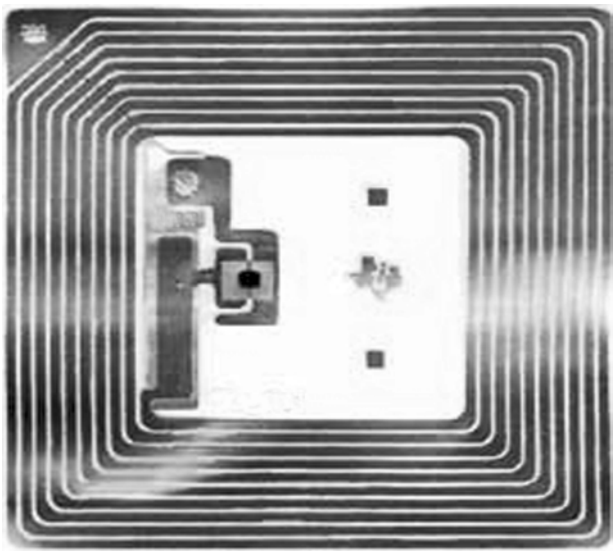


Traçabilité contre vie privée : les RFIDs

Ou l'immixtion des technologies dans la sphère personnelle

Xavier Lemarteleur

DESS Droit du multimédia et de l'informatique
Université Paris II – Panthéon / Assas
Mémoire réalisé sous la direction de Monsieur G. KOSTIC

Octobre 2004

Contact : xavier.lemarteleur@free.fr

Remerciements,

Je tiens à remercier M. Le Professeur J. Huet
ainsi que toute l'équipe professorale du
DESS Droit du Multimédia et de l'Informatique,
avec une attention particulière à mon maître de mémoire
M. G. Kostic et à
M. F. Coupez pour son aide et ses conseils avisés.

Un grand merci à la Commission Nationale de l'Informatique et des Libertés
où j'ai pu faire mon stage dans le cadre du
DESS Droit du Multimédia et de l'Informatique.

Plan

Introduction

> *Jadis, l'identité n'était qu'une « rumeur » faisant consensus. Vos proches ou votre voisinage pouvaient l'attester : on était qui on était parce que chacun en convenait. Le code civil conserve trace de cette histoire à travers la possession d'état, c'est-à-dire le témoignage humain confirmant ce que chacun observe et qui a valeur de preuve devant le juge, notamment en matière de filiation. L'identité est désormais devenue affaire de techniciens à la recherche d'une preuve informatique de l'identité, d'un numéro d'identification, d'une carte d'identité infalsifiable. Le temps n'est plus à la rumeur mais à la rationalité. On n'est plus qui on est parce que cela se dirait ; on est qui on est parce qu'un fichier informatique l'atteste.*
>
> CNIL, 22ème rapport année 2001 p.97

Traçabilité, le mot est devenu d'usage commun dans nos sociétés modernes, pourtant son apparition est récente dans notre vocabulaire et la notion reste encore absente de la plupart des dictionnaires. La traçabilité pourrait être définie *« en première approche, comme la possibilité qu'offrent les techniques modernes, à des fins d'information du public, de suivre pas à pas, en une sorte de « trace » continue, les produits de l'industrie dès qu'ils sont diffusés par le grand et le petit commerce. Ils sont en effet marqués, dès leur fabrication, par une information spécifique qui se maintien tout au long de leur vie en quelque lieu qu'ils se trouvent. On pourra ainsi à tout moment identifier un objet, défini par une information virtuelle que les réseaux électroniques diffusent sur toute la planète, de son origine à sa fin, et du producteur au consommateur »*[1].

L'essor du concept de traçabilité peut trouver ses origines notamment dans la crise qu'a connue la filière bovine et dans celle rencontrée au sujet des produits de santé. Ces différentes crises ont ainsi été l'occasion d'une appréhension par le droit de cette notion. Différents textes organisent les modalités de traçage des produits considérés comme sensibles pour la santé publique[2].
Depuis la traçabilité est devenue un centre d'intérêt primordial pour le secteur industriel. L'émergence de technologies de pointe permet en effet d'envisager de façon plus globale la traçabilité des biens et des personnes[3].

---

[1] J. F. Mattéi, Traçabilité et responsabilité, In Traçabilité et responsabilité sous la direction de P. Pedrot, Ed Economica, p. 35. L'auteur poursuit, complétant son ébauche de définition, en précisant que *« bien entendu, et dans la mesure où toute trace est indifférente à celui qui la laisse, tout en le trahissant en un certain sens, on n'a pas hésité à appliquer la traçabilité, non pas à des marchandises industrielles, mais au hommes qui les produisent dans les milieux du travail afin de suivre et de contrôler leurs comportements. On aurait tort de s'en formaliser, du moins dans le principe, même si la traçabilité semble ravaler le travailleur au statut de produit. En réalité, le monde moderne étant essentiellement défini par la généralisation de l'information du fait de l'ubiquité de ses moyens techniques, il est naturel que l'homme lui-même se trouve inscrit dans un système d'identification global (...) »*

[2] On peut ainsi citer de manière non exhaustive : l'arrêté du 10 février 2000 portant création de la base de données nationales d'identification et de traçage des bovins et de leurs produits, ou encore le décret du 6 mai 1995 qui a inséré dans le code de la santé publique l'article R-5144-25 qui définit la traçabilité.

[3] Bien que la distinction doive normalement être faite entre traçabilité des personnes et des choses. Ainsi on retrouve une *« distinction du droit entre les personnes et les choses, la traçabilité des premières étant bien différente de la traçabilité des secondes. La traçabilité des personnes est un vieux rêve du pouvoir politique, à l'origine du nom, de l'état civil, du passeport, du domicile (...).Cette traçabilité est parfois avouée, souvent*

Il est vrai qu'historiquement on peut constater qu' *« une poignée de découvertes remontent à la seconde moitié du XIX ème siècle et au début du XX ème : le microphone puis le téléphone (...), la photographie instantanée suivie des appareils d'enregistrement des sons et de l'image filmée. Ce que la doctrine américaine appelle le premier défi technologique fut suivi d'un second défi qui se poursuit de nos jours. Nul besoin d'insister sur les multiples moyens d'observation à distance, de captation, d'enregistrement et de reproduction de l'image et du son qui, difficiles ou impossible à détecter, ont transformé l'être humain en un animal exposé à une surveillance insidieuse et, dans le pire des cas, constante. (...) L'informatique permet de gérer des stocks illimités de données, aisément disponibles et détachées des supports matériels traditionnels. La société de l'information est ainsi devenue une société de l'informatique, ce qui a bouleversé l'antique relation entre l'individu et les renseignements auxquels il a accès ou qui le concernent »*[4].
Ainsi les technologies de l'information et de la communication (ou TIC)[5] sont désormais omniprésentes dans notre vie quotidienne. Les « puces »[6] ont envahi notre monde et leur prolifération n'en est qu'à ses débuts. L'ordinateur offre à l'être humain des possibilités accrues en matière de traitement de l'information, cependant l'informatisation de notre société peut avoir des effets pervers notamment à l'égard de la vie privée[7]. En effet l'automatisation des tâches et la vitesse de traitement offertes par les machines permettent de collecter et de retracer les informations provenant de multiples sources. En parallèle l'utilisation des TIC induit nécessairement la production de traces souvent nécessaires aux machines afin de pouvoir remplir leurs fonctions[8].

La possibilité ainsi offerte a conduit le législateur à s'intéresser très tôt aux enjeux induits par le développement des techniques principalement au regard de la protection des personnes. Ainsi dès 1978 la France se dotait des moyens de contrôler le respect de la vie privée et des données personnelles dans l'usage des technologies. La loi 78-17 du 6 janvier 1978 fut adoptée suite au projet SAFARI (Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus) qui organisait l'interconnexion de différents fichiers grâce à un

---

cachée (...). La traçabilité des choses est une entreprise plus récent, liée à la production de masse, au libre échange et aux risques propres à ce système de circulation généralisée. Elle s'annonce officiellement comme un instrument du principe de précaution ». M. A. Hermitte, La traçabilité des personnes et des choses, Précaution, pouvoir et maîtrise, In Traçabilité et responsabilité, Précité. p. 1.

[4] F. Rigaux, L'individu, sujet ou objet de la société de l'information, In La protection de la vie privée dans la société d'information, Groupe d'études Société de l'information et vie privée, sous la direction de P. Tabatoni, Paris, P.U.F. p. 118.

[5] On parle souvent de « nouvelles technologies » de l'information et de la communication (NTIC), cependant il semble que l'adjectif « nouvelles » doive être abandonné. En effet en raison de la place qu'occupe l'informatique dans notre vie quotidienne et ce depuis plusieurs années il semble peu approprié d'employer l'adjectif « nouvelle », même s'il est vrai que l'on se surprend encore à user de cet adjectif pour désigner le continent américain (Nouveau Monde) alors que sa découverte remonte à plusieurs siècles.

[6] En référence aux composants électroniques utilisés dans le monde informatique qui par leur apparence (petits, noirs et dotés de multiples pattes) ne sont pas sans rappeler ces parasites.

[7] *« L'informatique aux fabuleux bienfaits comporte, en revers, une aptitude effrayante : la mémoire totale, instantanée. A la fois par la minutie, l'immensité, la fréquence des informations recensées sur la vie quotidienne, donc largement privée ; par une capacité sans limites de conservation de ces données, cela sous un volume de plus en plus restreint, qui permet le transfert instantané de telles informations ; par une aptitude de tri à la vitesse de la lumière, d'où s'ensuit la facilité des rapprochements et recoupements les plus inattendus, mais d'autant plus révélateurs. »* J.C. Soyer, In La protection de la vie privée dans la société de l'information, Précité, Tome 1, 2000, p. 9 et s

[8] Ainsi les ordinateurs enregistrent des traces des actions effectuées dans des fichiers communément dénommés « logs ». Il en va de même de toute connexion à l'internet qui laisse apparaître chez le fournisseur d'accès à l'internet des traces sous forme de dates, heures, adresse IP de la connexion,…

identifiant unique, le numéro d'inscription au Répertoire National d'Identification des Personnes Physiques de l'INSEE (RNIPP). Ce projet a provoqué un certain émoi dans la population française caractérisé dans un article parut dans Le Monde en 1974 et devenu célèbre : « *SAFARI ou la chasse aux Français* ». De nos jours l'utilisation massive de l'outil informatique conduit à la transformation des atteintes potentielles à la vie privée, la constitution de bases de données contenant des informations nominatives fait désormais appel à des procédés de haute technicité, tel est le cas notamment de l'identification par radiofréquence (plus fréquemment dénommée RFID[9]). Celle-ci, comme nous le verrons plus loin, fait appel à des micro-puces insérées le plus souvent dans des étiquettes qui elles-mêmes sont apposées sur des produits de consommation. Ces « étiquettes intelligentes » sont usuellement dénommées sous l'acronyme RFID en raison de la technologie utilisée.

Les RFIDs en quelques mots

Il convient de replacer les RFIDs dans un contexte historique ce qui permettra de voir comment une technologie, qui à l'origine ne paraissait pas devoir présenter de menaces pour les libertés individuelles, a pu, de part son développement, être ressentie comme une atteinte potentielle à la vie privée.
Ensuite, afin de bien appréhender les enjeux que représentent les RFIDs au plan juridique, il semble utile, voire nécessaire, de considérer les aspects techniques de leur fonctionnement. A partir de ces constations d'ordre technologique il sera alors plus aisé de comprendre pourquoi les RFIDs ont tant bouleversé une partie de l'opinion publique qui tend à y voir une solution permettant le traçage des individus.

Approche Historique

Les RFIDs (aussi dénommés radio tags, tag ou encore étiquettes intelligentes) sont de petits émetteurs radio constitués d'une puce et d'une antenne.
Ces étiquettes de haute technicité sont en fait issues d'un concept ancien découvert dès 1948[10]. Le principe physique d'une communication par voie électromagnétique était ainsi fixé mais la réalisation pratique nécessitait certains éléments encore indisponibles à cette époque. Ce fut dans les années 1950 que le concept fut repris[11] et mis en œuvre pour la première fois dans l'aéronautique afin de distinguer les avions ennemis des appareils amis ; ce système alors appelé IFF (*Identify: Friend or Foe*, soit littéralement : identifier : ami ou ennemi) est encore utilisé de nos jours pour identifier les avions. L'essor de cette technologie a pu permettre, au plan militaire, un traitement automatisé des avions ennemis en combat aérien en guidant les missiles directement sur l'avion ayant une signature ennemie, et a fait naître le concept du *« fire and forget »* (tirer et oublier), le tir étant verrouillé sur le transpondeur des avions adverses.

[9] Qui est en fait l'acronyme de ***R****adio* ***F****requency* ***Id****entification.*
[10] Harry Stockman, *Communication by Means of Reflected Power*, p. 1196-1204, Octobre 1948.
[11] F. L. Vernon's, *Application of the microwave homodyne*, et D.B. Harris, *Radio transmission systems with modulatable passive responder.*

Mais ce fut dans les années 1960 que l'utilisation des tags connut un essor important avec la commercialisation du système EAS[12] communément utilisé comme moyen de lutter contre le vol.
Durant les décennies 1970 et 1980 de nombreuses expérimentations furent menées visant à utiliser les RFIDs en tant que moyens d'identification grand public notamment afin de réguler l'accès à des sites sensibles.
Depuis 1990 l'utilisation des tags radio s'est grandement répandue[13]. Ceci est principalement le fait des progrès techniques réalisés dans le domaine de l'informatique et de la micro-électronique[14]. De fait de nos jours la miniaturisation de composants électroniques est telle que les tags mesurent moins d'un millimètre, ils peuvent même être miniaturisés pour atteindre l'aspect d'une sorte de poussière[15]. Ainsi *« les RFIDs sont utilisés pour des centaines, si ce n'est des milliers, d'applications comme par exemple la lutte contre le vol des automobiles, payer le péage sans s'arrêter, réguler le trafic, autoriser l'accès aux immeubles, ouvrir les portails aux véhicules, identification sur les campus et aéroports, fournir des biens, donner accès aux téléskis, suivre des livres dans une bibliothèque, acheter un hamburger, et plus encore survient la possibilité de suivre les produits tout au long de la chaîne de production »*[16].

Approche technologique

Les tags utilisés couramment de nos jours sont de types quelques peu différents. On distingue ainsi les RFIDs[17] passifs et actifs, à cette première distinction vient s'en ajouter une seconde entre tags permettant la lecture seulement et ceux autorisant à la fois la lecture et l'écriture.

---

[12] *Electronic Article Surveillance* utilisant un transpondeur (tag) ne disposant que d'une mémoire très petite (1 bit) n'autorisant le stockage que d'une seule information du type oui/ non et donc permettant uniquement de détecter la présence ou l'absence de tag.

[13] Pour de plus amples développements sur l'histoire de la technologie des RFIDs: *RFID a week long survey on the technology and its potential, Radio Frequency Identification*, Harnessing Technology Project, disponible à l'adresse suivante http://www.interaction-ivrea.it . Voir aussi: *Shrouds of Time–The history of RFID,* J. Landt and B. Catlin. Disponible sur le site http://www.aimglobal.org.

[14] Ainsi en informatique la loi de Moore (en référence à son auteur G. Moore) énoncée en 1965, vérifiée depuis de manière empirique, stipule que *« le nombre de transistors d'un microprocesseur double tous les deux ans environs »*.

[15] Il a été présenté un type de puces RFID si petites qu'elles ressemblaient à une sorte de poussière de couleur bleue. Selon l'auteur d'un article cette poudre pourrait être introduite dans les CD lors de leur fabrication ou pourquoi pas dans des savons. The inquirer, *Hitachi shows off RFID dust*, article disponible à l'adresse internet suivante: http://www.theinquirer.net/Default.aspx?article=14819, de même une nouvelle technologie permet simplement d'imprimer des puces RFID grâce à une encre spéciale. RFID journal, *Firewall Protection for Paper Documents*. http://www.rfidjournal.com/article/articleprint/790/-1/1/. Dans ce cas le tag ne doit pas avoir d'antenne mais le composé du produit dans lequel il est incorporé peut remplir cet office, comme par exemple la fine couche métallisée contenue dans un disque compact.

[16] *Shrouds of times, the History of RFID*, AIM publications. p. 3. Disponible sur le site http://www.aimglobal.org. Traduction libre de l'anglais.

[17] On usera tout au long de cette étude du terme générique de « RFID » ou encore « tag » mais, plus rigoureusement, il convient de noter que ces termes recouvrent plusieurs en fait plusieurs applications distinctes. En effet *« les Rfid ont au moins trois "killer applications" : les "smart labels" (étiquettes intelligentes destinées à améliorer la traçabilité des produits et l'optimisation de la chaîne logistique), les "smart cards" (cartes intelligentes, pour développer des systèmes "sans contact" de contrôle de billets, de péages, ou d'entrée dans les bâtiments) et les "smart tags" (tatouages intelligents, pour améliorer la sécurité, par exemple en immobilisant des voitures volées, ou pour localiser des biens - ou des animaux - perdus). »* Mario Rivas, vice-président de Philips Semiconductors. Propos recueillis lors du *« RFID Privacy Workshop »* du Massachusetts Institute of Technology (MIT). Compte rendu disponible sur le site http://www.fing.org.

Quoi qu'il en soit un radio tag comprend au minimum un microprocesseur (puce) et une antenne. C'est principalement au niveau de la puce que les distinctions peuvent être faites[18] :

- D'abord en raison de la quotité et du type de mémoire[19] dont dispose la puce. Il est clair que plus le composant disposera de mémoire plus la quantité d'informations pouvant être stockées dessus pourra être importante. Ensuite cette mémoire peut être simplement réservée à l'écriture (*Read*) ou permettre à la fois la lecture et l'écriture (*Read/Write*). Dans ce second cas il sera possible d'ajouter des informations sur la puce ultérieurement (par exemple au passage d'un produit en caisse), le contenu du tag peut alors s'enrichir dans le temps.

- Ensuite selon que le tag dispose ou non d'une alimentation propre. En effet il existe des RFIDs passifs (qui sont alimentés par le courant induit généré par le lecteur de tag) et actifs (qui disposent d'une pile assurant leur alimentation électrique). Une sous distinction est opérée au sein des tags actifs entre ceux équipés d'un émetteur et ceux qui en sont dépourvus. D'une manière globale on peut considérer que les RFIDs actifs sont plus performants notamment quant à la portée de réception[20] (mais bien plus coûteux) que les passifs.

Les possibilités offertes sont ainsi multiples, et le coût des tags varie grandement selon la technologie retenue, d'une dizaine de centimes à une dizaine d'euros pièce.

[18] Sur le développement de ces points techniques nombre d'articles peuvent être cités mais on renverra le lecteur curieux aux documents suivants : S. Hodges et M. Harrison, White *paper : Demystifying RFID : principles and practicabilities*, octobre 2003 disponible sur le site http://www.autoidlabs.org/, The Association for the Automatic Identification and Data Capture Industry (AIM), *Draft paper on the characteristics of RFID-sytems*, juillet 2000 disponible sur le site http://www.aimglobal.org, mais surtout K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, chapitre 3, p. 29.

