ». En fait, si l'information du radio-tag ne contient aucun renseignement personnel et n'est pas non plus combinée avec des données à caractère personnel, alors la directive « protection des données » ne s'appliquera pas.
17. Cette notion de profilage pourrait conduire à considérer que la recherche de l'identité s'opère alors par référence non à des données administratives (nom, prénom, adresse, *etc.*), mais par rapport « *à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* », comme le permettrait le dernier membre de phrase de l'art. 2, a), de la directive. Ainsi, un cookie serait une donnée à caractère personnel lorsque le nombre de données collectées grâce au cookie permettrait de constituer une image suffisamment précise de la personnalité de l'individu, peu importe l'aspect considéré (profil économique, psychologique ou physiologique). Cette piste apparaît plus féconde, mais elle se heurte au fait que dans l'esprit de la directive, ces profils ne sont pas pris pour eux-mêmes et ne constituent des données à caractère personnel que dans la mesure où ils permettent de découvrir l'identité de la personne concernée.
18. Sur ce critère, les réflexions de Y. POULLET et J.-M. DINANT, in « Information Self-determination in the Internet area », Report on the application of data Protection principles to the worldwide telecommunications networks, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (T-PD), Strasbourg 13 décembre 2004, (2004)04 final. En ligne sur le site du Conseil de l'Europe.
19. Dans un autre écrit (Y. POULLET, « Pour une troisième génération de législations de protection des données », *JusLetter*, n° 3, octobre 2005), nous avons essayé de montrer combien la directive 2002/58/CE, lorsqu'elle réglemente les données de trafic et de localisation générées par l'utilisation des services de communication, se soucie peu du fait que ces données soient des données à caractère personnel. « *La définition même des 'données', dont la protection est au cœur même de la directive récente ne suit pas exactement celle de 1995. Les définitions de 'données de trafic' et de 'localisation' reprises à l'article 2 évitent soigneusement les expressions de 'données à caractère personnel', qui circonscrivent pourtant le champ d'application de la directive 95/46/CE, dont la directive de 2002 ne serait qu'une application. Autant, l'article 2 c) que le considérant 14 de la Directive définissent la donnée de localisation par la seule référence à l'équipement terminal d'un utilisateur. Lorsqu'il s'agit de commenter la notion de donnée de trafic, le considérant 15 parle 'd'informations consistant en une dénomination, un nombre ou une adresse, fournie par celui qui émet la communication ou celui qui utilise une connexion pour effectuer la communication'.*
Qu'est-ce à dire ? Ces données peuvent ne pas être des données à caractère personnel, en d'autres termes que la recherche du lien avec une personne identifiée ou identifiable n'est plus nécessaire ».

La CNIL française, par la voix de son commissaire, Mr Philippe Lemoine[20], avait introduit le débat en identifiant quatre «pièges» concourant à une minorisation des risques que présente cette technologie en matière de protection des données personnelles et de la vie privée:

- l'insignifiance seulement apparente des données: en effet, les volumes d'informations que l'on peut analyser grâce à un maillage dense sont infinis et, en tout cas, peuvent donner lieu à des applications pour le moins sensibles[21];
- la priorité donnée aux objets: s'agit-il vraiment de données personnelles ? Les applications relatives aux personnes sont plus éloignées dans le temps, et ceci pour une raison de logique économique (il y a plus d'objets que de personnes), ce qui contribue à endormir la vigilance[22];
- la logique de mondialisation: les standards sont définis dans des centres de recherche essentiellement américains, c'est-à-dire hors de la tradition européenne «informatique et liberté»; ils s'imposeront à l'ensemble de la planète;
- la non-vigilance individuelle: la collecte se fait subrepticement et même automatiquement; il n'y a pas nécessairement de possibilité de stopper la communication, et comme il n'y a pas de batterie, la durée de vie du dispositif est illimitée.

39. À l'instar des organisations citoyennes de défense des droits des consommateurs, le Groupe de l'article 29 souligne les effets bénéfiques de l'utilisation des RFID pour les entreprises, les individus et les services publics, mais également les possibilités de «violation de la dignité humaine et des droits des protections des données» induites par certaines applications RFID (immixtion dans la sphère privée grâce au maillage dense des milliers d'objets qui entourent une personne, et permettant de profiler cette dernière).

Le Groupe de l'article 29 a ainsi publié un premier document de travail qui poursuit deux objectifs différents selon le public ciblé et les exploitants, d'une part, et selon les concepteurs de cette technologie, d'autre part:

- fournir à ceux qui exploitent la technologie RFID des orientations concernant l'application des principes fondamentaux définis dans les directives communautaires (c'est-à-dire tant la Dir. 95/46/CE «protection des données» que la Dir. 2002/58/CE dite «protection des données et secteur des communications électroniques»);
- fournir aux concepteurs de cette technologie, ainsi qu'aux organismes de normalisation de la RFID, des orientations quant à leur responsabilité à concevoir une technologie respectueuse de la vie privée, et afin de permettre aux exploitants de s'acquitter de leurs obligations au titre de la directive protection des données.

