Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Conseil Général
des Technologies de l'Information

Comité de l'Inspection

LES TECHNOLOGIES DE RADIO-IDENTIFICATION (RFID) : ENJEUX INDUSTRIELS ET QUESTIONS SOCIETALES

Rapport présenté par

Françoise ROURE, Inspecteur général
Jean-Claude GORICHON, Inspecteur général
Emmanuel SARTORIUS, Ingénieur général

RAPPORT N° II-B.9 - 2004 - Janvier 2005

MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

Conseil Général
des Technologies de l'Information

Comité de l'Inspection

LES TECHNOLOGIES DE RADIO-IDENTIFICATION (RFID) : ENJEUX INDUSTRIELS ET QUESTIONS SOCIETALES

Rapport présenté par

Françoise ROURE, Inspecteur général
Jean-Claude GORICHON, Inspecteur général
Emmanuel SARTORIUS, Ingénieur général

Rapport N° II-B.9 - 2004
Janvier 2005

Conseil Général des Technologies de l'Information

Rapporteurs :
Françoise ROURE, Inspecteur général
Jean-Claude GORICHON, Inspecteur général,
Emmanuel SARTORIUS, Ingénieur général

Rapport n° II-B.9 - 2004
Janvier 2005

Les technologies de radio-identification (RFID) : Enjeux industriels et questions sociétales

S Y N T H E S E

La problématique de l'identification numérique est au cœur d'enjeux industriels, de société et de souveraineté. Elle concerne les objets ou groupes d'objets physiques sous forme de stock ou de flux, les objets numériques, et enfin les entités vivantes, animales et humaines.

Les technologies RFID transforment en profondeur un équilibre informationnel des échanges internationaux fondé sur l'étiquetage et la gestion de biens matériels par un système de codes à barres, au profit d'une traçabilité généralisée et d'un contrôle permanent des flux de biens, des supports d'accès à des services et des déplacements des personnes. **La maîtrise des systèmes d'information en réseau qui sous-tendent l'identification numérique devient, dès lors, un puissant enjeu de souveraineté dans un contexte de guerre économique**.

Cette situation est de nature à conférer aux acteurs maîtrisant les premiers l'offre technologique et industrielle de l'identification numérique, notamment par les technologies RFID, un avantage compétitif considérable et durable du fait de leur accès *dissymétrique* au renseignement économique et commercial qui compte dans une économie ouverte, mondialisée.

Les technologies de marquage et de traçabilité ont connu ces dernières années une évolution considérable rendue possible par la conjonction de la dématérialisation des processus de suivi, de la baisse des coûts des supports et des capacités de traitement de l'information (étiquettes, lecteurs, réseaux de communication électronique, intelligence logicielle), et de la lecture sans contact par radio-identification.

La substitution des puces RFID (*radio-frequency identification*) aux codes à barres est amorcée dans les marchés de masse professionnels et grand public. Alliée aux options technologiques prises par des acheteurs influents, au rang desquels le département américain de la défense, elle laisse entrevoir une généralisation mondiale au service d'un commerce international en forte expansion.

Les standards technologiques et les architectures de systèmes d'information qui agrègent les données et produisent d'autant plus de services à valeur ajoutée que les marqueurs RFID progressent en capacité de mémoire, conduisent à **une concentration importante de connaissances dans la main d'un nombre très réduit d'acteurs industriels, qui se trouvent être les mêmes que ceux choisis pour la gouvernance « technique » mondiale de l'Internet**. Ainsi, la société VeriSign a été choisie pour gérer le serveur racine du réseau d'information mondialement intégré d'EPC Global, qui répartit les codes électroniques de produit venant se substituer aux codes à barres.

L'exigence de traçabilité sera certainement facilitée par les technologies de radio-identification, notamment en ce qui concerne les obligations légales nouvelles relatives à la sécurité alimentaire et sanitaire. Elle appuie également les efforts de lutte contre la contrefaçon et la fraude, et de gains de productivité dans l'ensemble de la chaîne logistique. Appliquée aux personnes, à leurs déplacements, voire à leur comportement d'acheteur ou autre, elle soulève de redoutables questions

de protection des données à caractère personnel sensibles qui font que les équilibres institutionnels sont remis en cause par la généralisation du RFID. La protection des données sensibles individuelles peut être significativement compromise, de même que la capacité des pouvoirs publics de faire respecter les lois y afférant.

La généralisation de la traçabilité constitue en soi un enjeu économique et sociétal majeur, par la qualité et la diversité des solutions proposées par les technologies RFID en matière de rapidité et de sécurisation des chaînes logistiques en général, mais aussi par le bouleversement des structures classiques de l'offre en ce domaine.

Au regard des enjeux industriels et sociétaux considérables des technologies de radio-identification, la présence de l'industrie française et européenne dans les dynamiques de recherche appliquée, de normalisation et de développement de nouveaux marchés est très insuffisante**. L'ampleur des marchés, les solutions apportées aux entreprises, aux particuliers (notamment dans le domaine de la santé et de l'aide aux personnes présentant une mobilité réduite) et à la puissance publique dans sa recherche du juste équilibre entre plus de sécurité et autant de liberté à des coûts acceptables, les gains de productivité et de lutte contre la contrefaçon auxquelles les technologies RFID donnent accès, sont autant de motifs pour définir et mettre en œuvre une politique publique de promotion bien comprise des RFID qui vienne dynamiser l'offre et contribuer à l'innovation**.

Le rapport recommande une initiative forte des pouvoirs publics en faveur de la sensibilisation de tous les acteurs concernés aux opportunités des technologies de radio-identification, tout évaluant pour mieux les contenir leurs impacts négatifs, ***en commençant par les acteurs de l'offre :***

- sensibiliser les acteurs de l'offre et de la demande en matière de RFID aux opportunités considérables de productivité, d'innovation et de création de valeur présentées par cette technologie ;
- effectuer une analyse approfondie des menaces présentées par les technologies RFID, qu'elles visent les aspects relatifs à la traçabilité des personnes, la maîtrise des informations économiquement stratégiques pour les entreprises ou la souveraineté nationale, notamment eu égard à leur facilité d'usage et porter les résultats à la connaissance de toutes les parties intéressées en vue de leur sensibilisation ;
- mettre en oeuvre la pédagogie correspondante (colloques, forums, articles) de façon à créer la confiance dans le grand public et à armer les pouvoirs publics dans leur action pour préserver la souveraineté nationale ;
- adapter l'offre de services en matière de RFID à la lumière du retour d'expérience, voire prendre des mesures incitatives au renforcement de l'offre française et européenne en ce domaine ;
- favoriser la participation de la France aux instances de normalisation et fora internationaux en matière de technologie RFID, de nommage alternatif et d'adressage ;
- favoriser les initiatives professionnelles, qu'elles viennent des fabricants ou des utilisateurs, en vue du développement d'applications RFID de nature à engendrer une confiance bien comprise du consommateur et du citoyen ;
- investir dans la recherche sur les effets économiques et sociaux des technologies RFID et des systèmes d'information qui sous-tendent les applications de portée sociétale ;
- évaluer l'applicabilité de la loi garantissant la protection des données à caractère personnel du point de vue de la technologie d'identification numérique par radio.

S O M MA I R E

INTRODUCTION

Les enjeux de l'identité numérique tels que nous nous proposons de les analyser dans ce rapport se limitent à l'ensemble des questions, technologiques mais aussi sociétales, posées par la collecte, l'archivage et le traitement des informations liées à l'utilisation des technologies sans contact (puces électroniques, antennes imprimables notamment), les systèmes d'information qui portent les objets communicants et en particulier les logiciels de traçage.

Ils concerneront, suivant ainsi une approche institutionnelle, les informations qui, prises ensemble, permettent par leur collecte, leur stockage et leur utilisation, de réaliser l'identification d'une personne, quelle que soit la licéité de cette identification et/ou de son usage, en mettant en perspective les choix technologiques et les évolutions du cadre réglementaire aux plans national, européen et international.

Ils concerneront ensuite, dans une approche industrielle, les informations qui permettent l'identification d'un objet, en mettant en perspective les systèmes d'information globaux requis pour permettre le développement mondial des applications concernées.

Notre mission a choisi de limiter son approche aux technologies d'identification sans contact, qui présentent les perspectives de développement les plus importantes dans les dix années à venir, du fait des prix très bas attendus de leur généralisation rapide, et pour lesquelles le positionnement récent des acteurs autour d'une norme susceptible de remplacer le code-barres en y ajoutant des fonctionnalités intelligentes, ouvre la voie à court terme à des applications de masse, répondant à des marchés aussi bien civils que militaires, publics ou privés.

Les marqueurs, lecteurs et logiciels de la technologie RFID constituent, pris ensemble, un système d'identification par radiofréquences auquel contribuent au premier chef les acteurs bien établis de l'économie numérique mondiale (IBM, Philips, VeriSign, Gemplus notamment). D'autres entreprises du secteur de l'offre se développent rapidement, en particulier en France autour du technopôle de Sophia-Antipolis (mais non exclusivement). La technologie RFID accompagne le développement sans précédent des échanges commerciaux internationaux. Elle est, en termes de flux de données numériques relatives au commerce international, la contrepartie matérielle des flux financiers et par conséquent ne connaît pas, à priori, de borne à son développement futur. Elle permet de réaliser des économies en évitant les erreurs logistiques humaines et en limitant les « opportunités » de fraude quelle qu'en soit l'origine.

PARTIE I - IDENTIFICATION NUMERIQUE DES OBJETS ET ENJEUX INDUSTRIELS

1.1. Les technologies RFID et les acteurs de l'offre

1.1.1. Définition, feuille de route technologique, applications industrielles

La technologie RFID (*Radio Frequency Identification)*, on parle aussi parfois de *smart tags* (étiquettes intelligentes) se trouve au croisement de celle du code-barres et de celle de la carte à puce sans contact. Au code-barres elle reprend, en le modernisant, le principe de doter tout objet d'un code d'identification qui peut être lu par une machine. A la carte à puce sans contact, elle reprend la possibilité de lire des informations, voire de faire effectuer un traitement, à distance. La technologie RFID se prête donc bien à une automatisation de toute la chaîne logistique, d'autant que l'objet peut être en mouvement et dans une position quelconque, même si elle présente encore quelques faiblesses[1]. Dans son principe, le RFID n'a rien d'innovant dans la mesure où on peut considérer que le passe *Navigo* de la RATP ou les boîtiers de télépéage sur les autoroutes en relèvent.

La supériorité du RFID sur le code-barres, qui doit passer devant une fenêtre de lecture ou être scanné par un lecteur mobile ("douchette" des caissières de supermarchés), tient au remplacement des techniques de lecture optique par des techniques électromagnétiques. Le RFID, qui peut être inséré dans l'épaisseur d'un emballage, voire imprimé dessus, ne se distingue de la carte à puce sans contact que par l'absence du support "carte plastique". Le principe physique reste le même : un microprocesseur doté d'une antenne et "éclairé" dans des conditions convenables par un champ électromagnétique est capable d'émettre des informations qu'il porte en lui, voire de procéder à des traitements.