[19] Ici les puces peuvent être équipées de quelques bits à plusieurs kilo-octet d'espace mémoire pour le stockage de données ce qui permet l'écriture de quelques informations à plusieurs milliers de caractères.

[20] La portée d'un tag peut aller de quelques centimètres à plus d'une centaine de mètres.

Les RFIDs sont souvent perçus comme présentant un risque important d'atteinte à la vie privée. Cela est principalement dû au fait que leur emploi est destiné à se généraliser dans un avenir très proche.
En effet l'utilisation de cette technologie permet la lecture, à distance, des informations stockées dans la puce RFID. Un exemple concret est fourni par la Régie Autonome des Transports Parisiens (RATP) qui a développé cette solution sous le nom de Navigo pour les abonnements de transport en remplacement des traditionnels coupons à valider. En pratique l'usager disposant d'un passe Navigo ne doit plus introduire son billet pour accéder aux quais, il lui suffit simplement d'approcher sa carte contenant une puce RFID du lecteur incorporé au portillon pour que la machine lise le contenu de sa carte et détecte un abonnement valide pour finalement lui accorder le passage.
Ainsi *« Navigo résume à lui seul tout l'intérêt - et tout le danger potentiel - de la technologie. L'usager n'a pas le sentiment d'utiliser le dernier cri de la technologie sans fil, et ignore d'ailleurs le terme même de RFID. Il se contente d'utiliser une carte fonctionnelle et pratique, qu'il n'est même pas nécessaire de sortir de son portefeuille ou de son sac pour voir s'ouvrir les portillons du métro. Pour la Ratp, le dispositif est un outil de régulation et de connaissance des usages de tout premier ordre. Il n'en demeure pas moins que le système "pourrait" être utilisé pour surveiller en permanence les déplacements individuels de chacun des parisiens (...) »*[21]. Le risque est ici bien résumé, il consiste en la difficulté de connaître l'usage effectif qui sera fait de la technologie, l'utilisation des tags est empreinte d'un manque de transparence, d'ailleurs la CNIL n'a pas manqué de se préoccuper des enjeux induits par l'utilisation des RFIDs dans le cadre des transports. Elle a ainsi constaté que *« les traitements automatisés mis en œuvre pour assurer le bon fonctionnement de ces titres billettiques créent un risque sérieux en matière de protection des données personnelles. En effet, les déplacements des personnes utilisant ces cartes peuvent être reconstitués et ne sont plus anonymes, ce qui est de nature à porter atteinte tant à la liberté, fondamentale et constitutionnelle, d'aller et venir, qu'au droit à la vie privée qui constitue également un principe de valeur constitutionnelle »*[22].
La technologie permet de nos jours d'identifier les individus. Alors que, dans le cadre des transports, le traditionnel billet offrait à son utilisateur un total anonymat, l'emploi des tags conduit à une identification automatique de l'usager.
Mais cet exemple fourni par la RATP ne constitue pas un cas isolé, l'emploi des RFIDs est appelé à se généraliser, nombre de projets sont en cours de réalisation pour implanter ces puces dans tous les biens de consommation[23]. En effet la technologie de radio identification

[21] C. Fiévet, Rfid : entre mythes et réalités, la nécessité du débat. Article disponible sur le site http://www.fing.org
[22] CNIL Délibération N° 03-038 du 16 Septembre 2003 portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives par les sociétés de transports collectifs dans le cadre d'applications billettiques.
[23] On peut déjà citer des exemples comme speedpass aux Etats Unis qui permet de payer automatiquement les stations essence, ou encore Gillette qui a introduit des puces dans ses rasoirs, mais aussi la future insertion de tags dans les billets de banque européens. Cette liste est bien entendu non exhaustive, le nombre d'applications et de projets d'implémentation augmente chaque jour.

est promue par plusieurs organismes internationaux qui favorisent une standardisation des protocoles utilisés dans les tags[24].
A terme chaque produit manufacturé pourrait être reconnu et individualisé grâce à la puce qui y aura été incorporée. Ainsi il sera possible d'identifier individuellement[25] chaque cannette de soda à l'aide de son numéro unique qui sera différent d'une autre cannette de la même boisson de la même marque[26] en lisant, à distance et de manière totalement transparente, le numéro contenu dans la puce RFID.
L'utilisation de la radio-identification vise à améliorer la gestion des stocks dans le secteur industriel, il est certain que l'avantage en terme d'optimisation de la chaîne de production qu'autorise l'emploi des tags est non négligeable, mais les préoccupations de la société civile se sont tournées vers les usages annexes qui pourraient être faits de cette technologie. En effet avec la généralisation de l'emploi des RFIDs se profile la possibilité de tracer, géolocaliser et de profiler les actions de chaque individu en fonction de ce qu'il porte sur lui.

Il est ainsi possible d'imaginer ce que pourrait permettre la technologie RFID dans un avenir proche sous la forme d'une chronique relatant la vie quotidienne de tout un chacun.
Imaginons par exemple une personne qui, n'ayant plus d'encre dans son imprimante, décide de se rendre dans le supermarché le plus proche afin de se procurer à moindre coût une cartouche. Afin de ne pas se méprendre sur le modèle de consommable, elle décide d'emmener sa cartouche usagée sur laquelle est inscrite la référence de l'article. Arrivée dans la grande surface, elle reçoit sur son téléphone portable une publicité promotionnelle[27] pour des cartouches d'encre de marque générique (la puce RFID contenue dans le consommable usagé ayant été lue montre son intérêt pour cette catégorie d'article). Attirée cette promotion, elle décide d'acheter les cartouches génériques. Elle sort ensuite du magasin, le lecteur RFID à la sortie reconnaît automatiquement l'article et lit ensuite sa carte bancaire (elle aussi pourvue d'un tag), son compte sera automatiquement débité. Arrivée chez elle place le consommable dans son imprimante, cependant cette dernière refuse de fonctionner avec la nouvelle cartouche de marque générique (le lecteur de l'imprimante ne reconnaît pas de numéro valide propre au consommables de la marque et dont les génériques sont dépourvus)[28].

---

[24] Un des principaux organismes de promotion et de standardisation de la technologie RFID n'est autre que Massachusetts Institute of Technology (MIT) qui a mis en place deux groupes distincts : l'Autoid center qui est en charge de réaliser des études afin de promouvoir l'essor de l'emploi des tags et l'EPCglobal qui a pour mission de créer un standard (EPC pour Electronic Product Code) permettant une reconnaissance du contenu des RFIDs partout dans le monde grâce à un code unique standard lisible par tout lecteur.

[25] Cela est rendu possible par la norme EPC qui établi un standard à l'échelle mondiale pour l'identification précise de chaque objet. (Voir développement chapitre I B-p. 18).

[26] La possibilité de tracer les cannettes de soda est à l'étude depuis déjà plusieurs années chez Coca-Cola. Un article sur le sujet est disponible sur le site internet du Journal du net : http://solutions.journaldunet.com/itws/040120_it_coca_cola_entreprise.shtml

[27] Répondant à une interview Scott McGregor de Philips Semiconductor envisage ainsi l'utilisation qui pourra être faite de la technologie RFID dans les téléphones portables :
« We're discussing with a number of mobile-phone manufacturers embedding an RFID technology we call NFC, for near-field communications. Then the phone could pick up information from various things, like movie posters, and the tags could allow you to do things like carry an embedded Visa card. You'll see trials of such phones in the U.S. this year. » Article : *Like It or Not, RFID Is Coming*, interview disponible sur le site http://www.businessweek.com

[28] Il faut noter que ce genre de spéculation sur notre futur n'est pas irréaliste. Nombre d'entreprises disposent de projets assez similaires. Pour s'en persuader il suffit par exemple de se rendre sur le site de Microsoft (Microsoft Home Fact Sheet May 2002) disponible sur le site de Microsoft : http://www.microsoft.com/presspass/presskits/ 2002/mshome/docs/MSHomeFS.doc

On voit que même si l'utilisation de la radio identification, principalement dans la grande distribution, présente de nombreux intérêts en permettant l'automatisation de l'approvisionnement, la lutte contre le vol ou encore la sécurisation du transport des bagages et colis[29], *« les avantages de cette technologie peuvent aussi constituer un redoutable outil de profilage de la population de nature à porter atteinte à la vie privée des citoyens-consommateurs ! »*[30].

Face aux inquiétudes que suscite l'emploi massif des RFIDs, il convient de voir comment les lois qui constituent notre cadre juridique et au titre desquelles figure au premier plan la loi informatique et libertés de 1978, peuvent concilier RFID et vie privée (chapitre I). Il sera alors possible de voir quelles mesures sont envisageables afin de respecter l'intimité des personnes (chapitre II).

[29] Des tests sont actuellement en cours dans les aéroports de New York, Amsterdam et Singapour.

[30] N. Bondois et N. Samarcq, Les étiquettes intelligentes, l'univers Orwellien en marche ? Disponible sur le site http://www.clic-droit.com/web/editorial/article.php?art_id=267

Chapitre I – Appréhension de la technologie de radio-identification par la loi du 6 janvier 1978

Les technologies de radio identification sont susceptibles de permettre l'identification non seulement des objets mais aussi des personnes, offrant ainsi la possibilité d'entrer dans l'intimité de la vie privée[31] des individus. A ce titre diverses législations pourraient leurs être applicables, principalement celles relatives aux libertés publiques[32] et aux données personnelles. Au premier plan des textes protégeant l'individu, dans ce qu'il est désormais convenu de dénommer la société de l'information, figure la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[33] récemment modifiée[34]. Celle-ci envisage la protection des personnes au travers des données personnelles, traces indélébiles laissées au gré des relations humaines et souvent utilisées à des fin de fichage tant par l'administration que par les entreprises. Dans cette optique la loi institue une autorité administrative indépendante (la CNIL) en charge de veiller à la protection des données nominatives dans une société où l'informatique autorise le traitement massif de fichiers relatifs aux individus.
L'utilisation des RFIDs relève-t-elle de la loi de 1978 ? Il convient, à titre préliminaire, de vérifier que le système de radio identification permet bien le traitement de données nominatives. La première question a se poser sera alors celle de la qualification des tags (s'agit ou non d'informations personnelles ?) (I). Si cette première question reçoit une réponse positive, il s'agira ensuite de voir comment la loi informatique et libertés est susceptible de réguler l'utilisation de ces données (II).

I – Qualification des RFIDs en tant que données nominatives

Le texte de la loi de 1978 prend soin de définir ce qu'il faut entendre par données nominatives[35], le traitement informatisé de telles données entrant seul dans le champ d'application de la loi.

---

[31] Sur la notion de droit au respect de la vie privée et notamment sur la subtile distinction entre « informations » et « éléments » relatifs à la vie privée, voir A. Maitrot de la Motte, le droit au respect de la vie privée, In Protection de la vie privée dans la société d'information Précité, Tomes 3,4 et 5, p. 271 et s.

[32] On peut penser notamment à l'article 8 de la Convention Européenne de Sauvegarde des Droits de l'Homme du 4 novembre 1950 qui déclare dans son alinéa 1 *« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance »* ou encore l'article 12 de la Déclaration Universelle des Droits de l'Homme : *«Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes »* et enfin l'article 9 du code civil issu de la loi du 17 juillet 1970 qui prévoit que *« Chacun a droit au respect de sa vie privée ».*

[33] Il paraît utile de préciser que la Charte Européenne des Droits Fondamentaux du 7 décembre 2000 envisage, dans son article 7, la protection des données personnelles : *« Toute personne a droit à la protection des données à caractère personnel la concernant. Les données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».*

[34] 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 a été publiée au JO du 07 août 2004.

[35] La doctrine de la CNIL a pris soin de préciser ce qu'il convenait de considérer comme étant une donnée nominative : *« On entend par "information nominative", appelée aussi donnée à caractère personnel, toute information concernant une personne physique identifiée ou identifiable.*

- *Une personne est identifiée lorsque son identité apparaît dans un fichier.*

Ainsi, dans son article 2 alinéa 2[36], le texte précise que *« 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 susceptibles d'être raisonnablement mis en oeuvre, soit par le responsable du traitement, soit par une autre personne »*[37].

Il convient de rappeler la définition de la notion de donnée personnelle antérieurement au remaniement de la loi de 1978. L'article 4 prévoyait que *«sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale »*.

On peut percevoir une différence de rédaction entre les deux textes, le premier ayant une appréhension plus large de la notion de donnée nominative. En effet alors que la loi de 1978 originaire faisait une simple distinction entre ce qui identifie directement (typiquement le nom) ou indirectement (cas d'un numéro d'identification) une personne ; le nouveau texte semble vouloir introduire une nouvelle catégorie.

Ainsi en plus de cette première distinction se superposerait une seconde, seraient soumises à la loi les informations permettraient d'identifier un individu (c'est à dire le rendraient identifiable). Cela semble plus explicitement viser le cas des données permettant d'opérer un profilage des personnes[38]. On peut alors considérer que si la loi ne concerne pas les informations non nominatives, la multiplicité et le recoupement possible d'informations « anonymes » pourrait conduire à permettre d'identifier une personne et devrait donc être traité globalement comme étant une donnée nominative.

Cependant si la loi organise une distinction dans les données à caractère personnel, entre ce qui est directement et indirectement nominatif, c'est pour ensuite soumettre ces deux types d'informations à un régime juridique unique.

- *Une personne est identifiable lorsqu'un fichier comporte des informations permettant indirectement son identification (ex. : n° de matricule ou code, adresse IP, N° de téléphone, photographie...).*

Il peut s'agir évidemment d'informations associées au nom de la personne (par exemple "Benjamin Bernard a été condamné à 3 mois de prison"). Mais il peut s'agir aussi d'informations qui ne sont pas associées au nom d'une personne mais qui permettent aisément de l'identifier (par exemple, "le titulaire du numéro de ligne 0153732200 téléphone souvent au Sénégal" ou "le propriétaire du véhicule 3636AB75 est abonné à telle revue" ou encore "l'assuré social 1600530189196 va chez le médecin plus d'une fois par mois"). En ce sens, constituent également des données à caractère personnel, toutes les informations anonymes dont le recoupement permet d'identifier une personne précise (par exemple une empreinte digitale, l'ADN ou encore "le fils du médecin résidant au 11 boulevard Belleville à Montpellier est un mauvais élève"). »

[36] Cet article transpose en fait la directive 95/46 du Parlement Européen et du Conseil du 24 octobre 1995 qui définit ainsi la notion de données personnelles dans son article 2 :
« Aux fins de la présente directive, on entend par:
a) «données à caractère personnel»: toute information concernant une personne physique identifiée ou identifiable (personne concernée); 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; »
Encore pourrait on aussi ajouter la définition retenue par la convention 108 dans son article 2 qui pour sa part considère que le terme *«données à caractère personnel» signifie: toute information concernant une personne physique identifiée ou identifiable («personne concernée»); »*, Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signée à Strasbourg le 28 janvier 1981.

[37] Le texte de la « nouvelle » loi informatique et libertés est disponible à l'adresse suivante : http://www.cnil.fr/index.php?id=301

[38] Cet ajout semble consacrer une position déjà acquise par la CNIL notamment en ce qui concerne les informations statistiques. Voir Délibération CNIL n°89-10 du 14 février 1989 relative aux conditions générales de recensement de la population.

Dans le cas particulier des RFIDs la distinction a son importance, en effet il convient de noter que les tags radio ne constituent pas en eux-même une donnée nominative, ils ne sont qu'un vecteur qui sera chargé d'un message (le contenu inscrit dans la puce) qui, au final, pourra permettre une identification à distance. Ainsi un tag peut être, selon les cas, directement ou indirectement nominatif.

A- Les RFIDs en tant que données identifiant une personne

Le contenu inscrit dans une puce RFID sera directement nominatif dès lors qu'il permet d'identifier, de prime abord, un individu[39]. Il s'agit ici en tout premier lieu du nom patronymique pour lequel la qualification de donnée directement nominative ne peut faire aucun doute.
Mais de manière plus large toute donnée indirectement nominative est susceptible de rendre un individu identifiable. Les exemples de ce type de données sont légion, on peut penser principalement aux divers numéros d'identification, au premier plan desquels figure le célèbre numéro d'inscription au répertoire national d'identification des personnes physiques (RNIPP)[40]. Mais on peut aussi y ajouter tout élément qui peut être directement rattaché au nom, comme par exemple des coordonnées bancaires, un numéro d'abonnement, une plaque d'immatriculation d'un véhicule[41], une adresse de courriel[42], ou encore une image[43], un numéro de téléphone[44]…
L'utilisation de la technologie RFID ne modifie en rien le caractère nominatif de telles données. Alors que celles-ci figuraient généralement sur des supports papiers qui nécessitaient jusqu'à lors leur transmission volontaire aux personnes désireuses d'en effectuer le traitement, les radio-tags pourraient permettre de recueillir ces informations directement et de manière transparente en lisant les puces que la personne porte sur elle à distance.
Des cas concrets faisant appel à cette technologie existent déjà de nos jours, on peut ainsi citer le système mis en place par la RATP dénommé NAVIGO qui substitue au traditionnel billet de transport un abonnement contenu dans une puce qui est lue à distance par les portillons. Le mécanisme est simple, le tag est lu par le portique, le numéro d'abonnement contenu dans le RFID est transmis à une base de données et la validité de celui-ci est vérifiée pour décider d'octroyer ou non l'accès. Il est évident que ce numéro doit être regardé comme une donnée nominative dans le sens où il peut être rattaché (dans la base de données de la RATP) à un nom[45].
Un autre exemple nous provient de l'étranger, et plus précisément des Etats-Unis, où un système recourant aux RFIDs a été instauré permettant le paiement automatique des achats de carburant fait dans certaines stations essence[46]. En parallèle, en France on voit se multiplier les tags apposés sur les pare-brises des automobiles dans le but de lutte contre le vol[47].