20. Communication de Mr P. LEMOINE relative à la radio-identification, séance de la CNIL du 30 octobre 2003, disponible sur le site de la CNIL (http://www.cnil.fr).
21. Ainsi, le contrôle des déplacements d'un employé et la détection automatique de comportements *a priori* suspects, lorsque sa localisation révèle sa présence prolongée à la cafétéria ou dans des lieux où sa présence ne se justifie pas.
22. Dans le même sens, le rapport de l'IPTS «Sécurité et respect de la vie privée du citoyen à l'ère du numérique après le 11 septembre: visions prospectives. Document de synthèse», juillet 2003, à propos des systèmes dits d'intelligence ambiante.

40. Dans le cas où la directive s'applique[23], les responsables du traitement sont tenus de respecter ses obligations (intention et notification, transparence, principe de finalité, justification légitime du traitement des données, qualité, droits de la personne concernée, sécurité, traitement par un sous-traitant, transfert transfrontalier des données). Notons que le respect de ces prescrits est d'autant plus facile qu'ils disposent, de la part des fabricants, d'une technologie qui, dès sa conception, y incorpore les moyens de respecter les exigences légales[24].

Cette remarque préliminaire met ainsi en évidence la part de responsabilité des fabricants vis-à-vis du principe général du respect de la vie privée. Cette responsabilité se déduit du considérant 2 de la directive 95/46/CE : « *les systèmes de traitement sont au service de l'homme ... doivent respecter les libertés et droits fondamentaux des personnes, notamment la vie privée ... doivent contribuer au progrès économique et social et au bien-être des individus* ». Cette **responsabilité des fabricants des produits technologiques** et des concepteurs des applications de la technologie a été soulignée à plusieurs reprises par le Groupe dit de l'article 29. L'article 14, alinéa 3, de la directive 2002/58/CE lui donne une première concrétisation lorsqu'elle affirme : « *Au besoin, des mesures peuvent être adoptées afin de garantir que les équipements terminaux seront construits de manière compatible avec le droit des utilisateurs de protéger et de contrôler l'utilisation de leurs données à caractère personnel ...* ».

41. Quant aux **responsables du traitement des données à caractère personnel**, c'est-à-dire ceux qui utilisent les données collectées grâce aux RFID, sur base de la directive en son article 6, §§ 1 et 2, il leur est demandé de s'assurer que :

- les données qu'ils traitent sont loyalement et licitement traitées (exigence de communiquer aux personnes concernées par l'utilisation de ces technologies [p. ex. le client d'une grande surface] une information claire et compréhensible) ;
- les données sont collectées pour des finalités déterminées, explicites et légitimes, et ne peuvent être traitées ultérieurement de manière incompatible avec ces finalités (respect du principe de la finalité) ;
- les données sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement (respect du principe de la qualité des données) ;
- les données sont 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 (respect du principe de la qualité des données) ;
- les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour

23. Sur les doutes du Groupe de l'article 29 à propos de l'application de la directive à certaines applications RFID, voy. *supra*, n° 36.
24. Sur ce point, *cf. infra*, nos 55 et s., nos réflexions sur la technologie au secours du droit.

lesquelles elles sont collectées et traitées (respect du principe de la conservation).

42. Quant à la **légitimité** des traitements opérés à partir de l'utilisation des RFID (art. 7 de la Dir. 95/46/CE), le Groupe de l'article 29 souligne qu'en principe, seul le consentement préalable des individus[25] fournit une justification aux traitements des données à caractère personnel. Ce consentement devrait, à notre avis, être fondé sur une information claire sur l'existence, le type, la localisation, les finalités et les actions permises par la technologie RFID, de même que sur les informations transmises et leurs destinataires. Par ailleurs, le consentement doit être rétractable, ce qui en clair signifie la possibilité de désactiver momentanément ou de manière plus définitive le radiotag. Sans doute des exceptions au consentement peuvent exister, fondées, par exemple, sur les intérêts vitaux de la personne concernée, dans le cas du «marquage» d'un patient hospitalisé, ou sur l'intérêt public supérieur, dans le cas du passeport de voyage.

43. Quant aux divers **droits de la personne concernée**, selon l'article 10, le responsable du traitement ou son représentant doit fournir à la personne auprès de laquelle il collecte des données la concernant au moins les informations concernant l'identité du responsable du traitement, les finalités du traitement auquel les données sont destinées, les destinataires des données et l'existence d'un droit d'accès et de rectification des données conservées.

Dans le cas du commerce de détail, cela se traduit par l'obligation de mentionner, outre le marquage des produits par des radio-tags et la présence de lecteurs, le fait que cette lecture peut s'opérer sans action intentionnelle de la personne. On ajoute que cette information mentionne les finalités de l'utilisation des données, le cas échéant leur mise à la disposition de tiers, l'identité du responsable du traitement des données et, point important, la façon de neutraliser les tags et la façon d'exercer le droit d'accès aux informations, comme une version moderne du droit d'opposition[26].