On distingue :

- les étiquettes en mode lecture seule ou passives : dans ce cas, des données (code d'identification unique et infalsifiable) sont inscrites dans l'étiquette par le fabricant et ne peuvent être ni modifiées ni complétées ; les utilisateurs peuvent seulement lire le numéro de série inscrit sur la puce ;
- les étiquettes en mode lecture/écriture ou actives : dans ce cas, l'étiquette dispose d'une capacité mémoire qui peut être écrite, complétée, lue, voire effacée ; le nombre de cycles de lecture est illimité.

Les RFID peuvent également se classer en quatre catégories selon les bandes de fréquences dans lesquelles elles fonctionnent :

- les puces BF (fréquence inférieure à 135 kHz) avec une distance de lecture de quelques centimètres ;

[1] Le RFID fonctionne notamment mal en présence de masses qui réfléchissent les ondes électromagnétiques (emballages métalliques ou contenant de l'eau, par ex.).

- les puces HF (fréquence de 13,56 MHz) avec une distance de lecture de quelques dizaines de centimètres ; la plupart des puces passives utilisent cette bande de fréquences ;
- les puces UHF (868-950 MHz) avec une distance de lecture de l'ordre du mètre ;
- les puces UHF à 2,45 GHz (même bande que les normes Bluetooth et Wi-Fi).

1.1.2. Le processus de normalisation EPC

Les enjeux de la normalisation sont considérables dans la mesure où c'est celle-ci qui, *in fine*, garantira l'interopérabilité entre étiquettes, lecteurs et systèmes de traitement des informations et, plus généralement, le bon fonctionnement de l'ensemble dans le contexte d'une économie mondialisée où la circulation des biens ne connaît plus de frontières. La normalisation intervient aussi par le biais des effets de série, et donc des réductions de coût, qu'elle permet. Ses enjeux se situent à trois niveaux :

- au niveau des protocoles d'échange entre le RFID et son environnement ;
- au niveau des fréquences radioélectriques qui permettent les échanges entre le RFID et son environnement ;
- au niveau du codage des objets porteurs de RFID eux-mêmes.

Pour ce qui concerne le premier point, l'ISO a déjà développé des normes (14 443, 15 693, famille des normes 18 000[2]) qui sont encore loin de faire l'unanimité. Les normes propriétaires restent encore nombreuses, sans parler de celles produites par d'autres coalitions d'intérêts, comme la toute récente norme EPC*global* UHF *generation* 2[3].

Pour ce qui est des fréquences, il existe un sérieux problème dans la bande UHF, a priori la plus intéressante en termes de potentiel d'utilisation du RFID. Les fréquences utilisées aux Etats-Unis (915 MHz) sont réservées aux réseaux de téléphonie mobile de deuxième génération en Europe et au Japon, ce qui restreint fortement la puissance à laquelle on peut les utiliser et donc leur portée. L'Europe, elle, a retenu la fréquence de 868 MHz. Comme on voit mal ceux-ci disparaître avant un certain nombre d'années, des négociations internationales seront nécessaires sur ce point si on veut assurer une interopérabilité entre les systèmes américains et le reste du monde.

1.1.3. Les acteurs de l'offre des technologies RFID pour l'identification des objets

Les industriels présents dans le domaine du RFID sont :

---

[2] ISO 18 000-2 dans la bande 125-135 kHZ, future norme ISO 18 000-3 qui devrait remplacer les normes ISO 14 443 (A/B) et 15 693, dans la bande 13,56 MHz, future norme ISO 18 000-6 dans la bande 860-9340 MHz et future norme ISO 18 000-4 dans la bande 2,45 GHz.

[3] Sur EPCglobal Inc., voir § 1.2.1.

- les grands fabricants de composants électroniques : Hitachi, Infineon, NEC, Philips Semiconductors, STMicroelectronics, Texas Instruments, etc. ;
- les grands systémiers, capables de concevoir, de développer, de mettre en place, voire d'exploiter les systèmes utilisant les RFID et qui reposent largement sur les technologies de l'information (gestion de bases de données, réseaux, ...) ; IBM s'est clairement positionné sur ce créneau mais on y trouve aussi Accenture, Bearing Point, CSC, Unisys ou VeriSign ;
- les fournisseurs de logiciels comme Microsoft, Oracle ou SAP ;
- des industriels de la téléphonie mobile comme Nokia ;
- enfin, *last but not least*, les attributaires ou gestionnaires des codes attribués aux objets et qui permettent leur identification, comme EPCglobal Inc.

Pour ce qui est de l'aspect proprement manufacturier du RFID, ajoutons simplement qu'à l'heure actuelle l'enjeu majeur est de réduire drastiquement son coût actuel (environ 0,05 € contre 0,30 € aujourd'hui), que les utilisateurs potentiels comparent pour l'instant défavorablement à celui, quasi-nul, d'un code-barres. Compte tenu de la difficulté de jouer, au-delà des effets de série, sur le coût des microprocesseurs, les efforts des industriels se portent essentiellement sur le coût des antennes et du *packaging*. C'est ainsi qu'on voit apparaître sur ce créneau de petites sociétés innovantes, comme IER, Tagsys ou ASK, à Sophia-Antipolis, qui a développé des procédés qui permettent d'imprimer l'antenne par un simple jet d'encre sur tout type de support. Cela étant, les perspectives de marchés sont colossales : on parle de 10 à 20 milliards d'objets *RFIDéisés* à l'horizon 2008.

La gestion des codes est une affaire infiniment plus importante par les conséquences qu'elle entraîne et les enjeux de pouvoir qu'elle implique. L'entité américaine à but non lucratif EPCglobal Inc.[4], *joint venture* entre EAN International[5] et l'Uniform Code Council (UCC[6]) américain, s'est clairement positionnée sur le créneau, considérable, de l'étiquetage des palettes et des cartons et se propose de gérer les *Electronic Product Codes* (*EPC*) au niveau mondial et de fournir un service d'interconnexion aux serveurs contenant des informations relatives à des objets identifiés par des *EPC*. EPCglobal Inc. déclare vouloir au travers de son *EPCglobal Network*, relier tous les objets à Internet et fournir un service de transactions de base, telles que la localisation des informations relatives à un objet donné, la localisation d'un objet donné, la localisation d'un objet donné dans la chaîne logistique, ainsi que des services à valeur ajoutée de traçage et autres. EPCglobalInc. affirme ne viser que le marché du *B to B* (*business to business*) et non

[4] http://www.epcglobalinc.org/. On trouve dans son *conseil des gouverneurs* des représentants de firmes comme Carrefour, Cisco Systems, Coca-Cola, Gillette, HP, Metro, Nestlé, Procter & Gamble ou Wal-Mart.

[5] Organisation internationale représentant 101 organisations de 103 pays (Gencode EAN France pour la France), basée à Bruxelles et ayant le statut d'association à but non lucratif, créée en 1977, dans le but de développer des normes permettant une gestion de chaînes logistiques globales et multi-entreprises. EAN International fixe la structure des codes-barres hors Etats-Unis (EAN = *European Article Number*) (http://www.ean-int.org/).

[6] Organisme technique créé aux Etats-Unis il y a une trentaine d'années, l'Uniform Code Council développe des normes et des solutions pour améliorer la gestion de la chaîne logistique globale. UCC fixe la structure des codes-barres aux Etats-Unis (http://www.uc-council.org/).

celui du *B to C* (*business to consumer*). On voit en tout cas le pouvoir qu'elle pourra retirer de ce rôle central dans la circulation des marchandises à travers le monde. Ajoutons que EPCglobal a confié la gestion de son réseau (EPCglobal Network) à la société américaine VeriSign, qui, entre autres activités, gère les noms de domaine Internet (DNS).

1.2. La relation stratégique entre l'ONS et le DNS et les principaux acteurs de la demande

Longtemps reconnue pour le rôle qu'elle a joué dans le fonctionnement de l'infrastructure critique sous-jacente au DNS et à internet, la société VeriSign développe son infrastructure et son expertise pour soutenir le serveur racine du service de nommage d'objet d'EPCglobal Network (ONS *Object Numbering System*).

ONS est l'un des services qui permet la réalisation de « processus commerciaux de valeur supérieure sur le réseau EPCGlobal Network ». L'offre de VeriSign est celle de la technologie EPC Starter Service (SM), qui permet l'identification et la quantification de la valeur des informations de suivi et de repérage des produits marqués RFID, créées en chaque point de la chaîne de production, d'acheminement et de distribution des objets, et tout au long de leur vie en l'absence de désactivation volontaire ou fortuite.

1.2.1. La relation stratégique entre l'ONS et le DNS

La symbiose entre internet et identification des objets physiques n'était pas obligée. Mais cette fusion est simplement devenue très vite logique dans le contexte actuel où internet est le liant envahissant qui créé la complémentarité entre toutes les activités jusqu'ici en relation, mais aussi distinctes.

Les puces RFID sont les descendantes directes du code-barres. A ce titre, leur utilisation aurait pu rester enfermée dans une sphère propre à la logistique, comme cela avait été le cas des étiquettes à barres sur les 30 dernières années.

Mais leurs zélateurs[7] ont immédiatement perçu la fantastique démultiplication créée en s'appuyant sur les bases de données en ligne, et particulièrement sur les technologies IP de l'internet, pour rendre le processus « sans couture », dotant ainsi l'architecture des échanges d'une redoutable efficacité pour un surcoût d'infrastructure dérisoire.

Et très rapidement la similitude des situations a poussé à un copié-collé des solutions inventées pour l'adressage de l'internet, le DNS *(Domain Name System).*

[7] Essentiellement les laboratoires du MIT.

- L'adressage : un phénomène irréversible et pressant ?