---

[39] Sur ce point voir notamment : Lamy droit de l'informatique et des réseaux, ed Lamy 2003, n° 517
[40] Qui équivaut au numéro de sécurité sociale.
[41] CNIL délibération n° 94-056 du 21 juin 1994.
[42] CNIL délibération n° 99-048 du 14 octobre 1999.
[43] CNIL avis n° 87-121 du 15 décembre 1987.
[44] CNIL délibération n° 84-31 du 18 septembre 1984.
[45] Telle est d'ailleurs la position retenue par la CNIL dans sa délibération n° 03-038 du 16 Septembre 2003 portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives par les sociétés de transports collectifs dans le cadre d'applications billettiques.
[46] Le système dénommé SEEDPASS utilise le mécanisme suivant : *« l'identifiant contenu dans la puce Rfid y est couplé à un compte bancaire et se décline en trois dispositifs de paiement originaux. Le premier est un "tag autocollant" que l'on appose sur la lunette arrière d'une voiture, les autres sont de petits émetteurs portables, l'un s'attachant au porte-clé, l'autre inclus dans une montre-bracelet. Ces "portes-monnaies électroniques sans fil" comportent des tags Rfid (soit actifs, soit passifs), utilisés pour identifier l'utilisateur, instantanément*

On peut enfin citer à titre de dernier exemple le heurt ayant eu lieu lors du Sommet Mondial de la Société de l'Information, organisé à Genève sous l'égide de l'ONU à la fin de l'année 2003. Il fut révélé, postérieurement à la conférence que les badges qui avaient été remis aux différents participants étaient en fait pourvus d'une puce permettant la radio identification. Ceux-ci contenaient le nom, la photo, la fonction, l'organisation de rattachement, les heures des passages aux entrées/sorties et dans les salles de conférence de chacun des participants[48].
Les contenus inscrits dans les puces RFIDs sont, dans ces divers cas, directement liés à une personne identifiée, il en va de même dans les cas où les informations stockées auront trait à des caractéristiques physiques du porteur. L'intégration de données biométriques[49] est déjà utilisée dans les tags (photographie digitalisée)[50].
La question qui se pose alors est de savoir si tout un chacun aura la possibilité de lire le contenu de ces puces, en effet il convient de s'interroger sur la confidentialité des informations introduites dans les RFIDs. Ainsi le nom ou le numéro unique d'identification utilisé dans le titre de transport d'un abonné de la RATP est il susceptible d'être lu par le lecteur d'un supermarché[51]. Dans ce cas la traçabilité des personnes serait grandement facilitée, les individus pouvant alors être identifiés par leur nom ou indirectement par un numéro d'identification unique.
Le point mérite d'être évoqué car le nombre de projets tendant à incorporer des données nominatives permettant d'identifier des personnes va croissant. On peut citer notamment les futures cartes de vie quotidienne reposant sur la technologie RFID présentées par le Ministère de la Fonction Publique et dont le but est de *« permettre au citoyen de payer plus facilement les transports ou d'accéder à des services locaux »*. En vue d'une prochaine implémentation, des projets pilotes sont menés dans treize collectivités, ces *« projets explorent trois pistes principales pour faciliter les démarches quotidiennes: des cartes de transport, des cartes d'authentification et de contrôle d'accès, ou des cartes destinées aux étudiants et aux scolaires. Certains projets sont hybrides et proposent même de rassembler tous ces services*

---

et sans contact, à chaque achat. Concrètement, le tag de la voiture est automatiquement reconnu par la pompe à essence, qui autorise le propriétaire du véhicule à se servir. Une fois le réservoir rempli, le client s'en va. Seul l'identifiant personnel de son tag a été transféré, et sa carte bancaire est instantanément débitée. Les tags portatifs fonctionnent selon le même principe, mais étant passifs (sans batterie), ils nécessitent d'être à proximité du lecteur : le consommateur doit agiter son porte-clé ou sa montre à quelques centimètres d'un terminal ad hoc. Speedpass est d'ores et déjà accepté dans plus de 6 500 stations-service américaines (notamment dans l'ensemble des stations Mobil, le dispositif ayant été développé par le Groupe Exxon Mobil), dans plusieurs magasins de détail, et dans plusieurs centaines de restaurants MacDonald's. Le système compte 8 millions d'utilisateurs ». Propos issus de RFID : entre mythes et réalités, la nécessité du débat, disponible sur le site de l'association Fondation Internet Nouvelle Génération, http://www.fing.org/

[47] Le système appelé Identicar est présenté à l'adresse suivante : http://www.identicar.com/

[48] Pour plus de détails voir sur le site du journal du net RFID: les badges du sommet de Genève avaient des effets seconds, Par Christine Tréguier, ZDNet France, Mardi 23 décembre 2003, disponible sur le site : http://www.zdnet.fr/actualites/technologie/imprimer.htm?AT=39134545-39020809t-39000761c

[49] Sur la question de la biométrie et de ses implications au regard des données personnelles, voir : C. Guerrier, Protection des données personnelles et applications biométriques en Europe, Communication Commerce Electronique, n° 7-8, juillet-août 2003, p. 17.

[50] L'inclusion de données biométriques dans une puce sans contact peut aussi être fait en parallèle avec l'utilisation de véritables systèmes d'identification biométriques. Il semble que ce type de « double sécurité » soit grandement promu, notamment suite aux attentats du 11 septembre aux Etats Unis, principalement pour l'accès à certains sites sensibles tels les aéroports. Voir sur ce point: *Biometrics and RFID - Safe Choices to Meet Emerging Security Needs, Automatic Identification and Data Collection (AIDC) technologies provide the safety and security that users want today*, article disponible sur le site http://www.aim.org/.

[51] La question technique sous-jacente est celle de la cryptologie appliquée aux RFIDs. L'utilisation d'un système de chiffrement des informations contenues dans la puce pourrait permettre d'assurer la sécurité et la confidentialité de ces dernières. Notons qu'il semble que certains tags soient conçus pour permettre l'intégration d'un mécanisme de cryptologie.

sur une carte unique »[52]. Les futures cartes de vie quotidiennes, présentées comme un progrès simplifiant les relations que tout un chacun est amené à entretenir avec l'administration pourraient-elles avoir pour effet second de permettre de tracer les administrés ?[53].

Ce projet n'est d'ailleurs pas isolé, il apparaît que le passeport européen devant être prochainement mis en place devrait recourir, lui aussi, à la technologie RFID. Ce dernier prévoit l'utilisation d'une puce contenant certaines données biométriques[54] (notamment une photographie, des empreintes digitales, celle de la rétine), certaines informations semblent indiquer qu'il s'agirait plus précisément un passeport sans contact (RFID)[55]. Cela poserait d'ailleurs des questions annexes comme celle de la possibilité de contrôle de l'identité des individus à tout moment et sans justification de la part des forces de l'ordre.

Parallèlement des solutions d'identification à l'aide de tags directement implantés dans le corps humain sont à l'étude[56], ainsi la société *Applied Digital Solutions* a créé un tag RFID dénommé « VeriChip » destiné aux êtres humains. Long de seulement 11 mm, il a été construit pour être implanté sous la peau. Il est vendu comme une solution permettant de tracer les enfants ou encore les personnes atteintes de la maladie d'Alzheimer mais plus généralement toute personne ayant un handicap.

Devant la multiplication du nombre d'applications faisant appel à la technologie RFID il pourrait être à craindre que ce système dont la fonction première est de simplifier la vie quotidienne des individus ne soit en quelque sorte détourné à des fins de traçabilité des personnes. Cela reste d'autant plus vrai que, dans le climat qui règne depuis les attentats du 11 septembre et plus encore suite à ceux du 11 mars à Madrid[57], le besoin de moyens permettant la lutte contre le terrorisme, de la part des différents gouvernements de la planète, c'est grandement accru[58]. Dans ce sens un mémo de la Commission Européenne en date du 18 mars

---

[52] Zdnet, Treize collectivités vont tester des "cartes de vie quotidienne", article disponible à l'adresse suivante : http://www.zdnet.fr/actualites/internet/imprimer.htm?AT=2137370-39020774t-39000762c

[53] L'Agence pour le Développement de l'Administration Electronique (ADAE) semble s'être préoccupée de ce point, elle a d'ailleurs consulté la CNIL sur les principes à respecter dans le cadre de l'implémentation des cartes de vie quotidienne. Voir sur ce point ZDnet, La Cnil rappelle les principes de base à respecter pour les "cartes de vie quotidienne", article disponible à l'adresse suivante : http://www.zdnet.fr/actualites/internet/0,39020774,39144949,00.htm

[54] On notera tout de même que l'intégration de données biométriques dans le tag aurait pour effet de soumettre le traitement envisagé au régime d'autorisation (autorisation du traitement par la CNIL prévue aux articles 25 (secteur privé) 26 et 27 (secteur public)).

[55] Voir par exemple un article à l'adresse suivante : http://www.contactless-technology.net/E3-EUProjects.php , de même que les diverses communications de la Commission Européenne et propositions de règlement. Sur ces points voir notamment : http://europa.eu.int/eur-lex/fr/com/pdf/2004/com2004_0116fr01.pdf et http://europa.eu.int/eur-lex/en/com/pdf/2003/com2003_0558en01.pdf

[56] La solution n'est d'ailleurs pas véritablement nouvelle, elle est déjà largement utilisée pour « tatouer » les animaux.

[57] Le risque d'empiètement sur la vie privée suite aux différents attentats perpétrés depuis 2001 a d'ailleurs été relevé dans le rapport final « *The Opportunities Ahead* » de l'IST qui s'est tenue à Milan du 2 au 4 octobre 2003, le rapport évoque *« un risque spécial que les conséquences du 11 septembre puissent conduire, de manière inconsidérée, à ne pas se poser les justes et bonnes questions » ;* (traduction libre, texte original : *« There was a special danger that the aftermath of September 11th might unnecessarily suppress the asking of fair and right questions »)*. Texte disponible à l'adresse suivante : http://europa.eu.int/information_society/istevent/2003/cf/vieweventdetail.cfm?ses_id=109&eventType=session

[58] Voir sur ce point une étude approfondie (et notamment au regard de la technologie RFID) sur les risques d'atteinte à la vie privée suite aux attentats du 11 septembre : Rapport de l'Institute for prospective Technological studies, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview, Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs* (LIBE).

2004 incite au déploiement de la technologie RFID en vue de tracer les matières ou objets sensibles par satellite[59] (grâce au système Galileo mis en place par l'Europe)[60].

Il est certain que l'utilisation de données identifiantes dans les RFIDs représente un risque important d'atteinte à la vie privée en permettant d'identifier un individu à distance à partir d'informations uniques propres à leur porteur. Cependant d'autres applications utilisant les radio-tags dans des biens de consommation courante pourraient avoir pour conséquence de permettre de rendre identifiable les individus.

B- Les RFIDs en tant que données rendant une personne identifiable.

L'implémentation des RFIDs dans les produits de consommation courante pourrait permettre de rendre une personne identifiable en autorisant un « profilage » des individus. Cela s'explique par le fonctionnement même des tags, en effet ceux-ci ont été standardisés[61] notamment quant à leur contenu. Cette standardisation qui tend à créer un code normalisé pour tous les objets manufacturés est rendue possible grâce à l'Electronic Product Code (EPC), celle-ci est promue au plan international par une organisation dénommée EPCglobal[62]. Le but de l'Electronic Product Code est de fournir, pour chaque bien manufacturé, un numéro d'identification unique. Ainsi comme le note la CNIL, *« le passage de la codification à 12/13 chiffres à une codification plus riche est un moyen de mondialiser les codes (intégration UCC/EAN) dans un contexte d'enrichissement de l'information. Un identifiant ePC (electronic Product Code) à 96 bits permet par exemple de rajouter un numéro de série à l'actuel EAN-13: Fonctions Header (2) ePC Manager (7) Object Class (6) Serial Number (9)*

---

[59] Ce qui emmène à s'interroger sur les réelles possibilités techniques offertes par les RFIDs, ainsi Matt Reynolds, ingénieur spécialisé dans la conception de RFID chez ThingMagic affirmait *« tant pour des raisons légales (limitation de la puissance des émetteurs par le gouvernement) que des raisons physiques (liées à la propagation des ondes), les RFIDs ne pourront jamais émettre à une distance de plus de 20 mètres (…) il sera très difficile d'augmenter cette distance sans accroître considérablement la taille des puces ».* On ne peut que constater le décalage entre ses propos et les projets de la Commission Européenne.

[60] *« Afin de pouvoir détecter d'éventuels matériaux dangereux, la note recommande de «se servir au maximum des technologies avancées comme le suivi par RFID et satellite», couplant les puces à radiofréquences avec le futur réseau européen de géonavigation Galileo »* ZDnet, Surveillance électronique: les Quinze se mobilisent après les attentats de Madrid, article disponible à l'adresse suivante : http://www.zdnet.fr/actualites/technologie/imprimer.htm?AT=39146751-39020809t-39000761c.
Textes émanant des institutions européennes sur le sujet: MEMO /04/66, Brussels, 18 March, *European Commission action paper in response to the terrorist attacks on Madrid* du Conseil de l'Union Européenne dont on retiendra la phrase suivante: *« We need to urgently review whether we have adequate measures in place to allow us to monitor and trace bomb-making materials such as explosives, detonators, and radioactive sources as well as precursors. Detection and traceability should become our key words here. The tracing and checking of dangerous goods and explosives should be made possible by creating new databases or upgrading existing databases such as SIS II with new functionalities, as well as making full use of advanced technologies such as satellite enhanced (GALILEO) RFID (Radio Frequency Identification Device) tracking».* http://europa.eu.int/comm/external_relations/news/ip04_65.htm, et Projet de déclaration sur la lutte contre le terrorisme du 22 mars 2004. Texte disponible en version française à l'adresse suivante: http://www.edri.org/docs/ST07486-RE03.FR04.pdf

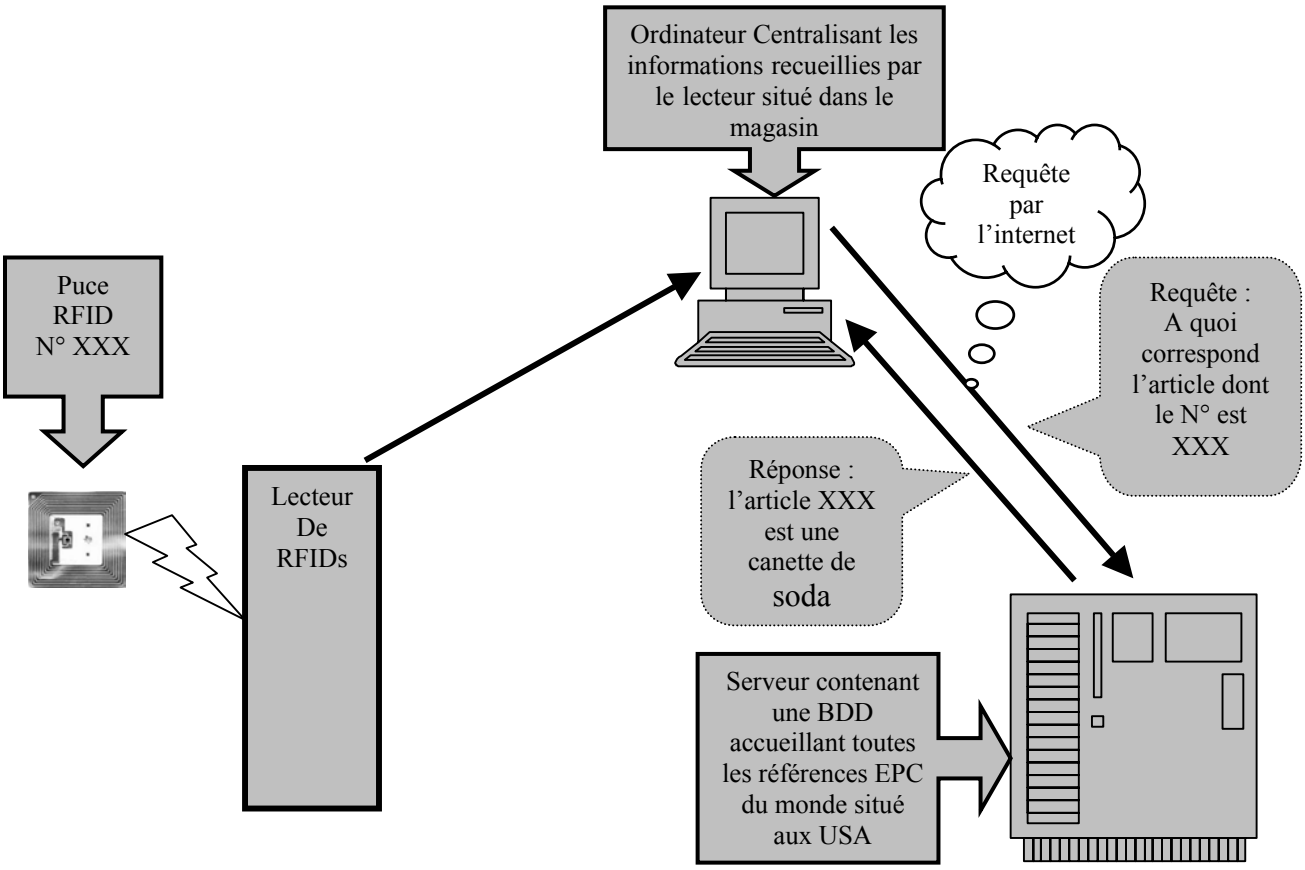
[61] Sur le plan technique les normes ISO 18000 et suivantes standardisent les fréquences utilisables. Le contenu du tag fait lui aussi l'objet d'une standardisation dénommée Electronic Product Code (EPC).

[62] EPCglobal, qui agit en étroite collaboration avec l'Auto-ID Center (devenu Auto-ID Labs) qui est lui-même une émanation du célèbre Massachusetts Institute of Technology (MIT), est une joint venture entre EAN International et l'Uniform Code Council (UCC). Le site d'EPCglobal se trouve à l'adresse suivante: http://www.epcglobalinc.org/index.html

Bits 0 à 7 | 8 à 35 | 36 à 59 | 60 à 95

Exemple : nationalité entreprise type de produit numéro du produit Dans cet exemple, si le type de produit est « cannette de soda light », chaque canette est identifiée par un numéro la différenciant des autres canettes du même type. Le passage à des codes ePC permet en effet d'identifier les objets industriels au niveau élémentaire »[63].

Plus concrètement l'utilisation de l'EPC permet d'identifier individuellement une canette de soda d'une autre canette de la même marque et du même produit, chacune d'elle disposant d'un numéro unique différent de celui de ses autres consoeurs. Selon les termes de l'EPCglobal : *« le réseau EPC est un système global pour l'indentification immédiate et automatique de tout objet dans la chaîne de production de toute société, dans toute industrie, dans le monde entier »*[64]. On peut schématiser, sommairement, ainsi le fonctionnement d'une identification par RFID :



[63] CNIL, Séance du 30 octobre 2003, Communication de M. Philippe Lemoine relative à la Radio-Identification (Radio-Tags ou RFIds), p. 4. Philippe Lemoine, auteur de cette communication relative aux RFIDs, est commissaire à la CNIL et membre du directoire des Galeries Lafayettes

[64] Traduction libre, texte original: *« the EPC network [is] a new global standard for immediate, automatic identification of any item in the supply chain of any company, in any industry, in the world».*

Ce système étant standardisé, il prévu pour être interopérable entre tous les lecteurs, c'est-à-dire que le tag apposé par un fabriquant pour une chaîne de supermarchés X pourra aussi être lu par les lecteurs de la société Y. En pratique le système fonctionne comme une sorte d'« internet des objets »[65], chaque produit ayant une référence l'identifiant (semblable à l'adresse IP qui identifie un ordinateur sur l'internet), ce numéro est lu par le lecteur et transmis à un ordinateur[66] qui va interroger la base de données contenant les références EPC pour identifier l'objet[67].