44. Le **droit d'accès** prévu par l'article 12 de la directive garantit à toute personne concernée le droit d'obtenir du responsable du traitement la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées, la communication des données faisant l'objet des traitements ainsi que toute information disponible sur l'origine des données et, enfin, la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la directive, et la notification de ce fait aux tiers auxquels les données ont été communiquées. Le droit d'opposition de la personne con-

25. Il faut préciser que dans le cas du consentement donné, ce dernier doit respecter certaines exigences: il doit être donné librement (sans contrainte ou tromperie), être spécifique (c'est-à-dire concerner une finalité particulière), être une indication de la volonté effective de la personne et, finalement, être donné en toute connaissance de cause et être indubitable (c'est-à-dire qu'il ne peut avoir plusieurs sens).

26. Le parallèle avec le droit de restreindre l'identification de la ligne appelante et de la ligne connectée, droit consacré par l'art. 8 de la Dir. 2002/58/CE, peut être proposé à ce propos. On note que cet article oblige le fournisseur du service de communication à offrir à l'abonné un moyen simple et gratuit d'empêcher la présentation de l'identification de la ligne appelante, de refuser des appels entrants de lignes non identifiées ou d'empêcher la présentation de l'identification de la ligne connectée.

cernée doit également être garanti, comme prévu à l'article 14.

45. L'article 17 impose au responsable du traitement de mettre en œuvre toutes mesures techniques ou organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, notamment lorsque le traitement comporte des transmissions de données dans un réseau.

Dans la mesure où les radio-tags s'intègrent dans une chaîne objet aboutissant, via internet, à une base de données de produits et que cette base de données peut se situer à l'étranger, le flux transfrontière de données, selon le Groupe de l'article 29, devrait se justifier en principe par l'indubitable consentement de la personne concernée au transfert hors de l'Union européenne.

Enfin, il y aura une obligation, pour les commerçants et industriels désirant utiliser les radio-tags, de **déclarer leur traitement**, ce qui implique une déclaration du mode de collecte de l'information traitée auprès de l'autorité de contrôle, selon le prescrit de la directive.

46. En conclusion, les législations de protection des données européennes ont et auront une influence importante sur le développement des applications RFID en Europe. Reste aux personnes concernées à être conscientes de leurs droits et à en exiger le respect, de même qu'aux entreprises et administrations de prendre connaissance de leurs obligations et responsabilités. Sans doute sera-t-il important également de s'interroger sur l'application de certains prescrits des législations de protection des données au-delà du champ d'application de la directive, c'est-à-dire lorsque les applications RFID ne concernent pas des données à caractère personnel au sens de la directive. Ainsi, l'obligation d'information relative à la présence d'une puce RFID, sa finalité, les données générées, la durée d'activation comme l'obligation d'offrir des moyens de bloquer temporairement ou définitivement l'accès à la puce et aux données y contenues devraient exister indépendamment du caractère personnel des données traitées.

c) Au-delà de la vie privée : Où il est question de protection de la dignité humaine ?

47. Dans son rapport n° 20 du 16 mars 2005[27], le Groupe Européen d'Éthique des Sciences et des Nouvelles Technologies auprès de la Commission européenne s'est penché sur la question particulière des implants TIC, en particulier par la technologie des RFID, dans le corps humain. Ces applications particulières soulèvent certes des questions de protection des données, mais leur spécificité conduit à soulever en outre les questions liées à l'inviolabilité du corps humain et, de manière plus générale, à la dignité humaine.

Le Groupe rappelle d'abord que les principes et règles juridiques servent généralement de garde-fou aux dérives technologiques et que tout ce qui est techniquement possible n'est pas nécessairement admissible sur le plan éthique, socialement acceptable, ni légalement approuvé. D'un autre côté, la puissance d'une technologie donnant

27. «Aspects éthiques des implants TIC dans le corps humain», Avis n° 20 du Groupe Européen d'Éthique des Sciences et des Nouvelles Technologies auprès de la Commission européenne, 16 mars 2005.

lieu à une infinité d'applications[28] ne saurait être contrainte par une législation faible manquant sa finalité ultime: celle d'assurer le respect des droits et libertés des humains.

En conséquence, le Groupe réaffirme la nécessité de se référer à des valeurs fortes, telles que celles reprises dans la Charte des droits fondamentaux de l'Union européenne, et de «*placer la personne au cœur de son action*». Par les traitements de données à caractère personnel qu'elle autorise, la technologie RFID doit être considérée «*comme touchant l'individu dans son ensemble, qui doit être respecté dans son intégrité physique et mentale*».

48. Le Groupe avance alors un nouveau concept global de l'individu, donnant à ce dernier le «*droit de revendiquer le respect total d'un corps qui est aujourd'hui à la fois physique et virtuel*». C'est donc le respect de la dignité humaine qui doit constituer le guide lors des débats relatifs à l'imposition de limites aux diverses applications des technologies RFID. Ces technologies sont capables à la fois de réparer et d'améliorer le corps[29] … «*Dans nos sociétés, le corps tend à devenir un matériau brut, qui peut être modelé en fonction des circonstances*».