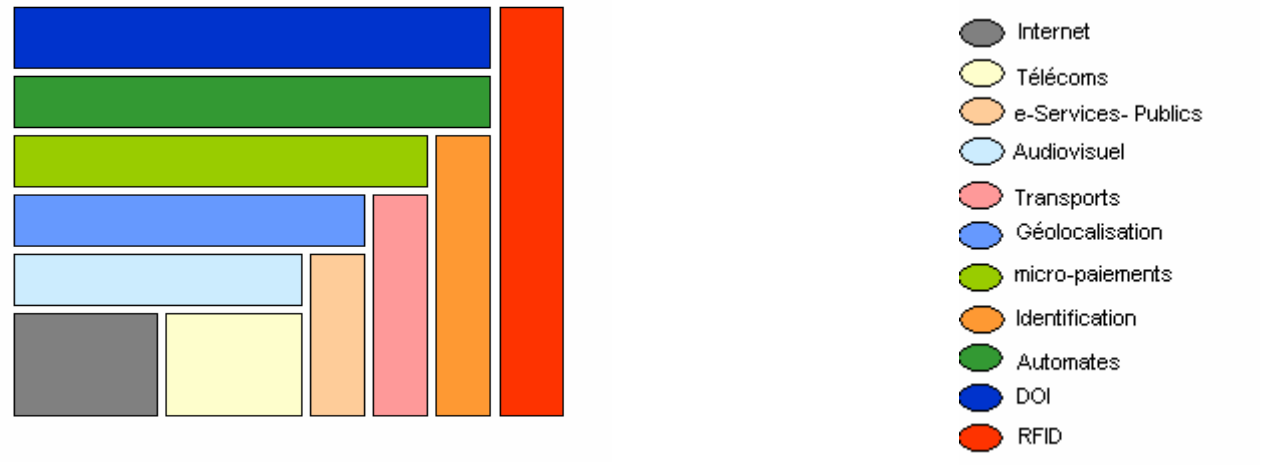
Le monde est entré depuis quelques années dans la frénésie de donner une adresse, de préférence permanente, non seulement aux objets physiques, aux individus, aux véhicules sur la route, aux animaux, sous prétexte de traçabilité, mais aussi à tous les objets virtuels, que ce soit les messages de type courriels ou SMS, les documents administratifs, les morceaux de musiques numérisés, ou les micro-esclaves logiciels (*applets, servlets* et autres agents dits "intelligents") qui parcourent inlassablement les réseaux en y troquant des micro-informations pour mieux nous servir, voire souvent, pour mieux nous espionner.

Certes, la bataille n'est pas encore gagnée entre les technologies, les normes ou les industriels qui sont entrés dans cette bataille d'influence entre les divers mondes en réseaux.

- Les luttes fratricides des mondes en réseau

Car, d'ores et déjà, ces multiples mondes en réseaux[8] qui vont des télécoms aux automates en passant par l'identification des personnes, et que le discours récurrent imagine volontiers converger dans une fusion idyllique pour le bienfait de l'utilisateur, sont en fait engagés dans une lutte fratricide sournoise, puisqu'ils ont tous décidé de s'approprier le monde IP, **mais** chacun d'eux en le déformant et le pliant à ses contraintes spécifiques.

Pour simplifier, une cartographie provisoire de ces mondes en réseaux pourrait être la suivante.



Il est prévisible que ces anciennes frontières entre des mondes qui œuvrent en permanence à phagocyter les autres ne vont pas demeurer intactes. La concurrence s'annonce en particulier féroce entre le DNS, l'ONS et les DOI *(Digital Object Identifier)*.

[8] Voir la présentation en annexe 4.7.

- Les similitudes poussées de l'ONS et du DNS

Rien d'étonnant à ce que l'on trouve des similitudes entre le premier mode d'adressage imaginé pour l'internet, DNS, et l'adressage de chacun des autres mondes, dès lors que les besoins sont de même nature.

Mais sous la conjonction de plusieurs facteurs, c'est certainement le monde ONS qui a été le plus rapide pour rester au plus près de l'architecture DNS.

D'abord, les acteurs en mesure de peser d'un poids suffisant dans les décisions sont essentiellement les mêmes : le gouvernement américain avec le DoD et le DoC, les grands industriels tels qu'IBM et l'acteur devenu rapidement incontournable dans la planète internet : VeriSign.

Dans les deux schémas, DNS et ONS, le serveur racine a été confié dans des conditions discrètes par le gouvernement américain à VeriSign sans, qu'apparemment les autres acteurs aient eu leur mot à dire. Il faut dire que depuis l'*Executive Order* américain du 16/10/2001 classant "Confidentiel Défense" les architectures essentielles de l'internet, il y a peu de chance que cette désignation soit jamais éclaircie.

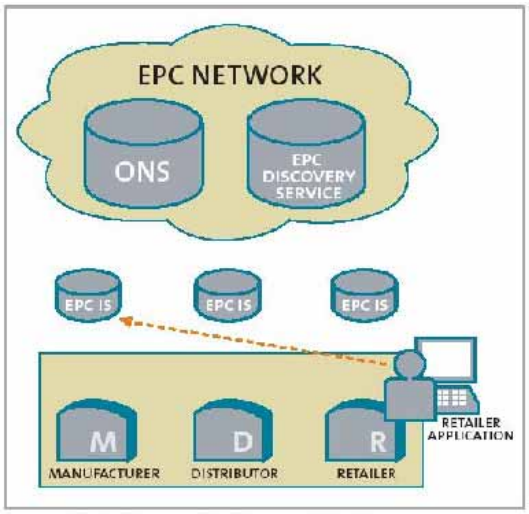
La différence de taille, à nos yeux, porte sur les serveurs de second niveau. Dans le DNS, le découpage géographique a été conservé, permettant à chaque Etat de garder sous contrôle l'opérateur des adresses correspondant à son territoire géographique.

S'agissant des normes d'EPC Global et de l'ONS, ce découpage géographique a totalement disparu. Les serveurs secondaires sont ceux des grands industriels, multinationaux dont on sait bien que les Etats n'y ont plus guère de moyen de contrôle. Ainsi, tout au moins, on peut en déduire que les débats onusiens pour savoir quelle place les Etats devraient avoir dans une gouvernance efficiente de l'internet ne se poseront plus.

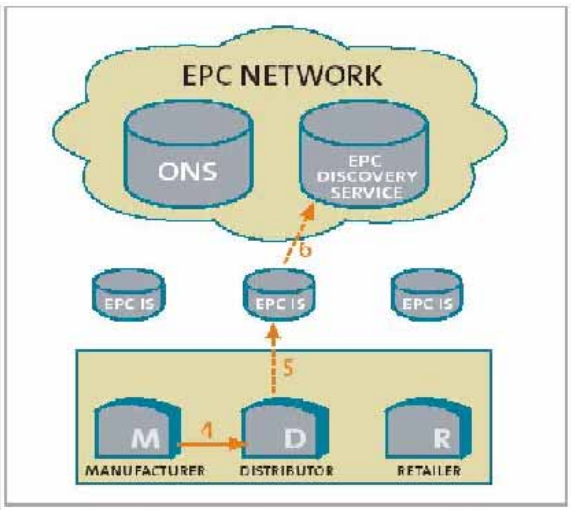
Comme les flux, les nombres d'objets à identifier, le nombre de sous-traitant et de magasins de distributions dépassent de plusieurs ordres de grandeur le nombre de sites internet, il y a fort à parier que l'ONS (ou tout au moins ses acteurs incontournables) pourrait rapidement phagocyter l'internet que nous connaissons, rendant ainsi illusoires les modestes tentatives du GAC *(Gouvernment Advisory Committee)* et du Sommet Mondial de la Société de l'Information (SMSI).

Les schémas ci-dessous illustrent les trois niveaux de l'architecture :

- au premier niveau : un serveur racine (ONS), accompagné de son *whois* (appelé ici Discovery Service)
- au second niveau : les serveurs propres aux professionnels (fabricants, grossistes, etc)
- au troisième et dernier niveau : l'accès des utilisateurs finaux dont, en particulier, la grande distribution (graphiques et légendes de VeriSign).



Retailers and other parties have real-time view through the EPC Network



Distribution information is available to all parties

Ce qui peut paraître sujet à questionnement et qui pourrait freiner l'essor d'un tel modèle est le risque d'intelligence économique que favorise une telle architecture. Rien ne dit que les industriels vont laisser librement chaque acteur des différentes sphères interroger leurs propres bases et collationner les données économiques et comportementales que le modèle laisse entrevoir.

Il est étonnant de constater que, apparemment conquis par les indéniables avantages entrevus de la gestion « sans couture » de leurs flux physiques, les industriels européens au sein des conseils de pilotage ou de surveillance d'EAN et d'EPC Global se soient montrés aussi discrets sur les risques indéniables que de telles architectures centralisées font peser sur des informations vitales pour leur compétitivité, leur avance et leur savoir-faire.

De la même façon, les divers fora, qu'ils soient professionnels, tel l'IETF, ou plus institutionnels, tel le SMSI, se focalisent avec insistance sur certains rouages (l'ICANN...), mais omettent systématiquement d'évoquer la place grandissante, voire inappropriée, de certains acteurs privés de la sphère Internet.

Il serait temps, à notre avis, que les autorités européennes, qui scrutent avec attention le monde de l'informatique (cf. le cas Microsoft), étendent leur veille aux « mondes » voisins, dont celui de l'Internet, et évaluent dans quelles conditions la société VeriSign étend ses filets sur les pans les plus sensibles de la gestion des mondes en réseaux.

En tout état de cause, il nous paraît important, à ce stade, d'alerter le gouvernement sur ces dérives potentiellement très dommageables à l'intégrité économique de pans entiers de l'économie.

Pourquoi, par exemple, faudrait-il laisser toutes les données d'échanges *en temps réel* de l'industrie française (que ce soit le luxe, l'aviation, la pharmacie, etc.) à la disposition centralisée d'une seule entreprise dont la déontologie en la matière reste encore à prouver ?

En effet, s'agissant d'internet, cette même entreprise est déjà particulièrement juge et partie puisqu'elle assure, par contrat avec le gouvernement américain, la maintenance des serveurs racines tandis qu'elle gère commercialement, par ailleurs, plusieurs dizaines de millions d'adresses en .com (et encore en .net) et qu'elle assure par ailleurs la certification et la confidentialité des liens cryptés (y compris certains services essentiels de l'administration française !).

1.2.2. Les acteurs de la demande, leurs exigences et leur influence sur le développement du marché

Le RFID et le réseau EPCglobal en cours de constitution ont le potentiel suffisant, compte tenu de l'attractivité de leur faible coût et leur forte valeur ajoutée dans la feuille de route communément admise par les professionnels des marqueurs et lecteurs RFiD, pour imposer une banalisation totale de cette technologie dans tous les domaines de la chaîne logistique des objets, mais aussi des déplacements et comportements des unités du vivant dans le règne animal et végétal : animaux vivants dans le cadre de la veille sanitaire obligatoire, humains pour leur comportement de (cyber) voyageur, de consommateur (y compris de systèmes de santé et de sécurité) et de citoyen…

Ainsi, en Corée, pays qui s'est doté d'un programme de 100 M€ sur 4 ans « *Ubiquitous-sensor Plan* » visant à devenir l'un des leaders du RFID à l'horizon 2010, une chaîne de grands magasins propose au consommateur de suivre sur son site internet l'itinéraire du bœuf qu'il est en train de déguster…

Les motifs d'adoption du RFID sont d'ordre économique. Ils permettraient de réduire les coûts d'inventaire et ceux de la main-d'œuvre utilisée pour l'approvisionnement, ainsi que les pertes dues aux vols à l'étalage et à la contrefaçon. L'économie sur la chaîne logistique de la grande distribution serait de l'ordre de 6 à 7 % (étude AT Kearney citée par le rapport de la DREE, cf. bibliographie).