La présence d'un identifiant unique sur chaque objet manufacturé pourrait conduire à considérer que ces données relèvent de la loi de 1978 en permettant l'identification, ou du moins le profilage, des individus. En effet est-il nécessaire de connaître l'identité d'une personne pour déjà intervenir dans la sphère de sa vie privée ? La simple lecture des tags portés par un consommateur à l'entrée d'un magasin (ceux de ses vêtements, des objets contenus dans son sac, ceux des achats qu'il vient d'effectuer dans un autre magasin,…) peut conduire à connaître ses habitudes de consommation, et peut servir à lui proposer des promotions sur mesure. De même, sans connaître le nom d'une personne celle-ci peut être identifiée grâce aux objets qui l'entourent. Il serait alors possible de savoir que quelqu'un ayant sur lui le manteau dont le numéro est XXXX était dans le secteur où un larcin a été commis, il suffira de rechercher le manteau (ou une combinaison d'objets si l'on veut une preuve plus sûre) qui répond à cet identifiant pour retrouver le suspect.

Il paraît probable que les entreprises seront tentées d'utiliser les données contenues dans les tags pour profiler leur clientèle, car comme le note la CNIL *« la gestion du risque sous les formes diverses de « capitalisation de l'information », de « segmentation », de « géomarketing », d' « hyperciblage » est devenue aujourd'hui impérative pour les entreprises, en quête d'optimisation de l'usage de l'information collectée et de production d'informations nouvelles. L'apport incontestable des NTIC dans la gestion de la relation client porte sur les possibilités d'interconnexion, d'automatisation de processus de traçabilité et d'optimisation des tâches, et enfin le partage de l'information »*[68]. Il semble que la technologie RFID n'échappe pas à cette volonté « marketing » de réutilisation et de croisement de l'information concernant les clients par les sociétés commerciales afin de créer des profils sans cesse plus précis de leur clientèle. Ainsi peut on lire dans la plaquette d'un fabriquant de tags vantant les mérites de l'utilisation de la technologie RFID : «*Vous offrez un meilleur service à vos clients et obtenez d'avantage d'informations sur eux. Sans manipulation, le périmètre RFID permet de détecter les cartes de fidélité de vos clients lorsqu'ils entrent dans le magasin : vous pouvez mieux personnaliser le service que vous leur offrez tout en acquérant des renseignements démographiques sur votre clientèle »*[69].

Les risques en matière d'atteinte à la vie privée sont donc ici bien présents, et ce d'autant plus que l'utilisation des RFIDs est amenée à ce généraliser. Nombre de grandes enseignes de la distribution prévoient d'imposer à leurs fournisseurs l'apposition de tags dans leurs produits

---

[65] Voir sur ce point: Traçabilité: Data Collection, ePC vise la création d'un "internet des objets", disponible à l'adresse suivante : http://dc.editricetemi.com/fr/

[66] Il est intrigant de constater que la machine chargée de gérer l'identification des objets s'est vue affubler du nom de SAVANT, cette dénomination est peu engageante et n'est d'ailleurs pas sans rappeler l'univers orwellien.

[67] La similarité au plan technique avec l'internet va plus loin, en détail, le code lu par le lecteur est traduit en une adresse internet par un système dénommé *Object Name Service* (proche des DNS de l'internet) pour interroger la base de données. Pour de plus amples détails voir notamment : *David Brock's White Paper on EPC* disponible à l'adresse suivante : http://www.autoidcenter.org/research/MIT-AUTOID-WH-011.pdf, mais aussi http://www.e-centre.org.uk/home.asp et enfin *EPC: The End of Bar Codes?* Disponible sur le site de l'AIM à l'adresse suivante : http://www.aimglobal.org/technologies/rfid/resources/articles/June03/EPCpart1.htm.

[68] CNIL, Rapport sur les listes noires, p. 7.

[69] Check point, http://fr.checkpointsystems.com/rfid/retail2.asp

(cas de Wall Mart[70], Metro[71] mais aussi le Département de la Défense des Etats Unis[72]), alors que certains fabricants ont pris d'emblé l'initiative de tagger leurs produits (Prada, Gillette[73], Michelin,…)
Au-delà des opérateurs privés, les projets visant à introduire des puces RFID dans les objets de la vie quotidienne, sont aussi issus de l'initiative publique. Ainsi le bien le plus courant est visé au premier plan, la Banque Centrale Européenne (BCE) a planifié d'implanter dans un avenir très proche des tags dans les billets de banques[74].
Dans un avenir proche les individus seront peut être « trahis » par les objets qu'ils portent sur eux. La technologie le permet déjà au travers des applications RFID, d'autant plus que l'utilisation annoncée des tags est amenée à évoluer, la prochaine étape se dénomme *« Near Field Communication »* (NFC). Celle-ci permet à des objets dotés de puces sans contact de communiquer entre eux[75]. Le projet est supporté notamment par le constructeur Philips, il permettrait par exemple de commander un produit en approchant un téléphone portable ou une carte bleue (dotés d'un tag) d'une affiche publicitaire (elle aussi équipée d'une puce)[76].
On voit que ces nouvelles possibilités risquent de conduire à un profilage pointu des habitudes des consommateurs, et ce d'autant plus que certains tags autorisent une écriture, il serait alors possible que le RFID d'un téléphone portable enregistre les opérations faites par son propriétaire, informations qui pourraient ensuite être récupérées pour retracer les habitudes de consommation (ou pourquoi pas les trajets d'un individu).

Selon leur contenu, les RFIDs peuvent donc conduire à identifier directement une personne ou du moins la rendre identifiable par une sorte de profilage. Ce point fut d'ailleurs noté lors de la 25ème conférence internationale des commissaires à la protection des données et à la vie privée, le rapport final relève que *« les étiquettes de radio-identification sont d'abord utilisées à des fins d'identification et de gestion des objets (produits) pour contrôler la chaîne d'approvisionnements ou bien pour protéger l'authenticité de la marque du produit ; cependant elles peuvent être reliées à des données personnelles telles qu'un numéro de carte de crédit, et même utilisées pour collecter de telles informations, ou bien pour localiser et "profiler" les individus possédant des objets équipés d'étiquettes RFID. Cette technologie*

---

[70] RFID journal, *Wal-Mart Details RFID Requirement* , http://www.rfidjournal.com/article/articleprint/642/-1/1/
[71] ZDnet, RFID: le groupe Metro contraint de réduire ses ambitions, disponible à l'adresse suivante : http://www.zdnet.fr/actualites/technologie/imprimer.htm?AT=39143686-39020809t-39000761c
[72] Sur ce point voir sur le site du Department of Defense, *DoD Discusses New Supply Tracking System With Vendors*, article disponible à l'adresse suivante : http://www.defenselink.mil/news/Apr2004/n04072004_200404073.html
[73] Voir article sur le site Droit nouvelles technologies, Gillette incorpore un identifiant unique dans ses rasoirs : rasez-vous, vous êtes fliqué ! http://www.droit-technologie.org/1_2_1.asp?actu_id=817
[74] *« Une étude est en cours sur la sécurisation des billets d'euros à la Banque centrale européenne pour mise en oeuvre en 2005. Il s'agirait d'une autre famille de µ-puce (surface de 0.4 x 0.4 mm) avec une portée de lecture annoncée de l'ordre du millimètre ».* CNIL, Communication de M. Philippe Lemoine relative à la Radio-identification (Radio-Tags ou RFIds), p. 5.
[75] D'autres projets visent à créer des environnements intelligents notamment afin de surveiller les personnes âgées. Voir sur ce point un article : *RFID chips watch Grandma brush teeth*, disponible à l'adresse suivante : http://www.newscientist.com/news/print.jsp?id=ns99994788
[76] Voir le site internet de Philips, *Philips to Enable Consumers with Easy Access to the Digital World et Philips Accelerates Realization of Connected Planet Vision with Near Field Communication (NFC) Technology*, aux adresses suivantes : http://www.newscenter.philips.com/InformationCenter/NewsCenter/FPressRelease.asp?lArticleId=3256&lNodeId=13', 550,450 et http://www.newscenter.philips.com/InformationCenter/NewsCenter/FPressRelease.asp?lArticleId=3254&lNodeId=13', 550,450

pourrait permettre le traçage des individus et le recoupement des informations avec des bases de données existantes. (…). La technologie RFID a de nombreuses implications en matière de vie privée. Cela paraît évident dans le cas de microétiquettes implantées. Mais dans les situations plus fréquentes où les objets et les biens sont équipés d'étiquettes, les informations transmises font référence aux personnes portant ou transportant (ou même associées à) un produit équipé de la technologie RFID ou bien une "constellation" de marques révélant les goûts des individus. Par conséquent des données personnelles peuvent être traitées et transmises ou lues grâce aux RFID ou du moins de telles informations relatives aux objets peuvent aisément être reliées à des informations nominatives (ex : lorsqu'on utilise une carte de crédit pour acheter un produit équipé d'une étiquette RFID). Les étiquettes RFID peuvent potentiellement servir au traçage des mouvements des personnes qui les possèdent »[77].

Il est vrai que l'on peut se « rassurer » en pensant que la radio-identification ne touche que des objets et qu'il peut apparaître démesuré de considérer que « l*a radio-identification concerne la protection des données personnelles et de la vie privée.*

Quatre pièges peuvent masquer l'importance cruciale des enjeux « Informatique et Libertés » de cette technologie.

Le piège lié à l'« insignifiance des données » : quelle importance d'avoir le numéro de série d'une boîte de corn-flakes ? Mais le problème ce sont les volumes d'informations (des milliers d'objets suivis) que l'on peut, grâce à un maillage très dense, croiser dans des « ambiances intelligentes » ou analyser à travers des « scanners » (profiling radio de tous les tags d'une personne).

Le piège de la « priorité donnée aux objets » : s'agit-il vraiment de données personnelles ? Le fait que les applications relatives aux personnes (paiement, géo-localisation, etc…) aient un horizon plus éloigné répond à une logique économique : il n'y a que 6 milliards d'êtres humains contre 50 000 milliards d'objets. Mais ceci contribue à assoupir la vigilance.

Le piège d'une « logique de mondialisation » : les sponsors et les centres de recherche principaux sont aux Etats-Unis. C'est là-bas, hors de la tradition européenne « Informatique et Libertés », que se définissent les standards. Compte tenu des enjeux économiques colossaux de réorganisation des process opérationnels, les standards définis aux Etats-Unis s'étendront au monde entier.

Le piège de la « non-vigilance individuelle » : avec les RFIDs les données sont saisies à distance (sans « geste » particulier du porteur) et sans possibilité de stopper la communication (comme un GSM à l'état de veille). On est toujours activable. De surcroît, comme il n'y a pas de batterie, le rayonnement potentiel d'un RFID est illimité dans le temps »[78].

Il ressort de tout ceci qu'il convient bien de traiter les RFIDs comme des données personnelles, et à ce titre de les soumettre aux dispositions de loi de 1978. Cependant il convient d'analyser comment les principes posés par la loi informatique et libertés sont susceptibles de répondre aux atteintes à la vie privée causées par l'utilisation des RFIDs.

---

[77] 25ème Conférence Internationale des Commissaires à la protection des données et à la vie privée Sydney, 12 septembre 2003, Résolution sur la radio-identification, Version finale 20 novembre 2003.

[78] CNIL, Communication de M. Philippe Lemoine relative à la Radio-identification (Radio-Tags ou RFIds), Précitée, p. 7 et 8.

II- Appréhension des RFIDs par la loi du 6 janvier 1978

A titre préliminaire il convient de rappeler que, comme tout traitement de données à caractère personnel, les traitements relatifs aux RFIDs (principalement en ce qui concerne la collecte des informations contenues dans les puces en vue de la constitution d'un fichier) doivent faire l'objet d'une déclaration ou autorisation de la CNIL en vertu des articles 22 et 25 de la loi du 6 janvier 1978[79]. La loi ne distingue plus selon que le fichier nominatif est constitué au profit d'une personne privée ou d'une personne publique[80].

Au-delà de l'obligation de déclaration ou de demande d'autorisation, la loi informatique et libertés instaure un mécanisme de protection des personnes physiques en leur permettant d'exercer certains droits lorsque des données personnelles les concernant sont traitées, alors

---

[79] Article 22 :

I- A l'exception de ceux qui relèvent des dispositions prévues aux articles 25, 26 et 27 ou qui sont visés au deuxième alinéa de l'article 36, les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés.

II. - Toutefois, ne sont soumis à aucune des formalités préalables prévues au présent chapitre :

1° Les traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné exclusivement à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;

2° Les traitements mentionnés au 3° du II de l'article 8.

III. - Les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux articles 23 et 24, sauf lorsqu'un transfert de données à caractère personnel à destination d'un État non membre de la Communauté européenne est envisagé.

Article 25 :

I. - Sont mis en oeuvre après autorisation de la Commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont mentionnés aux articles 26 et 27 :

1° Les traitements, automatisés ou non, mentionnés au 7° du II, au III et au IV de l'article 8 ;

2° Les traitements automatisés portant sur des données génétiques, à l'exception de ceux d'entre eux qui sont mis en oeuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements ;

3° Les traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux qui sont mis en oeuvre par des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées ;

4° Les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire ;

5° Les traitements automatisés ayant pour objet :

- *l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ;*
- *l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes.*

6° Les traitements portant sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques et ceux qui requièrent une consultation de ce répertoire sans inclure le numéro d'inscription à celui-ci des personnes ;

7° Les traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes ;

8° Les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

[80] Cette distinction, devenue « obsolète » fut abandonnée dans lors de la refonte de la loi de 1978 au profit d'une nouvelle qui établie une discrimination entre traitement de données sensibles ou non. En effet les évolutions de mœurs ont montré que les fichages les plus dangereux n'étaient pas forcément le fait des acteurs publics. Voir sur ce point les articles 23 et 24 de la loi de 1978 modifiée par la loi du 6 août 2004 (déclaration) et 25 et s (autorisation).

qu'en parallèle le même texte impose certaines obligations aux responsables mettant en œuvre des fichiers nominatifs.
Au titre des obligations on retiendra : l'obligation de loyauté et d'information, de sécurité et le principe de finalité (A) ; alors que les droits pouvant être exercés par les individus fichés comprennent : le droit d'accès, de rectification et d'opposition (B).

A- Les obligations imposées par la loi de 1978 aux responsables de traitements nominatifs appliquées aux RFIDs.

La loi de 1978, dans l'objectif de limiter le nombre et l'étendue des traitements de données nominatives, a instauré des principes et obligations constituant une limite à la possibilité de constituer des fichiers contenant des informations à caractère personnel. Le texte encadre dans un premier temps les modalités de la collecte des données nominatives en imposant une obligation de loyauté dans tout recueil d'informations personnelles.

1- L'obligation de loyauté et d'information confrontée aux RFIDs

Le principe général de loyauté est rappelé par l'article 6[81] qui énonce qu'un traitement ne peut porter que sur des données à caractère personnel qui «*sont collectées et traitées de manière loyale et licite*». Ce principe général imposant une obligation de loyauté dans la collecte recouvre en fait des réalités diverses. Ainsi il conviendra d'abord d'informer les individus de la collecte d'informations les concernant[82]. Ensuite certaines données dites *« sensibles »* nécessitent pour être traitées que soit recueilli l'accord exprès des intéressés (articles 8[83] L. 78).
Ce cadre juridique restrictif doit, à n'en point douter, être appliqué à la collecte des informations contenues dans les tags, ceux-ci ayant été qualifiés précédemment de données nominatives[84]. Il est bien évident qu'en l'état actuel il est peu probable que les puces soient

---

[81] Ce texte dispose d'ailleurs d'un pendant pénal, ainsi l'article 226-18 du code pénal prévoit que *« le fait de collecter des données par un moyen frauduleux, déloyal ou illicite, ou de procéder à un traitement d'informations nominatives concernant une personne physique malgré l'opposition de cette personne, lorsque cette opposition est fondée sur des raisons légitimes, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende »*.

[82] Article 32 L. 78 :
I. - La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant :
1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;
2° De la finalité poursuivie par le traitement auquel les données sont destinées ;
3° Du caractère obligatoire ou facultatif des réponses ;
4° Des conséquences éventuelles, à son égard, d'un défaut de réponse ;
5° Des destinataires ou catégories de destinataires des données ;
6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre ;
7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne.
Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°.

[83] L'article 8 qui énonce en fait une interdicition de traitement des données sensibles prévoit d'autres exceptions que le consentement (qui d'ailleurs ne peut être donné si la loi l'interdit) notamment : sauvegarde la vie humaine, défense d'un droit en justice,… Il faut noter que le texte dans son article 9 prohibe aussi le traitement d'informations relatives aux infractions (là encore sauf exceptions).

[84] Voir supra dans ce même chapitre :
I – Qualification des RFIDs en tant que données nominatives, p. 13.

susceptibles de contenir des données sensibles[85] ; plus intéressante est l'obligation d'information car en effet l'élément novateur des RFIDs repose sur leur caractère transparent[86]. La technologie sans contact alliée à la petitesse des tags ne permet pas à l'utilisateur d'avoir conscience qu'en permanence sont émises des données le concernant.
Nombreux ont été ceux (défenseurs des libertés individuelles) à plaider pour une labellisation des produits « taggés »[87]. L'idée peut paraître séduisante, mais elle n'est cependant pas exempte de toute critique. L'information ainsi fournie s'avère-t-elle suffisante ? Le consommateur peut-il, grâce à cette seule étiquette, être informé de l'existence et des enjeux en matière de vie privée induits par l'utilisation des RFIDs ? Sera-t-il alors conscient que la puce qui se trouve dans le manteau qu'il achète continuera pendant des années de transmettre des données le concernant ?
Il conviendrait pour le moins d'informer l'individu que les données contenues dans les tags qu'il porte vont être collectées (à l'entrée d'un magasin par exemple). La mention mériterait d'être apposée aussi sur les instruments de lecture (ce qui permettrait de connaître les moments où les informations sont traitées).
Il n'en demeure pas moins que la solution la plus respectueuse des droits des personnes serait une désactivation pure et simple des puces à la sortie des magasins[88], cependant étrangement la méthode ne recueille pas l'assentiment général[89].
Quoi qu'il en soit on perçoit mal comment l'obligation précise d'information imposée par l'article 32 (obligation d'indiquer si la collecte est facultative/obligatoire, conséquences du défaut de réponse, destinataires et existence d'un droit d'accès) pourrait être respectée par une simple étiquette. Cependant il faut noter que la CNIL s'est parfois montrée conciliante avec une information lacunaire (cas du système de vidéosurveillance mis en place par la RATP[90]).
Ce premier principe est complété par un second qui touche à la finalité des traitements.