Le Groupe rappelle l'existence de certains principes tels que la liberté de choix en matière de santé qui doit permettre à tout individu de ne se voir implanter un TIC qu'avec son plein consentement, et surtout son droit à l'autodétermination informationnelle qui exclut tout contrôle à distance et le refus de toute manipulation hormis celles exigées par un intérêt vital de la personne concernée. Il exige l'adoption de normes techniques harmonisées contraignantes pour les producteurs de telles technologies et l'application du principe de précaution, c'est-à-dire l'obligation de scruter en profondeur les conséquences sociales, psychologiques et relationnelles des technologies mises au point avant leur mise en application pratique. En particulier, le Groupe s'inquiète des utilisations non médicales des applications mises au point dans des contextes de soins de santé.

49. Ainsi, un implant médical TIC, s'il doit obéir en lui-même au respect de la dignité humaine et de la protection des données à caractère personnel, requiert en outre le consentement éclairé du patient et doit être régi par le respect des principes suivants: premièrement, l'implant doit s'avérer nécessaire à la sauvegarde, guérison ou amélioration de la qualité de la vie du patient; deuxièmement, cet objectif ne peut être atteint par un moyen moins invasif ou plus efficace en termes de coût; troisièmement, l'accès devra être conditionné par des besoins en termes de santé et non pas en termes de ressources économiques ou de position sociale.

Dans la mesure où le patient se voit ainsi transformé en maillon d'un réseau informatique, il convient de prendre en considération le fonctionnement de l'ensemble de ce réseau et pas unique-

28. Ainsi le système mis au point par Microsoft, et par ailleurs breveté (brevet Microsoft du 22 juin 2004, en date du 22 juin 2004), qui fait du corps humain un transmetteur de données à d'autres appareils (téléphones cellulaires, appareils médicaux et RFID). Ce système permet la localisation de personnes et leur surveillance à distance (p. ex. dans des maisons de retraite, à la maison, pour surveiller les enfants ou les personnes âgées).

29. … ce que les rapporteurs (RODOTA et CAPURRO) désignent sous le nom de «Cyborg», c'est-à-dire un corps dont le comportement, grâce à ces implants, peut être contrôlé de l'extérieur, «*objet de surveillance permanente*». Les auteurs s'appuient sur des expériences qui permettent de stimuler à distance certaines fonctions biologiques et psychiques. «*Il est en outre possible non seulement en théorie mais aussi en pratique d'implanter des dispositifs TIC dans le corps humain, notamment pour restaurer certaines fonctions corporelles ou … de remplacer certains organes ou membres*». *Cf.* égal. les biocapteurs MEMS, qui permettent à distance de surveiller des malades atteints de certaines maladies, comme celles de Parkinson ou du diabète, et d'agir à distance en cas de crises.

ment de l'implant, en veillant à ce que le pouvoir exercé sur ce réseau soit transparent, pour permettre à la fois le respect de la personne ainsi que la minimisation du préjudice.

Si le respect de l'inviolabilité du corps humain ne doit pas constituer un obstacle au progrès scientifique, il constitue cependant un garde-fou contre ses dérives possibles. Toute recherche nécessitera le consentement éclairé des personnes, ainsi qu'une explication concernant les risques à long terme ou le risque lié à des fins de localisation personnelle et/ou d'accès aux données sans le consentement du porteur d'un implant. Ces exigences devront être encore plus strictes en cas d'implantation irréversible. Le droit d'interrompre toute participation à un projet de recherche scientifique devra toujours être respecté. Les implants TIC chez les mineurs et les personnes en incapacité légale ne devraient être possibles que sous réserve du respect des principes énoncés dans la Convention du Conseil de l'Europe sur les droits de l'homme et la biomédecine.

50. Les applications non médicales constituant également une menace potentielle pour la dignité humaine et la société démocratique, il conviendra également de respecter en toutes circonstances les principes de protection des données de consentement éclairé, de proportionnalité et d'information quant à une possible manipulation des données contre leur gré. Le droit de déterminer quelles données pourront être traitées, par qui et dans quel but devra être respecté. Si l'implant a la surveillance pour finalité, il convient qu'il soit autorisé par le législateur et seulement pour satisfaire un besoin urgent et justifié et alors qu'il n'existe pas d'autre méthode moins intrusive. Il doit reposer sur une base légale et faire l'objet d'une approbation et du contrôle par une juridiction indépendante. L'implant TIC ne pourra être utilisé à des fins de manipulation mentale ou de modification de l'identité personnelle. Les dispositifs permettant le contrôle à distance de la volonté d'autrui doivent être strictement interdits, ou du moins sévèrement contrôlés.