Le coût d'utilisation du standard EPC devrait être majoré d'une rémunération des brevets de la société américaine Intermec sur les technologies RFID, le renchérissement dû au paiement des *royalties* serait de l'ordre de 5 à 10 % du prix de la puce électronique, selon EPC Global. Tous les autres constructeurs ont fait don de brevets pour que le standard EPC soit libre de rémunération de propriété intellectuelle.

Le coût d'une puce RFID reste à ce stade supérieur à celui du code-barres, mais il n'est pas directement comparable si l'on tient compte des possibilités supplémentaires de collecte, stockage et utilisation de données supplémentaires. D'importantes baisses de coût

sont attendues d'une part de la production de masse, et d'autre part d'innovations technologiques telles que l'impression.

Les premiers acteurs de la demande vont certainement influencer la démarche normative mondiale. Sont concernés : la grande distribution avec Wal-Mart et Marks & Spencer ; les conditions d'accès aux marchés d'approvisionnement du département de la défense américain (DoD) et de ses agences pour le marquage des objets ; les spécifications du Grid du système global d'information du DoD dans sa dimension sans contact *Wireless Global Information Grid* (WGIG) ; sans oublier les industries de la grande consommation (Coca Cola, Gilette, Nestlé, Whirlpool Europe notamment), la distribution de produits pétroliers (Exxon Mobil) ou encore les transports (RATP, gérants de péages d'autoroutes…). Des puces RFID sont utilisées sur les cartes de fidélité diffusées par Metro en Allemagne, ou encore dans le cadre du fret express (DHL) ou de la mesure de qualité des services postaux internationaux (Posteurop).

Acteur influent compte tenu, du point de vue logistique, du nombre de ses fournisseurs et de la quantité et de la diversité des produits approvisionnés, le DoD a opté pour une stratégie intégrée d'identification numérique des objets. Il a approuvé la bande de fréquences de 860-960 Mhz pour les marqueurs passifs *(passive RFID tags)*. Selon sa réglementation interne, accessible sur son site Internet www.dodrfid.org, ces marqueurs suivront les spécifications des marqueurs passifs de classe 0 et 1 du consortium EPCGlobal. Ils devront être appliqués sur tout envoi et toute unité de palettes. Ils seront complétés le 1er janvier 2007 par un système beaucoup plus fin de marquage à l'objet dans le cadre du concept de base d'identification universelle (UID *Registry concept*) dont le graphique est joint en annexe n° 4.1.

La politique d'identification par radiofréquences sur la base de marqueurs actifs a été explicitée le 30 juillet 2004 par le sous-secrétaire d'Etat américain à la Défense, l'objectif étant de fournir une visibilité globale des entités mobiles. Ce service doit être sous-tendu par une infrastructure de réseau Internet fonctionnant sur le schéma suivant : les données issues des marqueurs RFID seront acheminées vers les serveurs dits de visibilité régionale, puis adressées vers le réseau global de transport d'information. Une structure centralisée assurera les relations avec les serveurs régionaux, y compris celui du réseau d'adressage secret du protocole internet (*ITV server on the Secret Internet Protocol Router Network* – SIPRNET). Il incombera à ce serveur d'assurer l'interopérabilité de ces données ainsi centralisées avec le système global d'appui aux forces armées, le système global de contrôle et de commandement, ainsi que les autres systèmes d'information classifiés. (cf. annexes n° 4.2 et 4.3).

Bien qu'un audit de l'agence américaine chargée d'auditer la comptabilité fédérale (*General Accounting Office* : GAO) reste dubitatif sur la capacité, voire la volonté des différentes entités des forces armées américaines d'adopter un tel système centralisé et global, les moyens budgétaires ont été mis en place, à marche forcée.

Un autre facteur majeur d'influence du marché sera la position des instances chinoises de normalisation dans le domaine du RFID. En effet, sont à prendre en compte non seulement les marchés export, résultant notamment de la délocalisation d'acteurs internationaux vers ce pays, mais aussi le développement du marché intérieur chinois. Si la technologie RFID en elle-même est neutre, dans la limite de l'impact toxicologique et écotoxicologique relatif aux matières employées (nanotechnologies selon le calendrier de la

feuille de route), elle pose de redoutables questions de société en plus des freins de nature technique (disponibilité et harmonisation des fréquences) et économique (rapidité de la baisse des coûts) à sa généralisation à court terme.

L'exemple de la polémique soulevée par le caractère payant de l'anonymat pour les coupons hebdomadaires et mensuels de la RATP dans le cadre de la généralisation du système Navigo illustre **l'incertitude quant à l'acceptation sociétale**, au regard de l'ergonomie d'usage que la technologie apporte. Faut-il payer pour rester anonyme dans les transports quotidiens est une question à laquelle la CNIL répond par la négative. L'émergence de ce type de débat est induit par la banalisation des technologies sans contact. La stricte nécessité économique doit-elle prévaloir et si oui avec quelles conséquences ? **Ici, la fragile distinction entre l'identification des personnes et celle des objets est particulièrement tangible.**

PARTIE II - IDENTIFICATION NUMERIQUE DES PERSONNES ET EQUILIBRES INSTITUTIONNELS

S'agissant des personnes physiques, nous utiliserons uniquement le terme d'**identification** ; en effet, si la récente loi sur la bioéthique autorise dans certains cas la brevetabilité de phases de séquençage du génome humain en tant que procédé innovant, il ne saurait être question, à ce stade, d'une véritable identité numérique humaine.

Toutefois la question de l'identité numérique humaine commence à être posée globalement, au-delà des éléments désormais classiques tels que la numérisation du nom, du prénom, de la date de naissance, de l'adresse de résidence et de la signature, ou encore le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, ou à un répertoire international (par exemple dans le système d'information dit Schengen II – SIS II).

En août 2004, les autorités japonaises ont accepté à des fins de recherche médicale le clonage des embryons humains, pour lesquels les bases de données numériques génétiques pourraient constituer un élément d'identité numérique. Les banques de données biométriques humaines sont promises à un essor certain, y compris dans leur dimension commerciale, posant ainsi la question de l'anonymisation ou du consentement.

D'autres éléments constitutifs de l'identité numérique humaine sont en cours de développement sous la pression des exigences de sécurité, d'ordre public et de lutte contre le terrorisme : image numérique du visage, de l'iris, de l'empreinte digitale, imagerie numérique médicale de tout ou partie du corps humain, y compris de l'empreinte cérébrale (*brain fingerprint*, d'ores et déjà utilisée aux USA en justice dans les procès d'actes criminels). Le dossier médical unique, créé par la loi, devrait accélérer, en France, l'évolution vers la définition et l'usage public et privé de l'identité numérique humaine.

Nous qualifions ici d'*accessoire*, les identités numériques relatives aux objets communicants et aux services numériques, dans la mesure où la finalité comportant les plus forts enjeux se concentre sur le rassemblement, par tous moyens licites ou illégaux, de données numériques personnelles ou non personnelles, à partir desquelles il devient possible de procéder à l'identification d'une personne physique, - et de son comportement.

Pour autant, ces informations et leur traitement, pour la plupart issues de l'économie transactionnelle (libre ou marchande), constituent elles-mêmes un gisement considérable de valeur, directement et indirectement, et par là même, assurément, justifient que les autorités publiques chargées de l'industrie et de la société de l'information soient en mesure de connaître et d'anticiper les évolutions pour remplir convenablement leur mission. Par conséquent, elles sont fondamentales du point de vue industriel.

Les dispositions législatives en vigueur en France concernent le traitement des données à caractère personnel mais semblent en retard au regard des possibilités de fusion d'informations numériques qui permettent, dûment organisées, d'utiliser un ensemble de données dont chacune, prise isolément, ne relève pas du champ d'application de la loi, mais dont l'agrégation permettrait de parvenir, selon la finalité réellement poursuivie, non

seulement à l'identification, mais également à l'établissement d'un profil d'état et de comportement.

L'existence de ces informations agrégées, comme la finalité et les usages réels de cette agrégation, échappent alors au contrôle par les membres et les agents de la Commission nationale de l'informatique et des libertés (CNIL).

Il en résulte que l'esprit de la loi est, *de facto*, de contournement aisé, en particulier lorsque les obligations incombant aux responsables de traitement ne peuvent être ni appliquées, ni, a fortiori, contrôlées, du fait de l'extraterritorialité des actions contrevenantes.

2.1. Rappel des dispositions juridiques françaises ; portée et limites

La loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, transpose notamment les dispositions de la directive européenne « vie privée et communications électroniques » du 12 juillet 2002.

Elle définit précisément en son article 1er les données à caractère personnel et la façon dont il convient de procéder pour décider du caractère identifiable ou non d'une personne.

Ainsi, « constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ».

« Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ».

La définition légale du traitement est neutre au regard des technologies employées puisque « constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, *quel que soit le procédé utilisé,* et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

La combinaison d'éléments épars en vue de l'identification et à finalité d'établissement de profil ou autres, est ici prise en compte, notamment par les termes de rapprochement et d'interconnexion.

Il convient de noter que le droit communautaire est plus précis que le droit français quant à la liste des données pouvant contribuer à l'identification d'une personne. En effet, conformément au règlement (CE) n° 45/2001 du 18 décembre 2000, « est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification **ou à un ou plusieurs éléments spécifiques,**

propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ».

L'applicabilité de la loi française aux responsables de traitement est nécessairement limitée à l'établissement de ceux-ci sur le territoire français, ou à leur recours à des moyens de traitement situés sur ce même territoire, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit par l'un des Etats membres de l'Union européenne.

Parmi les obligations faites aux responsables de traitement, figure l'information préalable des personnes dont le transfert de données à caractère personnel est envisagé dans un Etat non membre de l'Union européenne.

En particulier, « toute personne utilisatrice des réseaux de communications électroniques doit être informée de manière claire et complète par le responsable de traitement ou son représentant :

- de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations stockées dans son équipement terminal de connexion, ou à inscrire, par la même voie, des informations dans son équipement terminal de connexion ;
- des moyens dont elle dispose pour s'y opposer. »

La loi prévoit également le droit de toute personne physique :

- de s'opposer, pour des motifs légitimes, à ce que les données à caractère personnel la concernant fassent l'objet d'un traitement ;
- et de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection commerciale par le responsable actuel du traitement ou celui d'un traitement ultérieur.

L'identification à *l'insu* des personnes concernées est donc clairement illégale, dûment sanctionnée et passible de dispositions pénales à l'encontre des personnes physiques ou morales contrevenantes, pour infractions aux dispositions légales, prévues et réprimées par les articles 226-16 à 226-24 du code pénal.