2- Le principe de finalité à l'épreuve des RFIDs.

Ce principe n'est pas clairement institué par la loi, il est une obligation qui était implicitement induite par le texte et l'esprit même de la loi de 1978[91] avant sa modification par la loi du 6aout 2004. Selon la CNIL, *« le principe de finalité est l'un des pilier de la protection. Un traitement d'informations nominatives est créé pour atteindre un certain objectif. Son contenu*

---

[85] Même si les RFIDs peuvent permettre indirectement d'avoir connaissance de telles données. On peut par exemple penser au cas où une carte syndicale serait dotée d'un tag ou encore à une combinaison d'achat alimentaires pouvant faire ressortir la confession religieuse d'un individu.
[86] Ce caractère a d'ailleurs valu aux RFIDs le sobriquet de *« peRFIDe »*.
[87] Il conviendrait alors d'apposer sur les biens de consommation une étiquette du type *« tag inside »* qui n'est pas sans rappeler le slogan d'un célèbre fondeur de microprocesseurs bien connu, reste à espérer que ce label ne soit pas l'objet d'une action en contrefaçon.
[88] Notons que cette possibilité figure dans le cahier des charges des RFIDs.
[89] Selon les propos d'Henry Holtzman, co-organisateur de l'atelier "Rfid Privacy Workshop", créé en novembre dernier et co-anime le blog du MIT consacré à la problématique du respect de la vie privée face aux RFIDs : *« Je ne suis pas très favorable aux procédés consistant à "tuer les tags". Il serait sans doute préférable de pouvoir les enlever. Cela éviterait d'avoir besoin de la technologie pour les tuer et de celle qui permettra de s'assurer qu'ils l'ont bien été. Un joli logo sur le tag lui-même permettrait de savoir ce qui doit être enlevé. Mais ce serait dommage que des gens tuent ou enlèvent des tags. Car ils ont un potentiel considérable dans la gestion du cycle de vie des produits ».*
[90] Voir, CNIL 13ème rapport d'activité, p. 45 et s, Délibération° 92-126 du 10 novembre 1992.
[91] Il convient ici de remarquer que le futur texte réformant la loi de 1978 fait, quant à lui, une plus large place au principe de finalité.

doit correspondre à cet objectif et ne pas servir à d'autres fins. Le choix des données que l'on décide d'enregistrer, la durée de leur conservation et les catégories de personnes qui peuvent en avoir communication doivent être déterminés en fonction de la finalité du traitement »[92].
La finalité est en quelque sorte le fait justificatif du traitement projeté, elle conditionne sa licéité. La CNIL porte une grande attention à la finalité déclarée, celle-ci en effet ne doit pas être trop approximative ou trop large[93]. Ainsi la finalité du traitement pourra justifier que tel type d'information soit recueilli pendant telle durée. La notion de finalité est désormais directement visée par le texte de la nouvelle loi informatique et libertés qui prévoit dans son article 6 qu'un traitement ne peut porter que sur des données à caractère personnel qui (…) « *sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités* ».
Appliquée à la technologie RFID le principe de finalité ne pose pas de problèmes particuliers. Si, comme les entreprises le font prévaloir, les tags sont utilisés afin d'optimiser la gestion de la chaîne de distribution, le traitement pourra facilement être admis. Il ne nécessiterait d'ailleurs pas de déclaration, informations contenues dans les tags apposés sur les objets ne pouvant pas encore être considérées comme des données personnelles. En effet n'ayant pas encore été acquis, ils ne peuvent être rattachés à un individu.
Cependant si, comme le supposent certaines associations de défense des libertés, l'implémentation des tags répond à un objectif de type *« marketing »* (profilage des consommateurs, promotions,…), il conviendra alors de ne pas négliger de déclarer cette finalité auprès de la CNIL[94].
Enfin, à titre de précision, il faut noter que les déclarations seront souscrites par ceux qui vont réaliser le traitement. Cette condition est indépendante du fait d'apposer des tags sur ses produits. On peut imaginer qu'un magasin n'utilisant pas de puces dans les biens qu'il commercialise ait acquis un lecteur pour connaître les clients qui entrent dans l'établissement. Il y a ici un traitement qui nécessitera déclaration.
Une autre obligation imposée par la loi de 1978 appelle plus de remarques, il s'agit de l'obligation de sécurité et de confidentialité.

3- *L'obligation de sécurité et de confidentialité.*

Cette obligation résulte de l'article 34[95] de loi de 1978 qui énonce que : « *le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment,*

---

[92] Voir le site de la CNIL à l'adresse suivante : http://www.cnil.fr/index.php?id=20&print=1.
[93] Voir CNIL, 2ème rapport d'activité, p. 80.
[94] Le détournement de finalité est d'ailleurs lourdement sanctionné par l'article 226-21 du code pénal : *« Le fait, par toute personne détentrice d'informations nominatives à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative ou l'acte réglementaire autorisant le traitement automatise, (Loi n° 95-116 du 4 février 1995, art. 34) "ou par la décision de la Commission nationale de l'informatique et des libertés autorisant un traitement automatisé ayant pour fin la recherche dans le domaine de la santé," ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».*
[95] Reprenant l'ancien article 29 de la loi de 1978 avant sa modification cependant le nouveau prévoit que « *des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2°* [sauvegarde de la vie humaine] *et au 6°* [médecine préventive] *du II de l'article 8* ».

empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès »[96].
Dans le cadre de l'utilisation des RFIDs il conviendra alors que le maître du fichier prenne les mesures adéquates afin de garantir la sécurité du traitement. Cela recouvre des dispositions permettant d'assurer la sécurité physique (limite des accès aux locaux) mais aussi logique (sécurité logicielle des serveurs).

Cependant, concernant l'emploi des RFIDs dans les produits de consommation, il convient de relever que l'utilisation de l'EPC (qui comme nous l'avons vu permet d'attribuer un numéro unique à chaque produit) repose sur des demandes d'identifications faites à un serveur qui n'est pas situé dans l'entreprise (il peut être à l'étranger[97]) par le biais de l'internet. La sécurité devra être assurée dès lors que les informations transmises seront nominatives[98]. Il faut donc se poser la question du moment où les informations acquièrent la qualification de données nominatives. Il est peu probable que la base de donnée contenant toutes les références EPC du monde soit constitutive d'un fichier nominatif étant donné que l'objet, tant qu'il n'a pas été acquis n'a pas, a priori, de lien avec un individu. Cependant il faut reconnaître que cette structure hautement décentralisée fait appel, pour identifier un objet et indirectement un individu, à une multiplicité d'acteurs. La sécurité du traitement doit-elle alors être envisagée globalement[99] (c'est à dire au niveau de chaque acteur indépendamment de la qualité des données transmises, même lorsque celles-ci ne peuvent pas encore être considérées comme nominatives). Alors que le principe de sécurité veut que l'obligation pèse sur le maître du fichier, c'est-à-dire la personne qui effectue le traitement ou l'a ordonné[100], faut-il dans le cas des tags imposer la sécurité plus largement à tous les acteurs de la chaîne (fabricant de puce, entreprise faisant usage des RFIDs, base de données EPC, sécurisation des échanges de données par l'internet,…).
Certains auteurs considèrent que l'obligation de sécurité repose non seulement sur le maître du fichier mais aussi sur les intermédiaires. Ainsi pourrait être recherchée la responsabilité de *« celui qui a procédé ou a fait procéder au traitement, (...) mais aussi du producteur, au sens le plus large, de bases de données, voire du serveur, en un mot de toute personne juridique qui est appelée a assurer à un titre ou à un autre la conservation d'informations nominatives »*[101].

---

[96] La sanction est prévue par l'article 226-17 du code pénal : *« Le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».*

[97] Il pourrait alors selon les cas s'agir d'un transfert de données nominatives vers l'étranger avec les implications que cela comporte (contractualisation du transfert avec le prestataire si celui-ci est situé hors Union Européenne,…).

[98] Et d'autant plus si ce transfert de données nominatives se fait vers l'étranger. Il faudra alors prévoir soit une adhésion au Safe Harbour soit insérer les clauses types dans les contrats. Il faut d'ailleurs noter que dans ce contexte le traitement sera alors sujet à autorisation de la CNIL conformément à l'article 25 de la loi de 1978.

[99] Ce soucis est d'ailleurs relevé dans le rapport *Security and Privacy for the citizen in the Post September 11 Digital Age*: A Prospective Overview, élaboré dans le cadre de l'Union Européenne, précité, p. 50: « *The potential therefore exists for a hacker with enough resources to gain unauthorised access to this database and thereby remote access to the tags in order to check, modify or even erase the information contained therein ».* Traduction libre : *« la possibilité existe pour qu'un pirate disposant des ressources nécessaires puisse obtenir un accès non autorisé à la base de données et de là un accès à distance aux tags dans le but de lire, modifier ou même effacer les informations qu'ils contiennent ».*

[100] En ce sens voir : TGI Paris, 17ème ch. Corr, 16 décembre 1997, à propos d'agents EDF ayant transmis des informations figurant dans un fichier nominatif, responsabilité d'EDF et non des agents.

[101] Lamy, droit de l'informatique et des réseaux, ed 2003, n° 559.

Il faut noter en dernier lieu que, certains tags étant réinscriptibles, la sécurité devrait être assurée dans ce cas avec encore plus de vigilance. L'inscription de données nominatives (par exemple pour confirmer qu'un produit a été légitimement acquis : nom de l'acheteur, date d'acquisition, lieu, références de la transaction bancaire ayant permis l'achat, …) devrait être considérée comme la constitution d'un fichier nominatif décentralisé, par la même automatiquement soumis aux prescriptions de la loi de 1978[102].

Les différentes obligations imposées aux personnes réalisant un traitement de données à caractère personnel pourraient permettre d'encadrer l'utilisation des RFIDs en garantissant le respect de la vie privée des personnes, et ce d'autant plus que ces obligations pour les responsables des traitements sont doublées par des droits accordés aux individus.

B- RFIDs et droits accordés aux individus par la loi de 1978.

Les obligations pesant sur les responsables de fichiers constituent souvent un droit vu sous l'angle des individus, tel est le cas de l'obligation d'information qui a pour pendant un droit à l'information, ou encore le droit à l'oubli[103] qui correspond au temps maximum de traitement et de conservation des données à caractère personnel et qui sera conditionné par la finalité du traitement.
Cependant le texte de 1978 prévoit indépendamment des droits distincts pour les « victimes » de fichage. On citera principalement le droit d'opposition ainsi que les droits d'accès et de rectification.

1- Le droit d'accès et de rectification mis en perspective avec les RFIDs

Les droits d'accès et de rectification sont étroitement liés, le second étant rendu possible uniquement par l'exercice du premier (il faut pouvoir connaître le contenu des informations traitées pour pouvoir ensuite les corriger si elles s'avèrent inexactes).
Ainsi le droit d'accès permet à toute personne[104], justifiant de son identité, d'interroger le responsable de fichier afin de savoir si des informations à caractère personnel la concernant

---

[102] Il serait similaire aux fameux « cookies » que l'on rencontre sur l'internet.

[103] Prévu par l'article 36 L. 78-17 : *«les données à caractère personnel ne peuvent être conservées au-delà de la durée prévue au 5° de l'article 6 qu'en vue d'être traitées à des fins historiques, statistiques ou scientifiques ; le choix des données ainsi conservées est opéré dans les conditions prévues à l'article L. 212-4 du code du patrimoine.*
Les traitements dont la finalité se limite à assurer la conservation à long terme de documents d'archives dans le cadre du livre II du même code sont dispensés des formalités préalables à la mise en oeuvre des traitements prévues au chapitre IV de la présente loi.
Il peut être procédé à un traitement ayant des finalités autres que celles mentionnées au premier alinéa :
- *soit avec l'accord exprès de la personne concernée ;*
- *soit avec l'autorisation de la Commission nationale de l'informatique et des libertés ;*
- *soit dans les conditions prévues au 8° du II et au IV de l'article 8 s'agissant de données mentionnées au I de ce même article».*

[104] On notera que l'exercice du droit d'accès est parfois difficile à réaliser en pratique, les personnes désireuses d'utiliser leur droit d'accès sont parfois confrontées à de nombreux obstacles pratiques. Sur ce point voir l'article de Me Valérie Sédallian : « La loi Informatique et Libertés vue par la "France d'en bas" ou le récit de Candide au pays des merveilles » disponible à l'adresse suivante : http://juriscom.net/pro/visu.php?ID=79

sont traitées[105]. Selon les cas ce droit sera exercé directement ou indirectement (par le biais d'un intermédiaire (la CNIL) lorsque le traitement concerne des informations relevant notamment de la sécurité publique[106]).
Il faut noter que l'exercice de ce droit n'est pas totalement gratuit. En effet si la personne désire obtenir une copie des informations traitées la concernant, celle-ci devra acquitter une redevance dont le montant a été fixé par un arrêté du 23 septembre 1980 (ce montant est établi à 3 € pour les demandes se rapportant à l'un des traitements prévus à l'article 15 de la loi (traitement privé) et 4,60 € pour les demandes se rapportant à l'un des traitements prévus par l'article 16 de la loi qui concerne les traitements publiques).
Devant la multiplication des traitements que risque de susciter l'emploi des RFIDs, il est possible que se démultiplient d'autant les demandes d'accès. *« Dans ce contexte compte tenu des volumes en cause, une révision des règles d'exercice du droit d'accès et de rectification devrait par ailleurs être menée (faudra t-il payer pour exercer ce droit ?) »*[107]. Cette proposition de réforme du droit d'accès formulée par la CNIL semble quelque peu injustifiée[108], il ne paraît pas juste de devoir limiter un droit pourtant reconnu par la loi au motif que les industriels ont décidé de recourir massivement à des technologies de traçabilité.
Cette position n'est pas conforme aux vœux du législateur tel qu'ils ressortent de la loi 2004-801 du 6 août 2004 modifiant la loi de 1978, en effet celle-ci prend désormais soin de préciser que *« le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction »*[109].
Cependant il est certain que le droit d'accès exercé massivement pourrait devenir une entrave à l'utilisation de la technologie RFID. Ce droit pourrait être exercé auprès de toute entreprise

---

[105] Principe prévu par les articles 39 de la loi de 1978 : *«Article 39 : I. - Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir :*

1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;

2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ;

3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne ;

4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;

5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle.

Une copie des données à caractère personnel est délivrée à l'intéressé à sa demande. Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction.

En cas de risque de dissimulation ou de disparition des données à caractère personnel, le juge compétent peut ordonner, y compris en référé, toutes mesures de nature à éviter cette dissimulation ou cette disparition. II. - Le responsable du traitement peut s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique. En cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable auprès duquel elles sont adressées».

[106] Cas atypique prévu par l'article 41 de la loi de la loi de 1978.

[107] CNIL, Communication de M. Philippe Lemoine relative à la Radio-Identification (Radio-Tags ou RFIds), précité, p. 8.

[108] Il est vrai que celle-ci est posée comme une ultime solution, la préférence de la CNIL allant vers une désactivation pure et simple des tags.

[109] Article 39 de la loi 78-17 modifiée. Il faut d'ailleurs remarquer que la rédaction retenue est plus stricte que celle de l'acte originaire (directive 95-46) qui, pour sa part, retient l'expression *« sans frais excessifs »*.

utilisant les radio-tags car il est impossible de savoir *a priori* si l'entrée dans tel ou tel établissement déclenchera ou non le recueil des données contenues dans les puces que la personne porte sur elle. A ce stade, on peut même se demander si le droit d'accès de l'individu ne serait pas neutralisé[110] devant le nombre des traitements susceptibles d'être effectués.

Le corollaire du droit d'accès que constitue le droit de rectification pourrait voir son efficacité réduite d'autant. Celui-ci est organisé par l'article 40[111] de la loi de 1978 modifiée. Il permet au titulaire du droit d'accès de demander au responsable du traitement que les informations le concernant soient mises à jour ou corrigées[112]. On peut d'ailleurs s'interroger sur la qualité des données sur lesquelles pourrait s'exercer le droit de rectification, plus facilement envisageable dans le cas où le traitement touche des données identifiant la personne (ex du numéro de passeport), il est plus douteux dans le cadre d'un simple profilage (comment savoir sur quoi interroger le responsable, faudra-t-il lui donner les numéros des tags que nous portons pour voir s'ils sont traités dans ses propres fichiers ?).

Au delà de ce contrôle *ex post* la loi de 1978 organise la possibilité de s'opposer purement et simplement au traitement de données nominatives.

2- Un droit d'opposition au traitement des informations contenues dans les RFIDs ?

La loi informatique et libertés permet aux individus de s'opposer au traitement des données nominatives les concernant. Ce principe est contenu dans l'article 38 de la loi : *« Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement. Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection,*

---

[110] Une personne faisant ses courses devra-t-elle rentrer dans tous les magasins qu'elle a visité pour exercer son droit d'accès ? La tâche semble fastidieuse et pour le moins décourageante. De plus, si l'on s'en tient à une information sur les produits « taggés », comment savoir si un établissement a pu lire et traiter les informations qui sont contenus dans les RFIDs. Ce point vient confirmer le besoin d'une information sur les lecteurs de tags et non simplement sur les produits. Voir sur ce point supra p. 24.

[111] *« Article 40 : 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 la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.*
Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent.
En cas de contestation, la charge de la preuve incombe au responsable auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord.
Lorsqu'il obtient une modification de l'enregistrement, l'intéressé est en droit d'obtenir le remboursement des frais correspondant au coût de la copie mentionnée au I de l'article 39.
Si une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa.
Les héritiers d'une personne décédée justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence.
Lorsque les héritiers en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent ».

[112] Cette obligation est pénalement sanctionnée par le Décret 81-1142 du 23 décembre 1981 qui la sanctionne par une contravention de 5ème classe.

notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur. Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement » [113].

Le droit d'opposition est parfois centralisé biais de listes d'opposition (liste orange par le téléphone, liste safran pour les télécopies et télex et fichier d'opposition Robinson pour la VPC) ou encore généralisé au travers d'une présomption d'opposition (couramment dénommée OPT-IN).
En dehors de ces cas le droit d'opposition peut donc être exercé au cas par cas, ainsi selon la CNIL *« il existe différentes formes d'expression de ce droit d'opposition :*

- *le refus de répondre lors de la collecte non obligatoire de données ;*
- *la nécessité de donner son accord écrit pour le traitement de données sensibles telles que les opinions politiques ou les convictions religieuses* [nouvel article 8 de la loi] *;*
- *la faculté de demander la radiation des données contenues dans les fichiers commerciaux ou de vente par correspondance ;*
- *la possibilité d'exiger la non-cession ou la non-commercialisation des informations »*[114].