51. Finalement, dans ses considérations générales, le Groupe Européen d'Éthique (GEE) soutient avant tout la dimension humaine que doit revêtir la société de l'information, que le développement de cette dernière nécessite un vaste débat social et politique ainsi que la mise en place par les États membres et par leurs comités d'éthique nationaux des conditions nécessaires à l'éducation et à l'expression de ces débats, garantissant également la transparence des enjeux du développement technologique et, en définitive, le contrôle démocratique[30]. En particulier, l'implantation des TIC dans le corps humain doit faire l'objet d'une réglementation fondée sur les principes de dignité humaine, de respect des droits de l'homme, d'équité et d'autonomie, ainsi que sur les principes dérivés de précaution, de minimisation des données, de spécification de la finalité, de proportionnalité et de pertinence. Les recherches quant à l'impact à long terme sur les plans social, culturel et de la santé devront être poursuivis, en accordant une attention particulière à la caractérisation, à l'évaluation, à la gestion et à la communication des risques. Enfin, l'évolution rapide du domaine imposera une révision de l'avis du GEE d'ici trois à cinq ans.

30. Dans le même sens, les réflexions de S. GUTWIRTH, P. de HERT e.a., «The legal aspects of the SWAMI project», in *Safeguards in a World of Ambient Intelligence (SWAMI), Deliverable D5,* Report on the Final Conference, Brussels, 21-22 March 2006 (EU 6th Framework Programme).

V. Au-delà de la loi : l'autorégulation et la technique, comme supports de l'effectivité des lois

A. L'autorégulation, au service de l'effectivité de la loi

52. À côté, et non en lieu et place, de la législation, l'autorégulation peut constituer un mode complémentaire de régulation des RFID. Cette autorégulation, faute actuellement de loi spécifique aux RFID, est prônée par divers milieux. On a déjà cité l'action de CASPIAN, qui exige cette autorégulation dans le cadre de l'utilisation par la grande distribution des RFID. On peut citer également l'action des associations qui veillent au respect de la vie privée des citoyens. L'association « Statewatch », située à Londres, qui milite pour la liberté des citoyens et la transparence des institutions européennes, a dénoncé les projets européens qui recourent aux technologies de surveillance (localisation, identification et suivi des déplacements) de tous les citoyens, dans le but d'« identifier les principales menaces qui pourraient toucher l'Europe ».

53. Les guides de bonne conduite de l'industrie et du commerce peuvent aussi contribuer à apporter une réponse aux risques d'atteinte à la vie privée véhiculés par la technologie RFID. Leur existence rend ainsi compte de la volonté du monde des affaires d'assumer sa responsabilité dans la protection de la vie privée des consommateurs.

L'EPCglobal, en particulier, a mis au point un « guide de bonne pratique », rédigé par des experts en vie privée et qui s'applique à tous les membres de l'Organisation. Ce guide leur recommande d'adopter différentes attitudes, comme les « notices » et l'utilisation de marques, qui permettent d'informer les consommateurs sur la présence de RFID. Le guide prévoit la possibilité pour ces derniers d'exercer le choix de bloquer l'identification du tag et rappelle l'obligation de s'assurer du respect de toute législation existante dans le domaine de la protection de la vie privée et des données à caractère personnel. Ainsi :

- pour les marques d'information, il est recommandé aux compagnies faisant usage des radio-tags d'appliquer sur les produits un label EPC indiquant la présence d'un radio-tag ; EPCglobal a développé un tel label, dont le design suit :

EPCglobal label d'information au consommateur

- le choix du consommateur concerne son droit à enlever, neutraliser ou désactiver tout radio-tag présent sur les produits qu'il acquiert ;
- ce choix (exprimé dans le point précédent) du consommateur doit pouvoir se faire sur une base éclairée, ce qui implique qu'il doit pouvoir disposer de toute information précise au sujet des tags EPC, de leur fonctionnement et de leur application ; cette « éducation » devrait aider les consommateurs à mieux comprendre les enjeux de cette technologie, ses bénéfices, et donc finalement à mieux l'accepter.

Il ressort de ce qui précède que ces guides de bonne pratique insistent tout spécialement sur le devoir de transparence, prélude indispensable à l'instauration d'un climat de confiance et de sécurité nécessaire à l'usage des technologies RFID. Cette transparence sera le fait des industries et pourra être garantie par l'intervention d'une tierce partie vérifiant et certifiant le respect des principes et la sécurité des systèmes mis en place.

54. En juin 2006, le Commissaire à la protection des données de la province d'Ontario a émis des «*Privacy Guidelines for RFID Information Systems*» qui doivent servir de modèles pour ceux qui conçoivent ou mettent en œuvre des systèmes d'information basés sur la technologie RFID. On en souligne plusieurs principes. Le principe de responsabilité «*Accountability*» insiste sur la responsabilité de toutes les organisations qui concourent à la mise sur pied ou au fonctionnement d'un système RFID, en particulier sur la responsabilité première des personnes en contact direct avec les individus. Le principe de «*data minimization*» implique que le minimum de données soit collecté en ce qui concerne l'identifiabilité de la personne concernée et les liens possibles avec d'autres données détenues sur elle[31]. La qualité des données est un autre souci, en particulier dans la mesure où ces données peuvent être déformées lors de leur transmission et servir à des décisions vis-à-vis des personnes concernées. La transparence «*openess*» des politiques et pratiques d'utilisation des systèmes d'information RFID doit être assurée par des notices d'information claires et compréhensibles.