2.1.1. De nouveaux moyens pour la CNIL, en retrait au regard des nouvelles menaces

Lors de la présentation du rapport annuel de la CNIL le 22 juin 2004, son président, M. Alex Turck, soulignait le renforcement de la capacité de cette Commission dans trois domaines, à savoir la possibilité de faire des contrôles sur pièce et sur place malgré l'opposition des organismes contrôlés ; celle de prononcer des sanctions pécuniaires allant jusqu'à 300 000 €, et enfin celle de jouer pleinement son nouveau rôle de conseil dans les

négociations internationales menées par le gouvernement ou dans l'octroi d'agrément de codes de conduite ou de logiciels contribuant à la protection des données personnelles.

Il convient de noter que le traitement des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes, doit faire l'objet d'une autorisation par décret en Conseil d'Etat après avis motivé et publié de la CNIL.

Toutefois, l'application pleine et entière de la loi semble soumise à un changement drastique de comportement de la part des acteurs responsables, dans le sens d'une prise de conscience et de responsabilité accrues. En effet, la CNIL estime à seulement 30 % le taux de déclaration des PME. Quant aux 700 000 associations répertoriées, seuls 7 000 fichiers de membres ont fait l'objet d'une déclaration depuis 1994... Encore s'agit-il de personnes morales dûment identifiées par registre du commerce ou déclaration à l'administration. Or, les acteurs des traitements de fichiers numérisés sont-ils tous assurément identifiables depuis le territoire français et pour un temps suffisamment long pour faire valoir efficacement ses droits à rectification ?

Sur les quatre axes majeurs de la nouvelle CNIL tels que définis par son président, à savoir, « communication, correspondant, contrôle et coercition », celui des vérifications a priori comme a posteriori reste à renforcer considérablement, qualitativement par un investissement fort dans la compréhension des techniques, notamment extraterritoriales, d'agrégation de données multiples, et quantitativement pour rester proportionné aux développements potentiellement exponentiels auxquels le développement de la société de l'information nous a d'ores et déjà conduits.

2.1.2. Traitements automatiques, fusion de fichiers et réalité du consentement préalable

En effet, si le consentement préalable est réputé donné pour chaque type de donnée, comment garantir aux individus le respect de la vie privée face aux traitements visant à fusionner les fichiers ? La loi considère bien le rapprochement ou l'interconnexion comme un traitement de données à caractère personnel, mais l'applicabilité de la loi au regard des multiples intervenants potentiels (responsables actuels et futurs, sous-traitance par communication à des tiers), d'autant moins soumis au risque de sanction ou de peine que la délocalisation est réelle, se heurte à des difficultés significatives qu'il convient de ne pas mésestimer.

Un certain nombre de données présentant un caractère personnel sont collectées, stockées et traitées à partir d'une identification *automatisée*, qui est réputée a priori connue de l'utilisateur et acceptée par lui pour chacune d'entre elles ; par exemple, la collecte automatique peut s'exercer via un portique, un usage du GPRS, du GSM ou d'antennes RFID. Pour autant, rien ne laisse présumer qu'un accord préalable est donné quant à la *finalité* d'un fichier agrégeant des données constitutives de l'identité et, au-delà, du comportement individuel, et dont la collecte s'effectue pour le compte de tiers...

Les risques encourus par les personnes au regard du respect de la vie privée du seul fait de traitements automatisés de données, sont pris en compte par le règlement (CE) cité *supra* en son article 19. Ils sont si reconnus que seules, des circonstances particulières,

peuvent autoriser l'utilisation de ce type de traitement pour des décisions produisant des effets juridiques.

Ainsi : « la personne concernée a le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise **sur le fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité tels que son rendement professionnel, sa fiabilité ou son comportement**, sauf si cette décision est expressément autorisée en vertu de la législation nationale ou communautaire, ou, si cela s'avère nécessaire, par le contrôleur européen de la protection des données ».

Pour mémoire, une seule dénonciation au Parquet parmi les 9 cas transmis par la CNIL en 2003, se rapporte à une opération de collecte illicite et déloyale de données personnelles réalisées à partir d'annuaires sans que le droit d'opposition ait pu être éventuellement exercé par les personnes concernées, cas « technologiquement » simple s'il en est... Les mailles du filet semblent par conséquent très larges au regard des pratiques.

2.1.3. De nouveaux risques technologiques pour l'applicabilité de la loi

Lorsque la société Cisco Systems, acteur dominant au plan mondial dans les routeurs utilisés dans le réseau Internet, acquiert de la société californienne P-Cube la technologie de plates-formes permettant aux opérateurs de téléphonie sur IP (VoIP) d'identifier leurs « abonnés », - c'est-à-dire des usagers gratuits [(sauf l'achat d'une oreillette et d'un microphone à brancher sur l'unité centrale d'un ordinateur) hors sujet] comme dans le cas de l'offre de Skype, ou des clients payants -, elle annonce son intention d'offrir, à ses propres clients opérateurs, ***des capacités nouvelles pour contrôler et gérer*** **des services tels que la voix sur IP, les jeux interactifs, la vidéo à la demande et le pair à pair, ou pour créer des offres spécifiques.**

Cela signifie qu'avec des usages de l'Internet en voie de maturation avec la généralisation progressive du haut, voire du très haut débit, les pratiques personnelles, privées comme transactionnelles, vont être soumises, *de facto*, à une croissance exponentielle des enregistrements automatiques de données personnelles et, par là même, à une envolée du nombre de combinaisons matériellement réalisables des fichiers numériques correspondants, dans le temps et dans l'espace.

Comment, face à la question actuelle de la gouvernance mondiale de l'Internet à des fins d'intérêt général, faire appliquer dans l'Union européenne et en France les obligations relatives à *l'effacement et à l'anonymisation* des données relatives au trafic, nécessaires à des fins d'établissement des communications et à la facturation ? (cf. art. 37 du règlement CE cité).

En particulier, le basculement, en voie d'accélération, du trafic de la voix, des réseaux classiques de télécommunications vers le tout IP d'une part, la multiplication des opérateurs de communication sur IP du fait de l'abaissement des barrières technologiques et financières d'autre part, font que l'application de la loi va nécessiter non seulement un investissement important dans l'efficacité des modèles de contrôle, mais aussi dans leur

financement au niveau adéquat. A défaut, c'est toute l'architecture de la confiance, patiemment étayée, qui sera fragilisée, et pour un temps long.

De plus, la « gratuité » du téléchargement des logiciels et parfois aussi des communications sur IP, ne permet plus de se référer aux critères classiques de responsabilité des opérateurs dans une économie transactionnelle classique basée sur le contrat (l'abonnement), rendant ainsi toujours plus ténues les traces dans la recherche de responsabilité en cas d'infraction à la loi, c'est-à-dire en cas de collecte à finalité illicite, de transfert en temps réel pour traitement par des « tiers » vers des pays dont le niveau de protection des données personnelles est estimé insuffisant par la Commission européenne, le traitement n'y étant pas soumis aux obligations déclaratives ou accord préalables protecteurs de la personne.

Pour mémoire, la société Skype basée au Luxembourg, créée par des fondateurs de Kazaa, a enregistré depuis le début de ses activités le téléchargement de son logiciel gratuit par 7 millions de personnes, gère 1,2 million d'appels par jour, n'est propriétaire d'aucun réseau, ne dépense pratiquement rien en publicité pour son service et emploie 50 employés (**Wall Street Journal Europe 25 août 2004**), ce qui caractérise économiquement et technologiquement le seuil très bas et pour ainsi dire inexistant à l'entrée sur le marché.

La rapidité de substitution du modèle de voie sur IP à celui des réseaux classiques de télécommunications est d'ores et déjà traduite dans les anticipations des analystes financiers, qui constatent la baisse de profit de géants industriels des télécommunications. Ainsi AT&T a subi une baisse de 18 % de ses bénéfices en trois ans ; l'évaluation de la valeur de l'action se dégrade pour atteindre parfois celle d'action «pourrie » (*junk bond*).

Au-delà des problèmes soulevés par les logiciels à téléchargement gratuit, du point de vue de la responsabilité de la collecte et du traitement des informations support d'identité ou d'identification, la question du consentement préalable se pose avec encore plus d'acuité s'agissant des processeurs embarqués pour lesquels il n'existe pas, par construction, d'option de désengagement (*opt-out*). Le surnom de ce type de puces est, Outre-Atlantique « *built-in digital handcuffs* ». A notre connaissance il n'existe pas de processeur « libre » à l'instar des logiciels libres.

Les puces électroniques envisagées sur les lignes de fabrication des micro-ordinateurs fin 2004 doivent inclure les spécifications adoptées par le groupement TCPA (Trusted Computing Platform Alliance) dont Microsoft et Intel sont membres. Elles comportent d'excellents arguments en termes de sécurité et de protection des droits de propriété intellectuelle. Le revers de l'innovation est toutefois l'impossibilité de choisir quant à l'exercice du droit de refus de la collecte automatisée de données.

Le département informatique de l'Académie des sciences de la Chine a annoncé en septembre 2002 la construction du processeur « dragon chip » fondé sur l'architecture RISC (et non pas CISC), qui utilise une forme sinisée de Linux, pour des raisons officielles de sécurité des systèmes d'information dans le domaine des applications militaires.

Dans l'un et l'autre cas, les spécifications techniques devront être étudiées à la lumière de l'applicabilité de la loi.

2.1.4. De l'exercice du droit de rectification

L'architecture juridique globale des obligations, sanctions et peines repose sur la notion de responsable du traitement, définie comme toute entité organisationnelle qui, seule, ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel.

Cette définition s'applique potentiellement à tant d'entités simultanément que l'exercice du droit de consentement préalable, de rétraction de ce consentement, même temporaire, ou de rectification au sens large, devient, -et est d'ores et déjà-, quasiment inapplicable. Comment identifier assurément le ou les responsables du traitement ? Où se situent-ils exactement ? Le temps que chaque personne concernée devrait consacrer à la vérification que ses données à caractère personnel numérisées sont dûment protégées de finalités illicites ou sans consentement préalable est infini compte tenu des incertitudes qui pèsent sur la bonne fin de ses recherches ou demandes.

La « gratuité » du droit à rectification, élevée dans la pratique législative au rang de principe, devient alors toute... théorique.

Comment dans ces conditions, imposer le respect de la loi sur l'information préalable et, a posteriori, l'application du nouvel article 43 de la loi n° 78-17 modifiée citée *supra* selon lequel « toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel qui sont inexactes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite » ?

A fortiori, comment vérifier efficacement que le responsable du traitement a accompli les **diligences utiles** si une donnée a été transmise à un tiers, afin d'être en mesure de notifier les opérations entreprises dans le cadre de l'exercice du droit de rectification (alinéa 4) ?

2.2. La puissance publique est responsable du cadre fixé pour le traçage numérique des personnes, à tous les niveaux de subsidiarité

La fusion de fichiers de données numériques présentant un caractère personnel peut soulever, lorsqu'elle est réalisée sous la responsabilité des autorités publiques, des questions quant au contrôle démocratique d'une finalité de traitement qui s'avérerait abusive au regard des dispositions légales.