Notons que ce droit peut être exercé librement, il n'est soumis qu'à un contrôle des motifs (ceux-ci devant être légitimes sans plus de précisions ce qui introduit une appréciation nécessairement subjective). Cependant nombre de traitements imposés par l'Etat ne seront pas susceptibles de se voir opposer ce droit[115] (billet de banque, passeport,…). Cependant hormis ce cas il pourrait alors permettre à un individu de demander au maître du fichier que les informations personnelles le concernant ne soient plus traitées. A cela on peut objecter que les difficultés observées pour le droit d'accès et de rectification (difficulté de savoir qui a recueilli les données contenues dans les puces pour les traiter) pourrait conduire, ici aussi, à une neutralisation du droit d'opposition.

Il est certain que l'utilisation d'une technologie comme celle de la radio-identification impose de remettre en perspective la loi au regard des évolutions techniques. Dans le cadre des radio-tags la difficulté vient du caractère diffus (et polymorphique) des traitements constitués par *« la lecture à distance et l'activation des étiquettes RFID, sans aucune possibilité pour les personnes concernées d'intervenir dans le processus »*[116]. Tel est bien le véritable risque en matière de vie privée : l'hermétisme et la transparence (pour les individus) des processus en cause et de fait une quasi impossibilité de contrôle *a posteriori*.
Cependant il faut noter que jusqu'à présent la CNIL a toujours su faire évoluer la loi au gré des avancées technologiques, en adaptant un texte, pourtant vieux de 25 ans, aux fabuleux

---

[113] Ici une sanction est prévue par l'article 226-18 du code pénal : *« Le fait de collecter des données par un moyen frauduleux, déloyal ou illicite, ou de procéder à un traitement d'informations nominatives concernant une personne physique malgré l'opposition de cette personne, lorsque cette opposition est fondée sur des raisons légitimes, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».*

[114] Voir la rubrique « Vos droits » sur le site de la CNIL à l'adresse suivante : http://www.cnil.fr/index.php?id=21&print=1

[115] L'article 38 de la loi de 1978 modifiée précise même que le droit d'opposition n'existe pas dans ce cas le texte disposant que *« les dispositions du premier alinéa* [droit d'opposition] *ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement ».*

[116] Résolution sur la radio-identification, Version Finale, 20 Novembre 2003, adoptée lors de la 25ème Conférence Internationale des Commissaires à la protection des données et à la vie privée, Sydney, 12 septembre 2003, précité.

développements de l'outil informatique qui a fait passer notre société de l'aire du matériel à l'immatériel, d'une société papier à une société de l'information.

On le pressent, la solution pourrait résider dans l'adoption d'une législation sectorielle semblable aux dispositions instaurant la règle du consentement préalable en matière de prospection par voie électronique.

Chapitre II – Au-delà de la loi de 1978 , la protection des individus face aux RFID

Au-delà des grands principes énoncés par la loi du 6 janvier 1978 en matière de protection des données personnelles, est-il possible de trouver une solution permettant de concilier les besoins de l'industrie et le nécessaire respect des libertés individuelles ?
L'individu peut-il encore, dans nos sociétés où l'informatique est omniprésente, conserver une sphère d'intimité ? Sans aller jusqu'à plaider pour un droit absolu à l'anonymat[117], il semble qu'il faille s'interroger sur les désires de traçabilité grandissants développés tant par les acteurs privés que publics. La conciliation des impératifs de vie privée et des nécessités de l'industrie devra passer par la *« recherche d'un équilibre entre anonymat et " traçabilité " des personnes »*[118].
Les progrès de la technique permettent de nos jours d'assurer une traçabilité accrue des personnes. Il est tentant pour les entreprises ou même l'Etat de profiter de ces développements dans l'objectif d'accroître la sécurité aux dépens d'une sphère de liberté des individus de plus en plus atrophiée[119].
Les entreprises voient assurément dans l'utilisation des RFIDs un moyen leur permettant d'optimiser la gestion de leurs stocks mais aussi une possibilité de recueillir de précieuses informations sur leurs clients. En effet *« en vingt ans, l'information nominative a acquis une valeur marchande. Cet attrait s'est très tôt manifesté dans le domaine de la prospection commerciale. Une adresse peut révéler une situation économique et sociale, un prénom, un age ou un profil. En outre, les possibilités nouvelles de corrélations associées à l'outil statistique et au développement des logiciels de « fouille » (data mining) permettent de faire produire à une information de base, somme toute assez ordinaire, beaucoup plus de renseignements que l'on imaginerait »*[120].

Parallèlement les consommateurs sont parfois favorables à une technologie qui leur est présentée comme un progrès[121] permettant de faciliter leur vie quotidienne[122] mais parfois au détriment de leurs libertés[123].

---

[117] Le droit à l'anonymat est souvent invoqué sur l'internet comme étant une sorte de « liberté fondamentale » de l'internaute, cependant on peut douter que ce droit existe. Il suffit de faire état des récentes dispositions législatives adoptées en matière de cybercriminalité pour s'en persuader : convention cybercriminalité, loi sur la sécurité quotidienne, loi 2000-719… imposant la conservation de certaines données de connexions, voire même du contenu des pages visitées par les acteurs de l'internet (FAI et hébergeurs). Sur ce point voir Eric A. Caprioli, *Anonymat et commerce électronique*, article disponible à l'adresse suivante : http://www.caprioli-avocats.com

[118] Conseil d'Etat, Internet et les réseaux numériques, Les études du Conseil d'Etat, La Documentation Française, 2 juillet 1998, annexe I, p. 241. Le rapport du Conseil d'Etat fait d'ailleurs grande place dans ses développements à la dialectique anonymat/traçabilité sur les réseaux numériques. Ce souci est totalement transposable à la technologie RFID qui est faite pour fonctionner comme un « internet des objets ». Voir supra chapitre I p. 18.

[119] Dans ce sens le climat qui règne depuis les attentats du 11 septembre 2001, encore renforcé suite à ceux du 11 mars 2004, a fortement favorisé l'adoption de mesures restreignant les libertés dans un contexte de lutte contre le terrorisme. Sur ce point voir notamment le rapport *Security and Privacy for the citizen in the Post September 11 Digital Age: A Prospective Overview*, élaboré dans le cadre de l'Union Européenne, précité ou encore E. Wéry, l'internet sera-t-il le bouc émissaire des attentats du 11 septembre ? Les dangers au quotidien de la dérive sécuritaire. Expertises des systèmes d'information. n°257. mars 2002.

[120] M. Gentot, La protection des données personnelles à la croisée des chemins, In La protection de la vie privée dans la société d'information, tome 3, 4 et5, Précité, p. 26.

[121] Sur ce point il faut noter que l'action de « lobbying » menée par l'Auto-id center pour promouvoir une expansion de la technologie RFID tient une place importante. Cette forte pression a été mise au jour

Le phénomène n'est pas nouveau, il est déjà connu dans l'internet sous la forme des cookies censés faciliter la navigation mais permettant aussi de connaître les goûts et les habitudes des internautes.

Dans le cadre de l'utilisation de la radio-identification la conciliation entre le respect des libertés individuelles et les besoins des entreprises (gestion des stocks, lutte contre le vol,…) peut être réalisée au travers de diverses solutions (I), cependant les mesures envisageables pourraient être limitées en pratique, et notamment en raison des directives européennes (II).

I- Solutions pratiques et ébauche d'une réflexion juridique sur la régulation des RFIDS.

L'utilisation des radio tags étant amenée à se généraliser, il convient de se pencher sur les moyens envisageables afin d'aménager les besoins de l'industrie et la protection des données personnelles.
Les solutions possibles permettant de concilier vie privée et RFIDs sont multiples. Il s'agira d'abord de présenter les moyens disponibles en pratique (A) pour ensuite analyser les réponses possibles du droit aux implications de la radio identification en termes de vie privée (B).

A- Solutions pratiques envisageables afin de concilier RFIDs et vie privée.

La protection de la vie privée des individus commanderait bien évidemment que les tags soient désactivés à la sortie du magasin. La solution semble simple d'autant plus que les promoteurs de la technologie RFID ont pris soin, dans leurs spécifications techniques, de prévoir une fonction permettant la désactivation. Cette possibilité est donc rendue possible par le cahier des charges applicable à la radio identification par tag. Ainsi selon les propos même de l'Auto-Id center *« chaque puce doit intégrer une fonction permettant de « tuer » le tag (kill feature). Si les consommateurs se montrent inquiets, les tags peuvent être facilement détruits grâce à un simple lecteur peu coûteux*[124]*. La façon de cela sera fait, c'est à dire à la maison*

---

notamment au travers de documents confidentiels qui furent dévoilés sur l'internet en raison d'un défaut de sécurité sur les serveurs de l'Auto-id center. Le document le plus probant, qualifié de confidentiel et à diffusion limitée aux sponsors, montre comment rallier l'opinion publique à l'emploi des RFIDs en organisant un groupe, sous la coupe du centre, qui réunirait des personnes en charge de débattre des enjeux des RFIDs en terme de vie privée. Le document montre ensuite comment faire prévaloir les avantages que représente la technologie et comment convaincre les « décideurs » au plus hauts rangs des états. Il est intéressant de noter que le *RFID privacy workshop* mis en place compte à sa tête un ancien du MIT (fondateur de l'Auto-id center et de l'EPCglobal). Le document intitulé *« Managing External communications »* peut sans doute encore être trouvé sur le net mais, celui-ci changeant périodiquement d'adresse, il n'est pas possible d'indiquer ici un site permettant de le consulter.

[122] La technologie RFID permettrait ainsi par exemple de ne plus oublier ses clefs, un lecteur situé sur la personne (téléphone mobile) détectant que les clefs ne sont pas dans la poche. On peut aussi citer l'ouverture automatique du véhicule sans clef, les exemples sont nombreux et sont appelés à se développer dans un avenir proche.

[123] Comme le notait Thomas Jefferson : *« Si vous êtes prêts à sacrifier un peu de liberté pour vous sentir en sécurité vous ne méritez ni l'un ni l'autre »*. Transposée aux RFIDs cela reviendrait à admettre que le choix d'une vie « technologiquement confortable » ne pourrait conduire qu'à un traçage de l'activité des personnes et qu'il n'y aurait qu'une alternative : soit vivre en dehors de tout progrès technique, soit accepter les effets pervers de la technologie. Pourtant il reste à espérer, et c'est le but de cette étude, que les deux sont encore conciliables.

[124] On parle tout de même d'un prix approximatif de 120 euros !

[il appartiendrait alors au consommateur d'acheter un appareil afin de tuer les tag sur les produits qu'il vient d'acheter] *ou sur le point de vente reste à définir, et sera analysée dans la troisième étape des tests sur le terrain »*[125].

Il apparaît donc que la solution la plus facile et en même temps la plus protectrice pour les individus consiste dans une désactivation pure et simple des puces, cependant on notera que l'industrie ne paraît pas très encline à favoriser la désactivation des tags[126] sans doute pour des motifs liés à l'intérêt que représente, pour ces sociétés, la connaissance des habitudes de consommation de leurs clients[127]. Ainsi les entreprises militent contre les lois en cours d'examen aux Etats Unis imposant de tuer les tags, tel est le cas de Procter et Gamble. Ainsi *« P&G et d'autres compagnies ont suggéré la semaine dernière qu'elles voulaient que les tags restent actif après le passage en caisse plutôt que de les désactiver avec des soit disant machine à tuer les tags (kill machines) les compagnies veulent aussi faire correspondre l'identifiant unique des RFIDs (EPC) avec des données personnelles propres aux consommateurs »*[128]. A l'appui de cette plaidoirie en faveur de la non désactivation, certains acteurs du secteur de la distribution, afin de rallier l'opinion publique à leur cause dans un climat sécuritaire, ont pu soutenir que le « taggage » des produits alimentaires était un élément *« essentiel pour assurer la sécurité des stocks de nourriture américain face aux menaces terroristes »*[129].

---

[125] Traduction libre de l'anglais. Ces propos sont issus d'une réponse donnée par l'Auto-ID Lab par voie d'e-mail dont le texte en version originale était: *« Auto-ID labs designed a kill feature to be built into every (RFID) tag. If consumers are concerned, the tags can be easily destroyed with an inexpensive reader. How this will be executed i.e. in the home or at point of sale is still being defined, and will be tested in the third phase of the field test»*.

[126] Voir l'interview d'Henry Holtzman sur le site de la FING précitée. Pour rappel : *« Je ne suis pas très favorable aux procédés consistant à "tuer les tags". Il serait sans doute préférable de pouvoir les enlever. Cela éviterait d'avoir besoin de la technologie pour les tuer et de celle qui permettra de s'assurer qu'ils l'ont bien été. Un joli logo sur le tag lui-même permettrait de savoir ce qui doit être enlevé.*
Mais ce serait dommage que des gens tuent ou enlèvent des tags. Car ils ont un potentiel considérable dans la gestion du cycle de vie des produits ».
Dans le même ordre d'esprit on peut remarquer la noble intention de Metro qui proposait de mettre une machine permettant au client de désactiver lui-même les tags dans ses magasins. Cependant il est apparu que cet appareil ne désactivait pas les puces. Sur ce point voir CASPIAN, *Scandal: The "Undead Machine" RFID Tag Deactivation Station that does not Deactivate Tags*, à l'adresse suivante:
http://www.spychips.com/metro/scandal-deactivation.html

[127] On peut citer à titre d'illustration les propos tenus par John Stermer Vice Président d'eBusiness Market Development à ACNielsen : *«The next "big thing"? Frequent shopper cards. While these did a better job of linking consumers and their purchases, loyalty cards were severely limited by the constraint of a single retailer view. This skewed perspective gave retailers a view of in-store loyalty trends, but it only let them see the fraction of consumer spending at that format.*
In addition to the constricting chain and channel blinders of scanner data and loyalty cards, consider the usage, consumer demographic, psychographic and economic blind spots of tracking data. Consumer panel information was added to fill the gaps left by traditional tracking information, and has been a step in the right direction.
However, something more integrated and holistic was needed to provide a ubiquitous understanding of on- and off-line consumer purchase behavior, attitudes and product usage. The answer: RFID (radio frequency identification) technology.
The intelligent microwave and refrigerator loom as first order RFID applications--good news for CPG marketers, since 75% of the consumer products ACNielsen tracks can be found in the bathroom or kitchen. Where once we collected purchase information, now we can correlate multiple points of consumer product purchase with consumption specifics such as the how, when and who of product use».
John Stermer, Radio Frequency ID: A New Era for Marketers? CONSUMER INSIGHT MAGAZINE (Winter 2001), disponible à l'adresse suivante : http://acnielsen.com/pubs/ci/2001/q4/features/radio.htm

[128] Pour de plus amples détails, voir un article parut sur le site Wired, *Watchdogs Push for RFID Laws*, à l'adresse suivante : http://www.wired.com/news/print/0,1294,62922,00.html.

[129] Voir un article paru sur Wired news, *RFID will stop terrorists*, à l'adresse suivante :

La technologie offre aux entreprises de la grande distribution un outil marketing de tout premier ordre, on assiste donc à des démonstrations qui tentent de prouver au consommateur que le fait de ne pas profiter de cette technologie reviendrait à l'handicaper dans sa vie quotidienne[130] tout en omettant les risques inhérents à la radio identification en matière de vie privée. Cette réticence des industriels pourrait d'ailleurs être considérée comme une entrave au droit de propriété qui pourtant s'est vu reconnaître une valeur constitutionnelle, son caractère absolu étant proclamé par l'article 2 de la Déclaration des Droits de l'Homme et du Citoyen[131].

Cependant si le secteur industriel semble réticent à tuer les tags lors du passage en caisse, certaines initiatives issues de la société civile et de certaines associations, ont pour objet de permettre à tout un chacun de désactiver les tags incorporés dans les produits qu'il a acquis[132]. Ainsi un projet Allemand dénommé « dataprivatizer »[133] vise à mettre sur le marché un appareil permettant de détecter les lecteurs RFID. Il serait ainsi possible de savoir si les puces se trouvant sur les objets portés par un individu sont lues à l'entrée d'un magasin ou à toute autre occasion.

En France des initiatives similaires sont apparues, un logiciel distribué sous licence libre (GPL) permet de connaître le moment où les tags communiquent avec le lecteur mais aussi de modifier le contenu des données inscrites dans les puces, voire de les effacer purement et simplement[134].

Une autre solution envisageable est fournie par les sociétés commerciales, ainsi *« Obivision, une entreprise danoise, spécialiste de la cryptographie, a mis au point une solution logicielle pour inclure un mode "vie privée" dans les puces et les rendre inactives une fois que le consommateur a quitté le magasin »*[135].

---

http://www.wired.com/news/print/0,1294,59624,00.html

[130] Il est certain qu'il peut y avoir un avantage à se voir rappeler que l'on a oublié ses clefs avant de partir du bureau, ou de voir sa maison s'ouvrir sans que l'on ait à sortir ses clefs. Mais en contrepartie il serait sans doute désagréable pour un salarié de savoir que son patron peut connaître tous ses déplacements ou encore qu'un consommateur se voit harceler de publicités en raison de son profil commercial et de ses habitudes de consommation, dont la connaissance sera rendue aisément possible par l'emploi des RFIDs.

[131] Ce point sera plus amplement développé infra p.64.

[132] On notera qu'une solution simple et radicale consiste simplement à détruire la puce en passant le produit au four à micro-ondes. Cependant cette méthode n'est pas applicable à tous les produits (objets métalliques notamment) et présente un certain danger (principalement pour l'appareil électroménager).

[133] Zdnet, des solutions pour protéger le consommateur face aux « étiquettes intelligentes », disponible à l'adresse suivante : http://www.zdnet.fr/actualites/technologie/imprimer.htm?AT=39130624-39020809t-39000761c

[134] Ce logiciel, développé par Loïc Dachary, ingénieur à l'INRIA, est donc librement distribuable et modifiable. Il permet notamment grâce à un émetteur assez puissant de se promener dans un magasin tout en effaçant tous les tags dans son périmètre d'émission. Des opérations de « détaggage » massif sont prévues si la technologie venait à être utilisée de façon importante dans les enseignes de distribution. On peut cependant s'interroger sur la légalité d'un tel procédé, et ce d'autant plus que la tendance de notre législation pourrait venir protéger les puces contre toute modification. Sur ce point voir ZDnet, un logiciel libre pour limiter les risques « intrusifs » des puces électroniques RFID, disponible à l'adresse suivante : http://www.zdnet.fr/actualites/technologie/0,39020809,2137736,00.htm

[135] Zdnet, des solutions pour protéger le consommateur face aux « étiquettes intelligentes », précité, disponible à l'adresse suivante : http://www.zdnet.fr/actualites/technologie/0,39020809,39130624,00.htm

De son coté la firme RSA, bien connue pour ses produits en matière de cryptographie, propose une solution dénommée *« blocker tag »*[136]. Celle-ci consiste en un logiciel contenu dans un petit appareil, similaire à un tag radio qui empêche les lecteurs de communiquer avec les RFIDs situés à proximité du *blocker tag*.