B. La technologie au secours du droit

55. La technologie – et le Groupe de l'article 29 le souligne amplement à propos précisément des RFID – peut également contribuer au respect des principes de la protection des données dans le contexte du traitement des données à caractère personnel collectées par un dispositif RFID. D'abord, comme dit précédemment, parce que les fabricants et les organismes normalisateurs peuvent être contraints via des normes que la Commission leur impose «*au besoin*» en cas de non-respect des prescrits de protection des données par les clients utilisateurs de cette technologie. Il s'agira alors de fournir aux utilisateurs des applicatifs de la technologie RFID des outils conçus et réalisés dans le respect des prescrits des législations de la protection des données[32].

L'apport technique à la garantie du respect de tels prescrits s'opère sur différents plans, selon le Groupe de l'article 29 (dans ce qui suit, tous les articles font référence à la Dir. 95/46/CE):

– par la définition de normes techniques relatives à la conception des éléments de la technologie RFID et de leur interopérabilité: tous les composants d'un système RFID font ou feront l'objet d'une norme; et il apparaît que la plupart d'entres elles incluront des caractéristiques de protection des données dans leur spécification; l'interopérabilité peut s'avérer positive en augmentant la qualité technique des données (respect de l'art. 6, § 1, d), relatif à la qualité et à la per-

31. Ainsi, la grande surface qui lierait les données relatives au parcours des clients, données qui peuvent être utiles dans le contexte d'un réaménagement des rayons et de leur contenu avec les dépenses de ce consommateur et le contenu de ses achats.

32. Comme le note A. CAVIOUKAN, Commissaire à la protection des données de la Province d'Ontario (Canada), dans l'introduction des Guidelines analysées *supra*, n° 54: «*Privacy and Security must be built in fropm the Outset- at the design Stage*».

tinence des données), mais également négative, par l'augmentation du nombre d'intervenants, en ce qui concerne la limitation des finalités et la gestion des droits d'accès;

– par les mesures techniques et d'organisation en ce qui concerne l'information sur la présence de RFID, sa visibilité et son état de veille (art. 10): outre l'obligation d'informer la personne concernée sur la présence de dispositifs RFID, la technique doit indiquer visuellement l'activation ou l'état de veille et permettre la neutralisation temporelle;
– par les mesures techniques et d'organisation pour l'exercice des droits d'accès, de rectification et d'effacement (art. 12): l'accès au contenu des tags (art. 12, a) nécessite un environnement complet d'application de la télécommunication; la récupération de cette information pourra se faire via la définition de normes sémantiques au moyen du méta-langage XML[33]. La rectification du contenu (art. 12, b) exige un lecteur fonctionnant avec le protocole du tag et un système permettant de suivre la lecture du contenu et sa modification; quant à l'effacement du contenu, il se justifie sans doute pour certaines applications (liées à des produits de consommation), mais pas pour d'autres (marquage d'un passeport). La désactivation peut se faire de façon permanente (au moyen d'une commande destruction, d'un brouillage de mémoire ou d'un détachement du tag) ou temporaire (mécaniquement ou au moyen d'un verrouillage logiciel). Enfin, deux autres solutions proposent soit de neutraliser les données par des zéros (mais des objections issues des commerçants ou pour raison sécuritaire s'élèvent), soit de recouvrir le radio-tag par une feuille d'aluminium (ce qui n'est pas toujours applicable);
– la légitimation du traitement: si le consentement est le seul motif légal légitimant la collecte de données à caractère personnel, le droit pour la personne de pouvoir retirer son consentement à tout moment ne pourra être exercé que si un dispositif de neutralisation (tel que défini précédemment) est effectivement présent;
– la sécurité des données: les articles 17 et 6, § 1, d), demandent, lorsque les radio-tags renferment des données à caractère personnel, que des mesures techniques puissent empêcher la diffusion non autorisée des données. Ces moyens pourront consister en un cryptage des données ainsi qu'en une authentification du lecteur, en utilisant des protocoles d'authentification standards (comme ISO/CEI 9798) qui comprennent des primitives cryptographiques (cryptographie symétrique ou asymétrique).

56. De manière très concrète, la technique fournit des moyens permettant de remédier aux problèmes d'atteinte à la vie privée. Ainsi en est-il de l'émergence de protocoles permettant l'encryptage ou l'usage de mot de passe afin de protéger les communications entre les lecteurs et les radio-tags, ou encore la mise au point de «blocker tags» qui, alors qu'ils sont placés sur un radio-tag ou à sa proximité, peuvent l'empêcher de communiquer avec un

33. *Infra*, n° 58.

lecteur. Le «kill switch» (*Kill command* de la norme EPC Gen 2) est un autre dispositif qui permet au consommateur d'exercer son libre choix de désactiver (via passage sous un portique spécial) ou non, et de façon permanente, les radio-tags associés aux produits qu'il a achetés. Il est permis de se demander si les solutions «blocker tags» ou «kill switch» sont intéressantes de part leur mise en œuvre pratique fort contraignante pour le consommateur. De plus, la commande de désactivation présente le problème de neutraliser des fonctionnalités utiles, par exemple contre le vol, ou d'effacer des données utiles, comme une date de péremption. Le consommateur devra sans doute tenir compte des informations fournies par le magasin[34].