En effet, les mêmes technologies qui permettent aux gouvernements la diffusion de programmes et de services, interactifs ou non, par les applications multiples de l'administration électronique nationale, régionale ou locale, peuvent, dans « d'indélicates mains », être détournées de leurs finalités initiales à des fins de surveillance et de contrôle de citoyens en dehors du contrôle d'une procédure par le juge, et en dehors de toute disposition légale.

En ce qui concerne la France, Etienne Wery, avocat, relève à cet égard dans un article publié le 11 août 2004 sur Internet, que le Conseil Constitutionnel n'a pas eu à se prononcer sur la question de savoir s'il était conforme à la constitution que la création d'un fichier de police contenant des données sensibles ne soit plus subordonnée à un décret en Conseil d'Etat pris sur avis conforme de la CNIL, car la question ne lui a pas été posée ; fait qui *semble* traduire un consensus, au moins conjoncturel, de la classe politique française sur ce sujet.

Symétriquement, avec la généralisation des modèles d'administration électronique, les autorités publiques utilisant des données numériques à caractère personnel pour identifier ou contribuer à l'identification et à l'authentification des personnes, doivent absolument être protégées de toute intrusion dans leurs systèmes d'information.

Elles doivent mettre leurs réseaux d'information à l'abri des tentatives dites de *cognitive hacking*, dont les modalités visent à introduire une ou plusieurs sources de désinformation, en particulier sur les éléments d'identification utilisés dans le cadre des applications de gouvernement électronique, en vue de modifier à leur insu le comportement des agents publics et des acteurs concernés.

Qu'il s'agisse d'entités publiques ou privées, l'une des menaces qui pèsent sur la gestion et le cycle de vie des objets tangibles, visibles ou non visibles par l'œil humain, et des objets intangibles, est l'usurpation d'une identité numérique. Celle-ci peut intervenir dans la phase de traçage par radiofréquence (étiquettes radio intelligentes pouvant se substituer à des codes- barres passifs et statiques), ou par logiciel (« tatouage » électronique à des fins d'identification et de reconnaissance).

Ces questions sont techniquement non résolues au plan des normes civiles internationales.

Ainsi, l'usurpation d'identité du domaine d'une adresse de courrier électronique, très pratiquée via le pourriel mais pas seulement, fait l'objet d'un appel à commentaires ouvert jusqu'en février 2005 dans le cadre d'un groupe de travail de l'IETF, sous l'appellation de protocole dit « Marid » intitulé « Sender ID : authenticating e-mail ». Une normalisation contraignante semble impossible avant un temps long (plusieurs années, le cas échéant)...

Face à l'ampleur de ce phénomène mondial, les internautes ont adopté le néologisme anglais de « *Phishing* », contraction des termes Fishing et Phreaking qui désigne la fraude informatique, pour désigner l'envoi d'un courrier électronique par un expéditeur se faisant délibérément passer pour une société ou toute entité réputée de confiance, à des fins de collecte d'informations sensibles auprès des destinataires.

Vers quel point d'équilibre tendre, entre le « big brotherisme » du tout électronique et le modèle réputé idéal, décentralisé, respectueux du statut des données personnelles, qui concernent la vie privée des citoyens, sa santé, son patrimoine, ses revenus et sa famille ? L'autorégulation des acteurs privés n'a pas apporté la confiance, tandis que l'interventionnisme des Etats fait toujours l'objet d'attentes paradoxales en faveur de plus de sécurité, mais aussi de plus de liberté... quand il ne s'agit pas d'une défiance radicale envers l'action publique dans les pays qui se dégagent progressivement de l'économie planifiée.

Mais dans tous les cas assurément, sans la volonté d'exercer concrètement les diligences dues, les auteurs du rapport sur l'Hyper République remis en janvier 2003 au secrétaire d'Etat à la réforme de l'Etat par Pierre de La Coste, estiment dans leur conclusion qu'« il n'est pas impossible que se réalise le cauchemar Orwellien, mais pas sous la forme prévue par son auteur ».

« Car les grands groupes qui détiendront les clés des technologies de l'information ne se priveront pas de décloisonner et de croiser à la place des Etats les informations personnelles qui tomberont en leur possession, et feront sauter les barrières juridiques dérisoires que ceux-ci tentent de leur opposer, notamment en France. *Big brother*, loin d'être à la tête de l'Etat, sera son pire ennemi ».

Un nouveau champ d'application de la loi s'est ouvert en France dans le contexte de la réforme de la santé et de l'assurance maladie. Il mérite un développement particulier.

2.2.1. Protection de l'identité numérique de santé : contexte et portée

Les technologies de sécurité des systèmes d'information, en tant qu'outil d'aide à la protection des données pour les responsables de traitement, sont utilisées par de nombreux acteurs privés, au premier rang desquels les acteurs de l'échange monétaire, mais aussi dans un avenir proche, par les professionnels de la santé.

La mise en œuvre du dossier médical personnalisé, créé par l'article 3 de la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie, va à cet égard constituer un défi particulier tant pour la définition des éléments constitutifs des données personnelles que pour leur numérisation, leur collecte, leur traitement et leur usage. Elle concerne toute la population relevant de l'assurance maladie en France, c'est-à-dire pratiquement 60 millions de personnes.

Créé auprès d'un hébergeur de données de santé à caractère personnel agréé, le dossier médical personnalisé sera d'accès restreint et, en particulier, ne sera accessible ni par la médecine du travail, ni dans le cadre de la conclusion de contrats de protection complémentaire en matière de couverture des frais de santé. Un décret en Conseil d'Etat pris après avis de la CNIL déterminera les conditions dans lesquelles un identifiant pourra être utilisé pour l'ouverture et la tenue du dossier médical personnel.

Un GIP dénommé « Institut des données de santé », institué par l'article 64 de ladite loi, a pour mission d'assurer la cohérence et de veiller à la qualité des systèmes d'information utilisés pour la gestion du risque maladie et de veiller à la mise à disposition de ses membres, à des fins de gestion du risque maladie ou pour des préoccupations de santé publique, des données issues des systèmes d'information de ses membres.

Un nouveau pas vers l'identité numérique humaine sera franchi avec la constitution de ce dossier médical numérique. Cette merveilleuse possibilité technique, qui promet de substantielles économies pour une efficacité accrue du service aux assurés, devra être entourée de précautions d'usage et de sanctions des contrevenants, qui soient à la hauteur des risques d'abus qu'elle engendre. Nous développerons ce point ci-après dans le cadre de la réglementation européenne relative aux données biométriques personnelles numérisées. L'avis de la CNIL portera, là, une responsabilité sociétale considérable.

Le droit communautaire repose sur l'article 286 du traité instituant la Communauté européenne, selon lequel les actes communautaires relatifs à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, sont applicables aux institutions et organes institués par le traité ou sur la base de celui-ci.

Les dispositions dites de *safe harbour* relatives au niveau de protection des données à caractère personnel exportées vers des pays non membres de l'Union européenne, ont été étayées par une décision de la Commission du 27 décembre 2001 relative aux clauses contractuelles types pour le transfert de ces données vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE.

En particulier, elles rappellent les obligations de l'exportateur de données « qui est le responsable du traitement des données à caractère personnel transférées » redevable de réparations en cas de recours, le droit d'exercer un recours à l'encontre de l'importateur faisant figure d'exception. On peut, ici également, s'interroger sur l'applicabilité du principe de gratuité des recours dans des procédures longues et complexes au plan international, en plus de la difficulté de traçabilité et d'établissement de preuves techniques.

L'interprétation par la société Microsoft de ces dispositions de *safe harbour* consiste à écrire dans son accord de confidentialité de janvier 2004 (disponible sur http://privacy.msn.fr), qu'elle « respecte le cadre portuaire défini par le département du commerce américain relatif à la collecte, l'utilisation et la conservation de données issues de l'Union européenne ». Elle précise que MSN « n'utilise pas ni ne divulgue des informations personnelles importantes comme celles identifiant votre race, votre religion ou vos tendances politiques sans votre accord explicite », ce qui suppose tout de même qu'elle serait en mesure de le faire, le cas échéant.

Le droit communautaire a été récemment complété, s'agissant de la protection des données personnelles. Il répond aux exigences contrastées de la société civile, qui demandent en même temps un respect accru et garanti des droits à la protection de la vie privée, et une confiance dans les institutions pour garantir l'ordre public, en particulier face à des actions terroristes.

La directive « vie privée et communications électroniques » citée *supra* vise à actualiser la directive du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications. Elle prend en compte l'introduction dans l'Union européenne de nouvelles technologies numériques, ainsi que des nouveaux services de communication électronique apportés par la généralisation progressive de l'usage de l'Internet et son cortège de nouvelles possibilités de collecte et de traitement des données relatives à la personne et à sa vie privée.

Elle prend bien la mesure des risques lorsqu'elle dispose que **« les logiciels espions, les pixels invisibles (*web bugs*), les identificateurs cachés et les autres dispositifs analogues peuvent pénétrer dans le terminal de l'utilisateur à son insu afin de pouvoir accéder à des informations, stocker des informations cachées ou suivre les activités de l'utilisateur, et peuvent porter gravement atteinte à la vie privée »**

(considérant 24). Elle estime que « l'utilisation de tels dispositifs ne devrait être autorisée qu'à des fins légitimes, et en étant portée à la connaissance de l'utilisateur ».

Elle reconnaît également que ces dispositifs, par exemple des témoins de connexion (*cookies*), peuvent se révéler indispensables, par exemple pour authentifier et contrôler l'identité des utilisateurs effectuant une transaction en ligne, mais sous réserve d'une information claire et d'un « droit de refuser ».

Elle admet également le fait que les données de position géographique de l'équipement terminal mobile peuvent être produites de manière plus précise que ce qui serait strictement nécessaire à l'établissement d'une communication, et qu'elles sont utilisables à des fins d'offre de services à valeur ajoutée personnalisés tels que la circulation et le guidage. Là encore, la directive préconise l'obtention, par le fournisseur du consentement préalable (art. 9), avec la possibilité gratuite et simple d'interdire temporairement le traitement des données de localisation même en cas d'accord.

Parmi les dispositions récentes du droit communautaire, trois d'entre elles méritent d'être mentionnées, à savoir le contrôleur européen de la protection des données (nommé le 22 décembre 2003), l'agence européenne pour la sécurité des réseaux et de l'information (créée par décision du Conseil et du Parlement européen le 20 novembre 2003) et le projet de système d'information sur les visas, suite aux conclusions du Conseil JAI des 5 et 6 juin 2003, intégrant des données biométriques.