Il existe donc des alternatives techniques afin de permettre la neutralisation des tags dans le cas où l'industrie déciderait de ne pas les désactiver lors du passage en caisse. Cependant il est certain que la solution la plus efficace serait que les enseignes établissent par elles-mêmes un politique générale de désactivation. Telle est d'ailleurs la position adoptée par les groupes de défense des libertés, relayés par la CNIL au travers de sa communication du 30 octobre 2004, dans laquelle celle-ci estime qu'il faudrait *« imposer la mise en place de mécanismes de désactivation des « smart tags » dans certaines situations et avec le libre choix des personnes »*[137].

Il faut cependant noter qu'énoncer un principe fort de désactivation ne serait pas forcément suivi d'effets concrets en pratique. En effet, techniquement, il paraît possible, dans certaines conditions, de désactiver un RFID pour le réactiver[138] par la suite[139]. Il convient donc de s'assurer que le procédé utilisé permette une destruction physique des tags.

Les particularités de la technologie RFID pourraient justifier l'adoption de textes spécifiques afin de prévoir, de manière globale, les conditions d'utilisation des tags et clarifier la situation. A ce titre une simple recommandation de la CNIL pourrait déjà permettre de fixer certaines limites à l'emploi de la technologie de radio identification dans la grande distribution. La recommandation sur les RFIDs que cette dernière a émise[140] montre déjà que le point a été remarqué et préfigure sans doute une véritable prise de position de l'autorité sur ce point.
Cependant en dehors de toute adoption de mesures propres à l'usage des RFIDs, il faut s'interroger sur l'éventuelle applicabilité des dispositions légales déjà mise en œuvre dans des domaines connexes. La prise en compte de ces mesures pouvant permettre de mieux appréhender les enjeux relatifs à la réglementation de la radio identification.

B- L'ébauche d'une réglementation de l'utilisation de la radio identification (RFID).

Envisager une réglementation propre à l'utilisation de la technologie RFID implique d'analyser les grands concepts propres à la collecte de données personnelles (puisqu'il est désormais établi que les données contenues dans les puces revêtent bien ce caractère) (1).

---

[136] Voir sur ce point un article paru dans e-week, *RSA keeps RFID private*, disponible à l'adresse suivante : http://www.eweek.com/article2/0,1759,1536569,00.asp

[137] On voit ici que la position de la CNIL tient compte des contingences liées aux RFIDs notamment sur l'éventuelle impossibilité de désactiver certaines puces en raison de leur nature (billet, passeport,…) mais aussi en raison du développement de législations en matière de droit d'auteur relatives aux mesures techniques de protection. Ces points seront plus largement évoqués dans la suite de l'étude, infra p. 47.

[138] Il apparaît plus que probable que la réactivation des tags constituerait un élément caractéristique d'une collecte déloyale d'informations nominatives et punissable en tant que telle par la loi du 6 janvier 1978.

[139] Pour illustration: extrait du brevet U.S. Pat. No. 5,313,192: *«By switching the second component between its activating and deactivating states the tag can be switched between its active and deactive states. A reusable tag with desired step changes in flux that is capable of deactivation and reactivation is thereby realized»*.

[140] CNIL, Communication de M. Philippe Lemoine relative à la Radio-Identification (Radio-Tags ou RFIds) ; précitée.

Dans une seconde étape il convient de rechercher si certaines dispositions sectorielles ne seraient pas susceptibles de s'appliquer à ce domaine (2). Il est enfin possible de s'inspirer de certaines initiatives législatives venues de l'étranger (3).

1- Les RFIDs envisagés au travers des grands principes applicables en matière de collecte de données personnelles.

En matière de données personnelles la collecte est souvent rattachée à deux grands principes, deux approches distinctes que l'on désigne sous les anglicismes d'OPT-IN et OPT-OUT.
Ces deux approches sont plus ou moins contraignantes en établissant des présomptions opposées. Alors que la première (OPT-OUT) présuppose que la personne dont les données nominatives sont collectées a donné implicitement son accord à une telle collecte (sauf opposition contraire), la seconde (OPT-IN) fait la présomption inverse en considérant que toute personne qui n'a pas donné explicitement et préalablement son consentement à ce que ses données personnelles soient recueillies est présumée être opposée à cette collecte.
Ce mécanisme est déjà largement utilisé dans les directives européennes, il semble être facilement transposable à la transmission des données contenues dans les puces RFID. Selon l'étendue de protection désirée, il conviendrait d'opter pour un régime ou pour l'autre. Il faut noter quoi qu'il en soit que les deux procédés offrent la possibilité pour le client d'obtenir que les puces incluses dans les articles qu'il achète soient désactivées.
Cet aspect est d'ailleurs déjà envisagé dans la communication de le CNIL relative à la radio identification lorsqu'elle énonce qu'il faudrait *« imposer la mise en place de mécanismes de désactivation des « smart tags » dans certaines situations et avec le libre choix des personnes »*[141]. La solution préconisée par la CNIL semble se rapprocher de la notion de l'OPT-OUT, le client devrait donc expressément demander au commerçant de désactiver les tags inclus dans ses achats.
On peut se demander si une telle position est conforme aux tendances des normes européennes. En effet le principe général de l'OPT-OUT[142] semble devoir être mis à mal depuis quelques années. Ainsi la directive 2002-58 du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, penche de son coté pour le principe de l'OPT-IN ; en ce sens elle semble montrer une volonté des autorités européennes de renforcer la protection des individus. Prenant le contre pied du principe retenu en matière de prospection par courriel dans les directives « commerce électronique » et « commercialisation des services financiers à distance » (OPT-OUT), la directive sectorielle renverse la tendance en établissant pour nouveau principe l'OPT-IN dans ce même domaine.
Faut-il y voir une solution isolée, restreinte à la prospection par voie électronique[143], ou une nouvelle tendance des autorités européenne appelée à être reprise de manière plus globale dans l'avenir ? Dans ce dernier cas, le principe vers lequel l'on se dirigerait serait celui de la

---

[141] CNIL, Communication de M. Philippe Lemoine relative à la Radio-Identification (Radio-Tags ou RFIds), précité, p. 8. Passage souligné par nos soins.

[142] Depuis plusieurs années le principe généralement retenu dans les directives communautaires est celui de l'OPT-OUT, ainsi les directives 97-66 (concernant la prospection par certains moyens de télécommunication) et 2000-31 (relative au commerce électronique et touchant à la prospection par voie d'e-mailling) ont opté pour une solution qui pose le principe que la personne est présumée consentir à la collecte et au traitement de ses données nominatives.

[143] Il faut cependant noter que le principe de l'OPT-IN avait déjà auparavant être reconnu à certaine prospection commerciales (prospection par automates d'appel, fax,…).

désactivation des tags lors du passage en caisse sauf au cas où le client souhaiterait que les puces restent actives[144].

La décision de placer l'utilisation des tags sous l'un ou l'autre des régimes permettrait de garantir un certain niveau de protection. Il faut noter cependant que même dans l'hypothèse où l'OPT-OUT serait consacré, l'utilisation des RFIDs imposerait une bonne information du public, les clients ne pouvant légitimement s'opposer à des traitements dont ils n'ont pas connaissance[145].

2- *Applicabilité des certaines règles sectorielles.*

Il est possible de s'inspirer de certaines règles sectorielles pour envisager la régulation des RFIDs. La technologie RFID permettant notamment une géolocalisation[146] (ce fut d'ailleurs sa fonction première pour l'identification des avions) on peut être amené à s'interroger sur l'applicabilité des dispositions propres à la matière. Celles-ci sont contenues à l'article 9 de la directive 2002-58 du 12 juillet 2002. Celui-ci prévoit ainsi que :
« 1. Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. Le fournisseur du service doit informer les utilisateurs ou les abonnés, avant d'obtenir leur consentement, du type de données de localisation autres que les données relatives au trafic qui sera traité, des objectifs et de la durée de ce traitement, et du fait que les données seront ou non transmises à un tiers en vue de la fourniture du service à valeur ajoutée. Les utilisateurs ou les abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données de localisation autres que les données relatives au trafic.
2. Lorsque les utilisateurs ou les abonnés ont donné leur consentement au traitement des données de localisation autres que les données relatives au trafic, ils doivent garder la possibilité d'interdire temporairement, par un moyen simple et gratuit, le traitement de ces données pour chaque connexion au réseau ou pour chaque transmission de communication.
3. Le traitement des données de localisation autres que les données relatives au trafic effectué conformément aux paragraphes 1 et 2 doit être restreint aux personnes agissant sous l'autorité du fournisseur du réseau public de communications ou service de communications

---

[144] La chaîne de magasins Metro semble vouloir retenir cette approche, ainsi celle-ci s'engage à ne traiter les informations contenues dans les tags apposés sur les achats de ses clients que dans le cas où ces derniers auraient expressément consentis à une telle collecte. Cependant cette approche n'indique pas si les puces seront désactivées en cas de non accord du client. Sur ce point voir Technology Information and Privacy Commissioner Ontario, *Tag, You're It: Privacy Implications of RadioFrequency Identification (RFID)*, Ann Cavoukian, Ph.D.Commissioner February 2004, précité, p 19.

[145] Cela est encore plus vrai dans le cadre de l'utilisation des RFIDs qui permettent un traitement totalement transparent pour le consommateur (technologie sans contact et taille de la puce).

[146] Cette fonction permise par l'utilisation des RFIDs est d'ailleurs clairement affirmée par la Commission Européenne suite aux attentats du 11 mars en Espagne. Voir Projet de déclaration sur la lutte contre le terrorisme du 22 mars 2004, précité. Texte disponible en version française à l'adresse suivante: http://www.edri.org/docs/ST07486-RE03.FR04.pdf

électroniques accessible au public ou du tiers qui fournit le service à valeur ajoutée, et doit se limiter à ce qui est nécessaire pour assurer la fourniture du service à valeur ajoutée »[147].
On voit qu'en matière de géolocalisation le principe d'information et de consentement des intéressés tient une place prépondérante. Il est certain qu'en raison du caractère intrusif de cette technologie, le législateur européen a souhaité apporter certaines garanties aux utilisateurs. Ainsi la conservation des données de localisation doit être limitée à ce qui est strictement nécessaire au service, le principe général étant la non conservation de ces données.

Il est certain que si la localisation par voie de téléphone mobile présente de réels risques en matière de libertés publiques, l'utilisation de la technologie RFID pourrait sans doute conduire au même résultat. La situation pourrait même s'avérer encore plus dangereuse pour le consommateur car les informations contenues dans le tag peuvent également fournir des détails précis sur la vie de la personne géolocalisée. La taille des puces rend transparente la géolocalisation, les individus n'auront pas conscience d'être géolocalisés. Si la technologie devient d'usage courant, il ne sera plus possible d'y échapper (si les tags ne sont pas désactivés l'individu ne pourra éviter d'être traqué dans le cas où les tags seraient inclus dans les vêtements[148], alors qu'il est toujours possible de laisser son téléphone mobile chez soi). Le risque est encore renforcé par le fait que les acteurs susceptibles de mettre en œuvre cette technologie sont nombreux et difficilement identifiables (contrairement aux opérateurs de téléphonie mobile).

La technologie de radio identification présente donc certains dangers potentiels ; pourtant jusqu'alors, même si l'opinion publique ainsi que les autorités de protection des données commencent à prendre conscience du risque que peut représenter cette technologie, on ne peut que constater l'absence de toute régulation sectorielle applicable aux RFIDs, cependant cet état de fait pourrait ne pas perdurer, déjà aux Etats-Unis des projets de loi ont été déposés afin de limiter le risque d'atteinte à la vie privée que représentent les RFIDs.

3- L'émergence d'une législation propre aux RFIDs

Face aux enjeux en terme de vie privée que représente l'utilisation de la technologie de radio identification, il pourrait paraître souhaitable d'adopter une législation particulière permettant d'encadrer l'usage des tags radio.

---

[147] Cette disposition de la directive est transposée par le projet de loi relatif aux communications électroniques et aux services de communication audiovisuelle, modifié par le Sénat le 15 avril 2004 dont l'article 10 dispose :
II. - L'article L. 34-1 du même code est ainsi modifié :
1° Le I est ainsi rédigé :
« I. - Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des II, III, IV et V. » ; (...)
3° Le dernier alinéa du III est ainsi rédigé :
« Les opérateurs peuvent en outre réaliser un traitement des données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si les abonnés y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période nécessaire pour la fourniture ou la commercialisation de ces services. Ils peuvent également conserver certaines données en vue d'assurer la sécurité de leurs réseaux. »

[148] Ce qui est le cas pour certaines marques de l'industrie textile comme par exemple la société Prada. De même un projet similaire était à l'étude chez Benetton.

Cette démarche a déjà été introduite aux Etats-Unis dans plusieurs Etats et tend à se généraliser. Un premier projet de loi a été proposé par le sénateur Bowen[149] dans l'état de Californie qui vise à ajouter au « *Business and Professions Code* » quelques paragraphes définissant les prérequis à l'utilisation de tags RFID. Ainsi *« cette loi rendra obligatoire pour une personne ou une organisation qui utilise des systèmes RFID de se conformer à certaines conditions, notamment le fait d'obtenir le consentement écrit d'un individu avant d'attacher ou de stocker des informations personnelles le concernant associées aux données collectées via un tag RFID »*[150].

Le texte dispose ainsi :

« Toute personne ou entité qui met en place un système de radio identification (RFID) qui peut être utilisé pour collecter des informations sur un individu doit obtenir le consentement écrit préalable de cette personne avant que toute information à caractère personnel, incluant le nom, l'adresse, le numéro de téléphone ou le numéro de carte de crédit, soit écrite sur ou conservée avec des données collectées via le système RFID.

Toute personne ou entité doit obtenir un consentement écrit distinct de l'individu avant que toute information concernant cette personne, collectée par le biais d'un système RFID, soit partagée avec un tiers.

Tout individu doit se voir reconnaître le droit d'accéder aux données à caractère personnel collectées par le biais d'un système RFID et de procéder aux rectifications nécessaires sur ces informations.

Toute personne ou entité doit prendre les mesures raisonnables pour s'assurer que les données à caractère personnel collectées par le biais d'un système RFID sont transmises et conservées dans de bonnes conditions de sécurité, et que l'accès à ces données est limité aux personnes dont la fonction est de faire fonctionner et maintenir le système RFID.

Si un commerçant [détaillant] *utilise un système RFID sur un bien de consommation, la puce RFID doit être détachée ou détruite avant que le consommateur quitte le magasin »*[151].

---

[149] Sur ce point voir RFID journal, *Bowen Seeks Balance in RFID Law*, disponible à l'adresse suivante: http://www.rfidjournal.com/article/articleprint/812/-1/1/

[150] Propos figurant dans les motifs précédant le texte du projet de loi relatif à l'utilisation des RFIDs, California Senate bill No. 1834

[151] Traduction libre de l'anglais. Le texte original est ainsi rédigé : Senate bill No. 1834

SECTION 1. Chapter 22.7 (commencing with Section 22650) is added to Division 8 of the Business and Professions Code, to read:

CHAPTER 22.7. RADIO FREQUENCY IDENTIFICATION

22650. A person or entity that uses a radio frequency identification (RFID) system that can be used to gather information about an individual shall obtain written consent from an individual before any personally identifiable information of the individual, including name, address, telephone number, or credit card number, is attached to or stored with data collected via the RFID system.

22651. A person or entity shall obtain separate written consent from an individual before any personally identifiable information about the individual collected by an RFID system is shared with a third party.

22652. An individual shall have the right to access his or her personally identifiable information collected through an RFID system and the opportunity to make corrections to that information.

22653. A person or entity shall take reasonable measures to ensure that any individual data collected via an RFID system is transmitted and stored in a secure manner, and that access to the data is limited to those individuals needed to operate and maintain the RFID system.

22654. If a retail store uses an RFID system on a consumer product, the RFID tag shall be detached or destroyed before a consumer leaves the store.

22655. Collecting information through an RFID system that is aggregate in nature and that does not personally identify an individual is not a violation of this chapter.

22656. A violation of this chapter is an act of unfair competition under Chapter 5 (commencing with Section 17200) of Division 7 and subject to the enforcement provisions of that chapter.

Les principes ainsi énoncés sont assez proches de ceux reconnus par la loi du 6 janvier 1978 que nous connaissons en droit français (droit d'accès, de rectification, obligation de sécurité,…), cependant l'aspect novateur concerne l'OPT-IN. En effet en prévoyant une autorisation écrite préalable au traitement des informations personnelles contenues dans les tags, le projet américain se montre très protecteur des consommateurs ; le texte va encore plus loin en imposant une destruction des puces à la sortie du magasin.
Cependant il convient de noter que lors de son passage devant le Sénat Californien, le projet du Sénateur Bowen a été considérablement assoupli[152]. Si le texte a été adopté c'est au prix de l'abandon du consentement écrit préalable et de l'obligation de destruction des tags, ce qui revient à réduire considérablement la protection des individus[153].
Cette initiative a été reprise par d'autres états américains comme le Maryland, le Massachusetts et la Virginie[154], on voit ainsi apparaître un peu partout aux Etats Unis des législations réglementant l'utilisation de la technologie RFID.

En Europe, ce type de dispositions n'existe pas (encore), cependant les autorités communautaires ont déjà commandé des rapports sur les incidences de cette technologie en matière vie privée[155]. Il faut noter que, contrairement aux lois en vigueur outre-atlantique, la législation européenne[156] offre déjà une certaine protection aux consommateurs en leur reconnaissant certains droits lorsque des données nominatives les concernant sont traitées. Etant donné que les tags sont reconnus comme étant des données à caractère personnel[157] ces dispositions de protection ont donc vocation à être appliquées.
Cependant il paraîtrait souhaitable qu'au plan européen des mesures soient prises afin que le traitement des informations contenues dans les puces soit soumis à un principe d'OPT-IN, ce qui a déjà était fait dans un domaine (la prospection par voie de courriel) alors que celui-ci est sans doute moins imprégné d'implications en matière de vie privée.

Il convient tout de même de noter que la consécration du principe de l'OPT-IN concernant la radio identification, qui conduirait sans doute nécessairement à la désactivation des puces, risque de se heurter à certaines difficultés d'ordre pratique mais aussi juridique.

---

[152] Voir un article du RFID journal : *States Move on RFID Privacy Issue*, disponible à l'adresse suivante : http://www.rfidjournal.com/article/articleprint/924/-1/1/
[153] Ne reste plus que les grands droits reconnus déjà par notre droit interne : droit d'accès et rectification, obligation de sécurité.
[154] Voir un article du RFID journal précité : *States Move on RFID Privacy Issue*, disponible à l'adresse suivante : http://www.rfidjournal.com/article/articleprint/924/-1/1/
[155] Report EUR 20823 EN, *Security and Privacy for the Citizen in the Post September 11 Digital Age: A Prospective Overview,* ou encore le rapport final de l'IST (Information Society Technology), *The oppurtunities ahead*, 2-4 octobre 2003, Milan Italie.
[156] Principalement la directive 95-46 du 24 octobre 1995.
[157] Ce point a été traité au chapitre I, voir supra p.13.