57. Les radio-tags ne constituent cependant qu'une partie de la chaîne de collecte des données; ces dernières finissent en effet par être stockées dans des bases de données qui, par leur exploitation, peuvent fournir les renseignements de marketing ou de «profiling» vraiment intéressants d'un point de vue commercial. Un aspect réellement critique en ce qui concerne les risques d'atteinte à la vie privée associés à l'usage des radio-tags, est tout simplement de s'assurer que ces bases de données sont adéquatement protégées. La FTC[35] a, dans ce cas, publié des directives, adressées aux compagnies usant de la technologie RFID pour collecter et stocker des informations relatives à leurs clients, destinées à implémenter des mesures raisonnables et appropriées pour protéger les données.

Il est clair que les questions de protection et de sécurité des bases de données liées aux produits RFID sont à envisager au-delà des mêmes questions soulevées par les produits RFID eux-mêmes.

58. Puisque la technologie est à l'origine des problèmes, on peut raisonnablement se demander si elle ne pourrait pas également être la source de solutions[36]. Cette standardisation technologique constitue une forme particulière d'autorégulation et présente sur cette dernière certains avantages:

1) l'obtention d'une uniformité;
2) son appui sur un système rationalisé et éprouvé de méthodes et procédures pour sa réalisation;
3) son caractère balancé entre tous les intérêts de toutes les parties en présence et sa capacité à garantir la transparence et la participation de tous les acteurs du marché;
4) la relation (et donc le statut) entre la loi et les standards est plus sûre qu'entre la loi et les autres formes d'autorégulation, et peut ainsi être invoquée par les cours et tribunaux;
5) le fait qu'elle possède un ensemble d'outils spécifiques (audit, certification, *reporting*) qui assure son effectivité;
6) son élaboration, qui tire parti de l'organisation et de l'expertise des organismes de standardisation (cadre de développement, documents directeur, manuels, publications ...).

Bref, ses avantages prennent appui sur une méthodologie techno-scientifique.

34. *Supra*, n°43.
35. Voy. FTC, *RFID: Radio Frequency Identification: Applications and Implications for Consumers*, A Workshop Report from the Staff of the FTC (March 2005), disponible sur le site de la FTC (http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf).
36. Selon l'expression de C. CLARK à propos des problèmes de copies illicites causés par la technologie de l'internet (C. CLARK, «The answer to the machine is in the machine», in *The future of Copyright in a Digital Environment* (B. HUGENHOLTZ ed.), La Haye, Kluwer Law International, 1996, pp. 139 et s.).

59. Les développements futurs de l'internet pourront peut-être également contribuer à aider les consommateurs et détenteurs d'objets munis de tags RFID à mieux exercer leurs droits, en particulier celui relatif à l'accès aux données acquises et stockées à partir de ces dispositifs techniques. À cet égard, certains évoquent l'intérêt de ce qu'ils appellent le futur web sémantique[37]. Ce futur Web devrait permettre de transformer la masse des pages web en un gigantesque index hiérarchisé, en manière telle que l'information y soit accessible non seulement par les humains, mais aussi par les moteurs de recherche spécialisés, permettant ainsi une automatisation des requêtes de recherche. Ceci permettra alors de retrouver les données alors même qu'elles sont distribuées dans un très grand nombre de sources et qu'elles se caractérisent par une très grande hétérogénéité en taille et en structure. Si l'accès à l'être humain s'en trouve facilité, la recherche automatisée des données soulève également des problèmes importants dans le domaine de la vie privée[38].

60. Il convient de rappeler et de souligner que la technologie n'est pas en soi la panacée pour la prévention des risques sur l'internet et qu'elle ne peut remplacer une plate-forme de régulation, une législation, des contrats ou des codes de conduite[39]. Elle doit plutôt s'inscrire dans un de ces cadres. Les deux instruments sont ainsi inséparables.

Dans cette optique, il faut mentionner l'initiative technologique P3P[40] (*Platform for Privacy Preferences*) du consortium W3C, qui permettra aux utilisateurs d'être informés des pratiques des sites web qu'ils visitent et d'automatiser leur navigation sans se soucier de lire la politique de confidentialité propre au site. L'élément essentiel est l'instauration d'un dialogue entre le navigateur internet et le site utilisant la politique P3P (en utilisant XML pour transcrire les pratiques de collecte d'information du site et les rendre lisibles par une machine, autant que par un humain), jouant le rôle de garde-fou avant que l'utilisateur ne soumette des informations personnelles. Un tel dispositif devrait permettre aux internautes de mieux maîtriser la collecte et l'utilisation de leurs renseignements personnels, et la politique de protection de la vie privée mise en œuvre sur les sites sera plus transparente.