Dans les trois cas, les intentions poursuivies par le législateur européen semblent en phase avec les attentes de la société civile ; pour autant dans chacun de ces cas, force est de constater la difficulté soulevée par la prise de décision finale ainsi que les retards de mise en œuvre parfois considérables constatés, voire l'application apparemment a minima des textes communautaires finalement adoptés.

2.2.2. Le contrôleur européen de la protection des données

L'institution du contrôleur européen de la protection des données a été créée par l'article 41 du règlement adopté le 18 décembre 2000. Le traité CE prévoyait qu'avant le 1er janvier 1999, une décision tripartite, prise sur la base de la procédure prévue à l'article 251 du traité, instituerait un organe indépendant de contrôle chargé de surveiller l'application par les institutions relevant du Traité, de l'obligation de protection des données.

Le statut et les conditions générales d'exercice des fonctions correspondantes n'ont fait l'objet d'une décision du Parlement européen, du Conseil et de la Commission que le 1er juillet 2002. Il a fallu attendre le 17 janvier 2004 pour que soit publiée la décision du Parlement européen et du Conseil portant nomination de l'autorité de contrôle indépendante prévue à l'article 286 du traité CE, ouvrant la voie à la nomination du Néerlandais M. Johan Hustinx et de son adjoint espagnol M. Joaquin Bayo Delgado pour une durée de 5 ans.

Somme toute, le retard entre l'intention du législateur européen et la mise en œuvre effective est de cinq ans, pendant lesquels la révolution de l'Internet a été accomplie dans l'Union européenne et dans le monde développé.

Pour l'avenir, l'article I-50 du titre VI du projet de traité constitutionnel de l'Union européenne, intitulé « Vie démocratique de l'Union », affirme le droit de toute personne à la protection des données à caractère personnel la concernant, et situe au plan de la loi européenne les règles relatives au respect de ce droit pour les institutions, organes et agences de l'Union, lequel doit être soumis au contrôle d'une autorité indépendante.

Parmi les cinq missions à court terme présentées devant la Diète polonaise le 26 mai 2004, le contrôleur européen ne cite pas l'évaluation de l'impact de l'évolution des technologies de l'information sur la protection des données. Il mentionne simplement que l'une de ses attributions importantes consiste à surveiller les faits nouveaux présentant un intérêt, qui pourraient avoir une incidence sur la protection des données à caractère personnel. Il omet de compléter son propos, pourtant repris textuellement de l'article 46, al. e) du règlement fondateur, par la fin de cet alinéa, à savoir « notamment l'évolution des technologies de l'information et de la communication ».

Il reconnaît toutefois pleinement l'incidence de la lutte contre le terrorisme, telle que menée par les Etats-Unis et l'Union européenne, sur le plan de charge de son institution. Il a pris l'initiative d'un contact avec le coordinateur de l'Union européenne de la lutte contre le terrorisme, M. Gijs de Vries. Il pourra être amené à formuler des avis et conseils, au-delà des accords dits « *safe harbor* » pour la sécurité des accords transfrontaliers de données, sur la question très sensible du transfert de données relatives aux passagers aériens, compte tenu des positions divergentes prises par le Parlement européen et, ultérieurement, la Commission européenne sur sa décision qui ne fait pas l'unanimité.

Il conviendra d'attendre les premiers rapports d'activité de cette nouvelle institution européenne pour évaluer les résultats obtenus au regard des missions qui lui sont imparties.

Avec 15 emplois à temps plein et un fonctionnement en double réseau avec les délégués de chaque institution communautaire d'une part, et la coopération avec les représentants des Etats membres au sein du groupe de travail dit de l'article 29 (de la directive de 1995), cette institution a certainement le potentiel pour mettre en œuvre la veille technologique dont elle a besoin et qui figure, *expressis verbis*, dans son texte fondateur. Encore faut-il qu'elle en reconnaisse l'importance stratégique, ce qui n'apparaît pas vraiment dans l'unique communication publique disponible sur son site Internet.

2.2.3. L'agence européenne pour la sécurité des réseaux et de l'information (AESRI/ENISA)

Décidée à la suite des évènements du 11 septembre 2001, dans le contexte de la banalisation des attaques logiques par internet, et en réponse aux pressions des acteurs du commerce électronique, l'Agence européenne pour la sécurité des réseaux et de l'information pouvait, à son origine, vouloir porter d'importantes missions d'intérêt général communautaire.

La décision du Conseil européen du 18 février 2003 se prononçait en faveur de la proposition de la Commission de créer un groupe de travail sur la cybersécurité. Elle invitait les Etats membres à développer la formation et la sensibilisation, en particulier des jeunes, aux problématiques de la sécurité des systèmes d'information.

L'agence, qui est juridiquement et budgétairement opérationnelle (24,3 millions d'euros sur 5 ans) depuis janvier 2004, dispose finalement d'un conseil d'administration où siège un représentant de chaque Etat membre, conformément à l'accord intervenu entre le Parlement européen et le Conseil le 20 novembre 2003. Henri Serres, Directeur central de la sécurité des systèmes d'information, y représente la France.

La vocation de l'AESRI consiste à conseiller et assister la Commission et les Etats membres dans la connaissance des menaces qui pèsent sur la sécurité des systèmes d'information et dans leur dialogue avec l'industrie, qu'il s'agisse d'infrastructures ou de données numériques réputées sensibles, présentant un caractère personnel ou non.

Son rôle est plus précisément d'identifier les problèmes relatifs aux matériels et logiciels offerts sur le marché intérieur ; de collecter et analyser les données sur les incidents de sécurité survenus dans l'Union européenne et expliciter les risques émergents ; de promouvoir les méthodes appropriées d'évaluation et de gestion des risques en vue de renforcer la capacité de faire face aux menaces relatives à la sécurité de l'information ; et enfin d'accroître la sensibilisation et la coopération entre les différents acteurs du secteur en développant, entre autres, le partenariat public-privé.

A ce stade, il n'est pas explicité que les risques nouveaux d'entrave à la législation sur la protection des données personnelles susceptibles d'intervenir par l'interconnexion et l'utilisation des réseaux et systèmes d'information, rendus possibles par les développements technologiques récents, fassent partie du champ des missions de l'AESRI. Rien pour autant dans les textes, ne permet d'exclure ce volet.

Là encore, il conviendra d'attendre les premiers rapports d'activité de l'AESRI pour savoir si cette agence entend, et si oui, dans quelle mesure, identifier le sujet complexe des potentiels et des menaces de l'identification numérique des personnes et de l'identité numérique des objets et services, dans sa dimension de respect de la législation européenne sur les données personnelles comprise comme l'un des éléments capitaux de la confiance des citoyens européens dans l'offre de biens et services de la société de l'information en Europe.

Le positionnement actuel, en phase de démarrage, semble être celui d'un organisme d'observation, les mesures à mettre en œuvre relevant du domaine de compétence de chaque Etat membre. L'utilisation du programme communautaire Modinis 2003-2005 de suivi du plan d'action e-Europe pourrait être un moyen de faire prendre en considération la relation étroite entre la confiance et le respect des données personnelles dans la recherche d'un niveau efficient de sécurité des systèmes d'information.

2.2.4. Des risques spécifiques inhérents à la centralisation des données numériques à caractère personnel.

Sur la centralisation des données, il convient de noter que le groupe de travail sur la protection des données, dit de l'article 29, s'est prononcé le 1er août 2003 sur l'utilisation de données biométriques. Adoptant une approche très équilibrée au regard des potentiels et risques, il insiste néanmoins sur les dangers particuliers de tout système centralisé des images et identifiants numériques.

Il rappelle que plusieurs autorités nationales se sont prononcées en faveur d'un stockage des données par des moyens appartenant à la personne elle-même, tels qu'une carte à puce, une carte bancaire ou un téléphone mobile, mais reconnaît l'impraticabilité d'une reconnaissance sans système doté de l'image numérique à partir de laquelle la vérification sera faite.

Il souligne que, dans certains cas, la biométrie peut permettre d'*augmenter* le respect de la vie privée lorsque ce type de données rend superflu le recoupement avec d'autres données d'identification telles que le nom, le prénom ou l'adresse.

Il insiste toutefois sur l'illusion de totale confiance qui pourrait être associée à ces identifiants numériques, tant par la baisse de vigilance au regard de la protection de la vie privée liée à un usage banalisé dès l'enfance (accès à la restauration scolaire, utilisation pour les prêts d'ouvrages dans les bibliothèques notamment), mais aussi, plus gravement, que par la quasi-impossibilité d'apporter la preuve d'une défaillance matérielle dont la portée pourrait créer d'importants préjudices et des difficultés considérables à assurer une défense en justice, le cas échéant.

Comment les citoyens de l'Union européenne seront-ils en mesure de se rendre compte d'une éventuelle erreur et d'exercer leur droit à rectification ? Quel en serait le coût réel ? Quelles réparations pour préjudice (s) subi(s), le cas échéant ? Quel délai pour l'obtention de l'information et la notification de sa rectification ?

Le groupe de l'article 29 conclut enfin par l'expression de sa forte préférence pour les systèmes fondés sur des données biométriques dont la collecte, la numérisation et la finalité du traitement ne s'effectue pas à l'insu des personnes à partir de traces qu'elles ont laissées sans y prêter attention (empreintes digitales, ADN...), qui ne soient pas centralisées dans un système unique, qui ne conduisent pas automatiquement à l'interconnexion avec d'autres systèmes et fichiers du fait même de leur architecture technique, et qui facilitent l'exercice du contrôle des traitements réalisés sur la base des données personnelles numérisées par les personnes concernées.

Le Parlement européen a adopté une résolution législative parlementaire le 2 décembre 2004 sur le projet de règlement du Conseil établissant des normes pour les dispositifs de sécurité et les éléments biométriques intégrés dans les passeports des citoyens de l'Union européenne, qui va dans le sens des recommandations du groupe de l'article 29. En effet, il a adopté un amendement à l'article 1er du règlement, selon lequel **« il n'est établi aucune base centralisée des passeports et documents de voyage de l'Union européenne contenant des données biométriques et autres de tous les titulaires d'un passeport de l'UE.** »

CONCLUSION

Le rapport a permis de montrer l'émergence d'une technologie d'identification d'entités numériques, dont le développement le plus rapide est présent dans le domaine logistique, en complément des technologies de code-barres, à ce stade.

La feuille de route technologique des puces RFID, d'une part, l'accélération de l'équipement des acteurs en systèmes d'information permettant de développer de manière performante la connaissance des stocks et des flux, mais aussi la connaissance des transits et des comportements, ouvrent des perspectives de marché importantes, bien au-delà de la simple substitution, à terme, d'un système entièrement numérisé et sans contact, mondialement interopérable, au système du code-barres.

Le rapprochement, voire l'identité des acteurs les plus significatifs des infrastructures du système de nommage de l'internet (DNS) et du système de numérotage des objets (ONS), laisse envisager des dérives incontrôlables en termes de captage d'informations de nature commerciale, économique, financière, technologique et, en un mot, stratégique.