Le projet de plate-forme pour les préférences de confidentialité (P3P) a été conçu pour être flexible et pour gérer un ensemble divers de préférences d'utilisateurs, de politiques publiques, de politiques de fournisseur de services et d'applications. Il vise à renforcer la confiance de l'utilisateur vis-à-vis des services web et à protéger la vie privée sur le Web, même si nombre de critiques peuvent lui être adressées dans la mesure où il laisse au seul internaute le soin d'assumer la protection des ses données à caractère personnel[41].

37. Voy. p. ex. le site de W3C (http://www.w3.org/DesignIssues/Semantic.html) pour une présentation du Web Sémantique.
38. Voy., p. ex.: http://www.automatesintelligents.com/echanges/2006/juil/semanticweb.html.
39. A cet égard, nos réflexions sur les relations entre droit et technologie, Y. POULLET, «La technologie et le droit: du défi à l'alliance», *Liber Amicorum Guy Horsmans*, Bruylant 2004, pp. 942 et s.
40. Voy. le site du W3C (http://www.w3.org/TR/P3P/).
41. Outre l'opinion émise en ce sens par le Groupe de l'article 29 (opinion 11/98 du Groupe européen de protection des données, Groupe dit de l'article 29, à propos de la Platform for Privacy Preferences (P3P) et des Open Profiling Standards (OPS),opinion disponible à http://europa.eu.int/comm/dg15/fr/media/dataprot/wpdoes/wp11.fr.pdf), sur la contractualisation du traitement des données ainsi opérée par la technologie, voy. P.M. SCHWARTZ, «Beyond Lessig's Code for Internet Privacy: Cyberspace, Filters, Privacy control and Fair Information Practices», *Wisconsin Law Review*, 2000, pp. 749 et s.; M. ROTENBERG, «What Larry doesn't Get the Truth», *Stan. Techn. L. Rev.*, 2001, 1, disponible sur le site: http://www.sth.Stanford .edu/STLR/Articles/01_STLR_1.

61. Les RFID contribuent, de manière essentielle, à la création de ces systèmes dits d'intelligence ambiante. Ces systèmes mettent l'individu et les objets en relation avec le monde qui les entoure et permettent à l'individu de s'y guider, d'envoyer les signaux adéquats et d'en recevoir. L'Homme et les choses parlent, pas toujours en le sachant, pas toujours en pleine connaissance des personnes à qui ils parlent et qui les écoutent et dirigent leur action. Sans doute, peut-on faire confiance à la technologie, les RFID de demain seront moins chers encore et leurs capacités de transmission, mais également leurs protections, seront sans commune mesure avec ce qui nous est actuellement offert. Les applications se multiplieront et, sans doute avec elles, les bénéfices pour ceux qui se servent de cette technologie pour mieux vendre, mieux protéger leurs intérêts d'entreprise ou la sécurité publique, en même temps que pour ceux qui en sont les utilisateurs finaux, qu'ils soient consommateurs ou patients.

Au-delà de ces constats, il est clair que cette technologie, qui réduit l'homme aux quelques signes qu'il émet, le chosifie et le considère comme le simple récepteur ou émetteur de messages stéréotypés, soulève des questions éthiques et légales peu aperçues encore[42]. La conduite du développement de la technologie est laissée à l'autorégulation des concepteurs de la technologie et à leur normalisation. Sans doute, cette autorégulation spontanée est-elle la phase obligée des premiers développements technologiques, comme elle l'a été et le reste largement pour l'internet, mais il est temps de songer à la deuxième phase, avant que les craintes de certains à propos de cette technologie qui autorise le contrôle et la surveillance de chacun ne deviennent réalité, sans parler des risques liés à l'absence de sécurisation de certaines applications[43].

Nous avons plaidé, avec d'autres, pour une meilleure transparence du fonctionnement de ces outils, pour leur maîtrise par les personnes porteuses de ceux-ci ; nous avons plaidé pour une sécurisation et un meilleur contrôle des flux engendrés par ces tags et ce, au nom de la protection des données. La dignité humaine ne permet pas, à notre sens, n'importe quel usage de ces technologies. Nous avons souligné la responsabilité des concepteurs et de ceux qui opèrent des systèmes d'information fondés sur la technologie RFID. Il leur revient de mettre en place dès le design de ces systèmes des solutions qui garantissent la sécurité et le respect des lois en matière de protection des données. Allons, les RFID méritent bien un débat sociétaire auquel chacun doit prendre part.

42. À ce propos, J. BOHN e.a., «Living in a world of Smart Everyday Objects - Social, Economic and Ethical Applications», *Journal of Human and Ecological Risk Assessment,* vol. 10, n° 5, octobre 2004, pp. 763-786.
43. Ainsi, la puce RFID de nos passeports contenant des données relatives à leur porteur, notamment les données biométriques, serait lisible à distance par certains lecteurs autres que ceux dûment autorisés.