La prise de conscience d'une concentration des pouvoirs d'intervention autour de quelques acteurs, venant renforcer le leadership américain dans la maîtrise des systèmes d'information, est encore faible voire inexistante, tant auprès des acteurs du marché que des autorités publiques, en France et dans l'Union européenne.

S'agissant de la protection des données à caractère personnel numérisées et des usages non licites de données identifiantes quant à la personne et à son comportement, la France et l'Union européenne sont encore à la recherche d'un point d'équilibre institutionnel.

La démultiplication des occurrences de collecte et des opportunités de traitement par interopérabilité et exportation de données à des « tiers », la mise en place de relations plus ou moins formalisées du point de vue contractuel entre acteurs privés et professionnels de l'internet, mais aussi le développement fort de l'administration électronique, créent un véritable dilemme à la société civile, dont les attentes parfois contradictoires n'aident pas les pouvoirs publics à choisir aisément les politiques les plus appropriées.

Des instruments juridiques contraignants existent désormais pour exposer les limites et sanctionner les usages délictueux. Toutefois, l'insuffisance de veille technologique et le retard dans l'adoption de modes coercitifs appropriés pour faire respecter la loi, au-delà des diligences dues par les acteurs, créent un contexte défavorable au libre arbitre et à la confiance requise pour la généralisation de la société de l'information au bénéfice du plus grand nombre.

Il existe un champ de recommandations à explorer pour pallier les faiblesses identifiées, qui va au-delà des simples conseils, mais propose d'intégrer dans le programme d'action du CGTI la préparation d'un cahier des charges pour l'évaluation dynamique et le contrôle des évolutions technologiques en France en ce domaine.

Le rapport prévu au programme 2004 sur l'Identité numérique pourra servir d'exposé des motifs à ce cahier des charges. Il présentera les problématiques de l'identification sous trois angles, à savoir la création, le traitement et l'usage des données personnelles ; la traçabilité des objets pendant tout le cycle de vie du produit ; et enfin celle des services. Il abordera les applications licites et celles qui peuvent être pratiquées de manière volontairement occultée, qu'elles entrent ou non dans le cadre de la licéité.

RECOMMANDATIONS

1. Effectuer une analyse approfondie des menaces présentées par les technologies RFID, qu'elles visent les personnes, les entreprises ou la souveraineté nationale, notamment eu égard à leur facilité d'usage.

2. Sensibiliser les acteurs de l'offre et de la demande en matière de RFID aux opportunités et aux menaces présentées par cette technologie.

3. Mettre en œuvre la pédagogie correspondante (colloques, forums, articles, ...), de façon à créer la confiance dans le grand public et d'armer les pouvoirs publics pour préserver la souveraineté nationale.

4. Adapter l'offre de services en matière de RFID à la lumière du retour d'expérience.

5. Favoriser les initiatives professionnelles, qu'elles viennent des fabricants ou des utilisateurs, en vue du développement d'applications RFID de nature à engendrer une confiance bien comprise du consommateur et du citoyen.

6. Evaluer l'applicabilité de la loi garantissant la protection des données à caractère personnel du point de vue de la technologie d'identification numérique par radio.

7. Favoriser la participation de la France aux instances de normalisation et fora internationaux en matière de technologie RFID, de nommage alternatif et d'adressage.

8. Investir dans la recherche sur les effets économiques et sociaux des technologies RFID et des systèmes d'information qui sous-tendent les applications de portée sociétale.

Conseil Général
des Technologies de l'Information

Comité de l'Inspection

LES TECHNOLOGIES DE RADIO-IDENTIFICATION (RFID) : ENJEUX INDUSTRIELS ET QUESTIONS SOCIETALES

Rapport présenté par

Françoise ROURE, Inspecteur général
Jean-Claude GORICHON, Inspecteur général
Emmanuel SARTORIUS, Ingénieur général

A N N E X E S

Rapport N° II-B.9 - 2004
Janvier 2005

SOMMAIRE des ANNEXES

_____

ANNEXE 1

Acronymes

AESRI : Agence Européenne pour la Sécurité des Réseaux et de l'Information (en anglais : ENISA, European Network Information Security Agency)

CEDH : Convention Européenne des Droits de l'Homme

CISC : Complex Instruction Set Computer

CNIL : Commission Nationale de l'Informatique et des Libertés

DNS : Domain Name System

DoC : Department of Commerce

DoD : Department of Defense

DOI : Digital Object Identifier

GAC : Government Advisory Committee

GAO : General Accounting Office

GIP : Groupement d'Intérêt Public

GPRS : General Packet Radio Service

GSM : Global System for Mobile communications

IP : Internet Protocol

JAI : Justice et Affaires Intérieures (Conseil)

ONS : Object Numbering System

RFID : Radio Frequency Identification

RISC : Reduced Instruction Set Computer

UID : Universal Identity

WGIG : Wireless Global Information Grid

ANNEXE 2

Bibliographie

_____

Dispositions juridiques citées dans le rapport :

Droit français

Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Code pénal, articles 226-16 à 226-24, section V, « Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques ».

Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie, « dossier médical personnalisé » art. 3 et « utilisation des données de santé » art. 64.

Droit de l'Union européenne

Règlement (CE) n° 45/2001 du Parlementent européen et du Conseil du 18 décembre 2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JOCE du 12 janvier 2001).

Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JOCE du 23 novembre 1995).

Directive 2002/58/CE du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (JOCE du 31 juillet 2002).

Décision de la Commission n° 2002/16/CE du 27 décembre 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE.

Décision n° 1247/2002/CE du Parlement européen, du Conseil et de la Commission du 1er juillet 2002 relative au statut et aux conditions d'exercice des fonctions de contrôleur européen de la protection des données (JOCE du 12 juillet 2002).

Décision n° 2004/55/CE du Parlement européen et du Conseil du 22 décembre 2003 portant nomination de l'autorité de contrôle indépendante prévue à l'article 286 du Traité de la Communauté européenne (contrôleur européen de la protection des données) (JOCE du 17 janvier 2004).

Council resolution (2003/C 48/01) of 18 February 2003 on a European approach towards a culture of network and information security (JOCE C 048, 28 février 2003).

Résolution législative parlementaire le 2 décembre 2004 sur le projet de règlement du Conseil établissant des normes pour les dispositifs de sécurité et les éléments biométriques intégrés dans les passeports des citoyens de l'Union européenne (P6_TA-PROV (2004) 0073 A6-0028/2004).

Proposition de décision du Conseil portant création du système d'information sur les visas (VIS) (COM (2004) 99 final).

Charte européenne des droits fondamentaux, art. 8 (futur II-8 du projet de Constitution), adoptée par le Sommet européen de Nice, juin 2002.

Article 29 – Data protection Working Party, « Working document on biometrics », 1268/02/EN WP 80, 01/08/2003, 11 p.

Droit international

Convention 108 du Conseil de l'Europe (Convention de sauvegarde des droits de l'homme et des libertés fondamentales, dite convention européenne des droits de l'homme/CEDH), adoptée en 1981, ratifiée par 31 Etats membres du Conseil de l'Europe, art. 8 notamment.

Rapports

La RFID dans la distribution : une technologie prometteuse mais limitée à la sphère logistique ? Synthèse Amérique du Nord, Asie, Europe occidentale. Ministère de l'économie, des finances et de l'industrie , DREE 5 C, avril 2004, 21 p.

L'Hyper République. Bâtir l'administration en réseau autour du citoyen. Rapport remis à Henri Plagnol, secrétaire d'Etat à la réforme de l'Etat par Pierre de La Coste. Rapporteur Vincent Bénard. 8 janvier 2003.

Spécifications techniques

Department of Defense standard practice. Military marking for shipment and storage. (Point 4.9 RFID), 29 octobre 2004.

Articles

Anne Debet, commissaire membre de la CNIL, « L'Europe de la sécurité », 23 juillet 2004. Tribune in http://www.cnil.fr.

Brett Glass : « Microsoft's Palladium : security for whom ? 24 juin 2004, in http://www.extremetech.com/print_article/0,3998,a=28481,00.asp.

Etienne Wery : « *La France transpose enfin la directive vie privée de 1995 ! La loi du 6 août 2004 est publiée au JO* », 11 août 2004, in http://www.droit-technologie.org/1_2.asp?actu_id=971.

ANNEXE 3

Sites Internet

http://www.dodrfid.org

http://www.EPCglobalUS.org

http://www.verisign.com

http://www.edps.eu.int Site du contrôleur européen de la protection des données.

http://europa.eu.int/comm/internal_market/privacy/links1_fr.htm Site de la Commission européenne sur les liens utiles relatifs à la politique de protection des données personnelles.

http://privacy.msn.fr Site de Microsoft relatif au cadre et aux engagements de respect des données personnelles numériques collectées par les sites et services MSN (par exemple MSN Hotmail, MSN Money ou MSN Health...).

http://www.ietf.org/internet-drafts/draft-ietf-marid-core-03.txt Site de l'IETF relatif au document de travail sur l'authentification des domaines de l'adresse des expéditeurs de courrier électronique. 2004, 10 p.

http://english.peopledaily.com.cn. rubrique Science-éducation, 29 septembre 2002 en particulier.

ANNEXE 4

Documents annexés

_____

- **4.1 UID *registry concept* : représentation graphique DOD et calendrier prévisionnel**

- **4.2 *Military marking for shipment and storage*. MIL-STD6129P w/Change 3 29 october 2004, DoD**

- **4.3 *Radio Frequency Identification (RFID) Policy*, The Under Secretary of Defense, DOD, Jul 30, 2004**

- **4.4 "*Verisign to run EPC Diretory*", RFID Journal, January 13, 2004**

- **4.5 Demain, une autre gouvernance de l'INTERNET, présentation .ppt, J-C. Gorichon, 4 janvier 2005**

- **4.6 Position de l'IEEE contre l'utilisation d'identifiants universels (UIDs)**

- **4.7 *Verisign : the EPC Network : Enanhancing the Supply Chain (White paper) 2004***

ANNEXE 4.1

UID *registry concept* : représentation graphique DOD et calendrier prévisionnel

ANNEXE 4.2

***Military marking for shipment and storage*.**
MIL-STD6129P w/Change 3 29 october 2004, DoD

ANNEXE 4.3

***Radio Frequency Identification (RFID) Policy*,**
The Under Secretary of Defense, DOD, Jul 30, 2004

ANNEXE 4.4

"*Verisign to run EPC Diretory*", RFID Journal, January 13, 2004

ANNEXE 4.5

Demain, une autre gouvernance de l'INTERNET,
présentation .ppt, J-C. Gorichon, 4 janvier 2005

ANNEXE 4.6

Position de l'IEEE contre l'utilisation d'identifiants universels (UIDs)

ANNEXE 4.7

Verisign : the EPC Network : Enanhancing the Supply Chain (White paper) 2004