II- Des obstacles à la désactivation des puces RFIDS ?

Si la solution la plus respectueuse de la liberté des individus reste sans doute la désactivation pure et simple des tags lors du passage en caisse, il existe des cas où il ne sera pas envisageable de « tuer » les puces. En effet en pratique, dans certaines circonstances, il sera impossible de désactiver les RFIDs et cela en raison d'obstacles pratiques (A), mais aussi juridiques, l'introduction de nouvelles législations au plan européen pouvant conduire à rendre pénalement sanctionnable le fait d'enlever un tag sur un bien de consommation (B).

A- L'existence d'obstacles pratiques à la désactivation des tags.

Il existe des situations où la possibilité de désactiver les puces RFID sera fortement remise en cause, pour ne pas dire totalement exclue. Tel sera le cas des tags directement apposés par une autorité publique (1) mais aussi pour les badges utilisés dans le cadre d'une relation de travail (2) et enfin dans le cas où le tag est nécessaire à l'exercice d'un droit dans le cadre d'une relation contractuelle (3).

1- L'utilisation des RFIDs par les autorités publiques.

Les projets visant à mettre en place des systèmes basés sur la radio identification ne sont pas uniquement le fait des acteurs de la grande distribution[158], les Etats tendent de plus en plus à recourir à cette technologie. Au travers de cette étude, les différents projets mis en œuvre par les autorités nationales ont déjà pu être abordés[159]. On rappellera simplement que ces projets concernent, au plan européen notamment : le futur passeport européen de même que les futurs visas sécurisés qui seront remis aux étrangers, mais aussi les billets de banques (Euros).
Il convient de noter que de manière plus abstraite la Commission européenne envisage de mettre des étiquettes RFID dans tous les matériels sensibles (armement) afin de permettre le suivi de leur circulation par satellite.
Des initiatives similaires ont lieu au niveau national en dehors de toute régulation européenne, ainsi en France des projets sont en cours afin de mettre en place un système de carte, dénommé carte de vie quotidienne, dont la fonction sera de faciliter les relations des administrés avec l'administration en centralisant certaines informations. La carte qui se veut multitâche pourra ainsi permettre de regrouper divers informations utiles au quotidien (abonnement de transport en commun,…).

Il est certain que dans les cas où l'utilisation de la technologie RFID est le fait des autorités publiques, il semblerait malvenu de désactiver les tags sauf à s'exposer à une sanction.
Ainsi l'individu pourra toujours être suivi grâce aux billets de banque qu'il transporte ou à son passeport. Dans ce cas la question primordiale ne sera pas l'existence d'un droit d'opposition au traitement qui impliquerait nécessairement la désactivation des puces, mais plutôt les conditions de traitement des informations contenues dans celles-ci. Il conviendrait ainsi que la

---

[158] Même si les deux peuvent être liés, ainsi le Department of Defense (DoD) américain va bientôt imposer à ses fournisseurs que tous les produits qui lui sont fournis soient pourvus de tags RFID. Voir : DoD RFID Policy Requires Suppliers' Compliance by January 2005 à l'adresse suivante : http://xml.coverpages.org/DoD-RFID.html

[159] Voir supra p. 15 et suivantes.

sécurité du transfert de données soit assurée avec une certaine rigueur[160], le cas est plus flagrant pour le passeport qui rendra directement identifiable un individu. Dans cette optique l'Etat devra s'assurer que la lecture de la puce soit bien réservée à l'autorité compétente[161] et non ouverte à tous les lecteurs (ceux des magasins notamment). La solution pourrait consister dans l'utilisation de la cryptographie[162] afin de réserver l'accès uniquement aux demandeurs légitimes qui disposeront du code secret permettant d'accéder aux informations[163].

Il paraît donc évident que l'individu qui ne désirerait pas être tracé par les RFIDs n'aurait pour unique solution que de ne pas emmener sa pièce d'identité et de préférer la monnaie métallique aux billets de banques. Cependant le cas de l'utilisation des tags par l'Etat ne semble pas le seul cas où il soit impossible de désactiver le tag, en effet la même situation existe dès lors que le traitement est instauré dans le cadre d'une relation de travail.

2- L'utilisation des RFIDs dans les relations de travail.

Les cas où la désactivation est *de facto* impossible concernent aussi les relations de travail. En effet dans ce contexte l'employeur peut sous certaines conditions dicter les choix, notamment quant à l'utilisation de la technologie de radio identification. Cependant l'employeur ne reste pas totalement libre, en effet le droit social s'est adapté aux risques que pouvaient représenter les technologies de l'information et de la communication pour les collaborateurs de l'entreprise. Le législateur a donc instauré des mesures ayant pour vocation de limiter les prérogatives de l'employeur devant l'équilibre inégal qui régit les relations salariales.

Ainsi, dans l'ordre interne, une première limitation législative aux pouvoirs de l'employeur est intervenue le 4 août 1982. Ce fut le règlement intérieur qui subit la première attaque au travers de la modification de l'article 122-35 du code du travail. La loi 82-689, comme le remarquait alors le professeur Lyon-Caen, *« s'est attaquée à la plus vieille institution du droit du travail : le règlement intérieur, acte dans lequel s'exprime le pouvoir réglementaire privé du chef d'entreprise »*. L'ajout fait à l'article 122-35 dispose que : *Article 122-35 : […] Il* [le règlement intérieur] *ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.[…]*
Cette modification n'avait pas alors pour but d'empêcher l'intrusion que pouvaient permettre le recours aux nouvelles technologies dans le monde du travail. Cependant cette première limitation aux pouvoirs de l'employeur permit à la jurisprudence de se développer et a ouvert la voie aux décisions et législation relatives plus particulièrement aux TIC. En imposant le principe de proportionnalité comme contrepoids à l'omnipotence du chef d'entreprise, la loi

[160] Ce qui est d'ailleurs une obligation générale imposée au responsable du traitement par la loi informatique et libertés.
[161] Bien que même dans ce cas il soit possible de se demander si l'état a un motif légitime de contrôle de l'identité et ce en toute occasion. On pensera à la police nationale qui pourrait bien être considérée comme une autorité devant avoir accès aux données de la puce (pour vérifier l'authenticité d'une pièce d'identité à l'aide des données biométriques qu'elle contient) cependant cela reviendrait à accepter le fait que les policiers aient le droit de contrôler un individu sans motifs et à son insu.
[162] Il semble que la sécurité permise par les puces RFID soit encore très approximative et que techniquement il soit très difficile voire impossible de garantir la confidentialité des données contenues dans les puces.
[163] Cependant le secret ne doit pas être trop épais, il faut qu'il soit partagé avec les états étrangers pour que le douanier américain puisse contrôler la validité du passeport d'un français.

de 1982 posait une première pierre qui allait ensuite permettre de construire une barrière à l'immixtion de l'employeur dans la vie privée du salarié.
Un second pas fut opéré par loi du 31 décembre 1992 qui généralisa le principe de proportionnalité. Ainsi le nouvel article 120-2 inséré dans le code du travail prévoit que :*« Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché »* : l'employeur peut contrôler l'activité de ses salariés mais ce contrôle doit être proportionné à la tâche.

Dans le même temps, l'article 122-39 a soumis au même régime juridique que le règlement intérieur lui-même toutes les notes de service ou tout autre document qui portent prescriptions générales et permanentes dans les matières qui relèvent du règlement intérieur, c'est-à-dire notamment les conditions d'utilisation des équipements de travail et les règles générales et permanentes relatives à la discipline.

Parallèlement la même loi a imposé l'obligation pour l'employeur d'informer et de consulter le comité d'entreprise, avant toute mise en œuvre de moyens techniques permettant un contrôle de l'activité des salariés. C'est ce qu'il ressort de l'article 432-2-1 qui dispose que :*« Le comité d'entreprise est informé, préalablement à leur utilisation, sur les méthodes ou techniques d'aide au recrutement des candidats à un emploi ainsi que sur toute modification de celles-ci. Il est aussi informé, préalablement à leur introduction dans l'entreprise, sur les traitements automatisés de gestion du personnel et sur tut e modification de ceux-ci. Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés. »*

Dans le même ordre d'idée l'article 432-2 imposait quant à lui : *« Le comité d'entreprise est informé et consulté, préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail du personnel. Les membres du comité reçoivent, un mois avant la réunion, des éléments d'information sur ces projets et leurs conséquences quant aux points mentionnés ci-dessus.*
Lorsque l'employeur envisage de mettre en œuvre des mutations technologiques importantes et rapides, il doit établir un plan d'adaptation. Ce plan est transmis, pour information et consultation, au comité d'entreprise en même temps que les autres éléments d'information relatifs à l'introduction de nouvelles technologies. En outre, le comité d'entreprise est régulièrement informé et périodiquement consulté sur la mise en œuvre de ce plan. »

Il ressort de toutes ces dispositions, directement ou indirectement relatives à la place des technologies de l'information et de la communication, que l'employeur ne peut agir unilatéralement, son pouvoir est limité par les textes. On considère généralement que la mise en place de nouveaux moyens technologiques dans l'entreprise doit répondre à trois types d'exigences.

- La première est la proportionnalité induite par l'article 120-2 du code du travail. Il vise d'une manière générale le respect de droits des personnes et forme le prolongement des principes de la loi informatique et libertés[164].

[164] Loi du 6 janvier 1978, n° 78-17 relative à l'informatique, aux fichiers et aux libertés.

- La seconde est la transparence, également issu de la loi informatique et libertés qui impose qu'aucune donnée ne peut être collectée par un moyen frauduleux ou illicite. Cela se traduit par une obligation d'information des personnes à l'endroit desquelles s'effectuent la collecte et le traitement, sur les destinataires des traitements et sur le lieu où s'exercent les droits d'accès et de rectification. Le même principe a été transposé au monde l'entreprise au travers de l'article 121-8 qui dispose qu' *« aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à un emploi. »*

- Enfin la dernière est la discussion collective, *« organisée par le code du travail lors de l'introduction dans l'entreprise de traitements automatisés de gestion du personnel ou de moyens et techniques permettant un contrôle d'activité du salarié (article L 432-2-1 du code du travail), la discussion collective donne sa substance au principe de proportionnalité. Le rapport inégal entre l'employeur et ses salariés, consubstantiel à la nature même du contrat de travail et au lien de subordination qui le caractérise, ne garantit pas naturellement la proportionnalité. Trop souvent, sous l'influence sans doute des entreprises américaines, les employeurs soumettent individuellement aux salariés, des chartes, des engagements écrits équivalant à une abdication complète par les salariés de leurs droits »*[165] .

Dans le cadre de l'entreprise l'introduction d'une nouvelle technologie comme celle de la radio-identification devra donc respecter les principes de protection posés par le droit social qui ne sont en fait qu'une sorte de transposition au monde du travail de la loi informatique et libertés. Cependant les droits ainsi reconnus ne garantissent pas aux salariés un droit à la désactivation des tags. Dans le cadre de la relation de travail l'employé devra donc se soumettre au règlement intérieur qui pourra prévoir une obligation de contrôle de la présence et de l'identité notamment au travers d'un système basé sur les RFIDs.
Plusieurs solutions sont déjà proposées notamment afin de verrouiller un ordinateur dès lors que l'employé n'est plus à son poste de travail. Le système est basé sur une puce portée par le salarié et un lecteur intégré dans l'ordinateur qui vérifie que le tag est toujours à proximité[166]. La mise en place d'un tel système pourrait avoir pour conséquence de connaître en temps réel les agissements de tous les salariés[167]. Dans cette éventualité néanmoins, le droit du travail aurait vocation à s'appliquer (conformément à ce que nous avons vu) pour qu'en France, tout du moins, ce système ne puisse être exploité.

3- L'utilisation des RFIDs dans l'exercice d'un droit.

Il semble que la désactivation des tags ne soit pas non plus en pratique envisageable dès lors que le tag est nécessaire à l'accomplissement d'une prestation, on pense en tout premier lieu

[165] CNIL, rapport d'étude et de consultation publique, La cybersurveillance des salariés dans l'entreprise, mars 2001. p. 18.
[166] Voir sur ce point un article paru sur le site FWC, *Vendors lock down PCs*, à l'adresse suivante : http://www.fcw.com/fcw/articles/2003/0623/tec-review-06-23-03.asp
[167] Le badge pouvant sans doute servir à identifier le salarié lors de l'entrée sur son lieu de travail, il est possible pour l'employeur de multiplier le nombre de lecteur (dans les couloirs, dans les salles de repos,…) pour savoir où sont ses employés et avec qui.

au passe Navigo mis en place par la RATP[168]. Mais cela ne se limite pas uniquement à ce cas particulier, il en ira de même pour les péages routiers et tout autre application utilisant la technologie RFID dans le cadre d'une relation contractuelle (prestation de services).
La personne qui ne souhaiterait pas que les données la concernant soient traitées ne pourrait alors pas profiter du service offert (en l'absence d'alternatives offertes par le vendeur). Dans ce cas, la désactivation ne paraît pas envisageable, celle-ci ayant pour effet de priver l'utilisateur des services auxquels il a souscrit.
Comme pour les traitements faisant appel à la radio identification mis en œuvre par l'Etat, à défaut de droit d'opposition, il appartiendra au maître du fichier (le responsable du traitement) de prendre les mesures adéquates afin de s'assurer que l'accès aux informations contenues dans la puce soit limité aux personnes habilitées.

Il ressort de tout ceci que le principe d'OPT-IN et donc de reconnaissance d'un droit de consentement préalable ne trouve réellement à s'appliquer que pour les biens de consommation. Cependant même dans ce domaine le droit à désactiver pourrait connaître certaines entraves, celles-ci, cette fois, ne sont plus d'ordre pratique mais juridique. En effet l'évolution de notre droit, sous l'influence des directives européennes pourrait conduire à rendre sanctionnable pénalement le fait d'enlever ou de désactiver un tag RFID.

B- L'existence d'obstacles juridiques à la désactivation des tags : vie privée *vs* lutte contre la contrefaçon ?

Le développement du piratage des œuvres de l'esprit telles que les disques musicaux de même que l'accroissement de la contrefaçon de biens de consommation, ont amené les instances européennes à s'intéresser aux moyens pouvant être mis en œuvre afin de lutter contre ces phénomènes. Dans ce contexte, la Commission Européenne rendait public, en 1998[169] un livre vert en vue de s'attaquer au problème de la contrefaçon et de la piraterie dans le marché unique. Parmi les solution proposées afin de lutter contre ce fléau la Commission considérait alors que *« l'un des moyens de lutter contre la contrefaçon et la piraterie à la disposition des titulaires des droits de propriété intellectuelle est l'utilisation de dispositifs techniques pour protéger et authentifier leurs produits et services qui peuvent prendre des formes diverses : hologrammes de sécurité, moyens optiques, cartes à puce, systèmes magnétiques, étiquettes microscopiques…Ces dispositifs permettent de "suivre la trace" des utilisations illicites et donc de poursuivre les contrevenants. Les programmes de recherche et de développement pourraient contribuer à apporter des solutions innovantes »*[170].
Alors que le terme de radio identification n'est pas utilisé on voit bien que les étiquettes qui permettront de « suivre à la trace » les produits contrefaits ne peuvent faire référence qu'aux tags RFID[171]. L'idée était lancée, mais il lui fallut tout de même quelques années avant de se voir consacrée par un texte.

---

[168] Encore faut il noter que concernant Navigo l'usager disposant aussi d'un titre de transport sous la forme d'un coupon, il a toujours la possibilité de ne pas utiliser le tag RFID.
[169] Commission, Livre vert sur la lutte contre la contrefaçon et la piraterie dans le marché intérieur, 15 octobre 1998, COM (98)569 final. Disponible à l'adresse suivante : http://europa.eu.int/comm/internal_market/en/indprop/piracy/lvconfr.pdf
[170] Voir communiqué de presse de la Commission à l'adresse suivante : http://europa.eu.int/comm/internal_market/fr/indprop/piracy/922.htm
[171] En ce sens la Commission fait preuve d'une grande anticipation technologique en prévoyant il y a tout de même 6 ans le recours aux RFIDs, alors qu' à cette époque cette solution ne devait pas être viable.

L'adoption de la directive 2001-29[172] du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information consacre la protection des mesures techniques (de protection) et donc de manière implicite justifie une interdiction de désactivation des tags.
L'article 6 de cette directive dispose ainsi que *« les États membres prévoient une protection juridique appropriée contre le contournement de toute mesure technique efficace, que la personne effectue en sachant, ou en ayant des raisons valables de penser, qu'elle poursuit cet objectif. (…)*
Aux fins de la présente directive, on entend par "mesures techniques", toute technologie, dispositif ou composant qui, dans le cadre normal de son fonctionnement, est destiné à empêcher ou à limiter, en ce qui concerne les oeuvres ou autres objets protégés, les actes non autorisés par le titulaire d'un droit d'auteur ou d'un droit voisin du droit d'auteur prévu par la loi, ou du droit sui generis prévu au chapitre III de la directive 96/9/CE. Les mesures techniques sont réputées efficaces lorsque l'utilisation d'une oeuvre protégée, ou celle d'un autre objet protégé, est contrôlée par les titulaires du droit grâce à l'application d'un code d'accès ou d'un procédé de protection, tel que le cryptage, le brouillage ou toute autre transformation de l'œuvre ou de l'objet protégé ou d'un mécanisme de contrôle de copie qui atteint cet objectif de protection (…) ».

Or l'implantation d'une puce RFID dans un produit pourrait très bien être considérée comme une mesure technique de protection. Cette mesure serait alors même extrêmement efficace grâce à l'attribution d'un code unique à chaque objet (propre au système EPC vu précédemment). La radio identification permettrait alors de contrôler l'authenticité des objets[173]. Dans ce contexte la désactivation des puces serait impossible en vertu d'une obligation légale et l'individu qui se risquerait à enlever le tag de son manteau de marque serait passible de sanctions pénales.
De même les initiatives telles que dataprivatizer, le blocker tag de RSA ou encore le logiciel de L. Dachary[174] seraient illégales car la directive interdit aussi que soit fournis des moyens permettant de contourner des mesures techniques de protection.
En effet l'article 6 de la directive dispose aussi que : *« Les États membres prévoient une protection juridique appropriée contre la fabrication, l'importation, la distribution, la vente, la location, la publicité en vue de la vente ou de la location, ou la possession à des fins commerciales de dispositifs, produits ou composants ou la prestation de services qui:*
a) font l'objet d'une promotion, d'une publicité ou d'une commercialisation, dans le but de contourner la protection, ou
b) n'ont qu'un but commercial limité ou une utilisation limitée autre que de contourner la protection, ou
c) sont principalement conçus, produits, adaptés ou réalisés dans le but de permettre ou de faciliter le contournement de la protection de toute mesure technique efficace ».

---

[172] Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information dont le texte peut être trouvé à l'adresse suivante : http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=FR&numdoc=32001L0029&model=guichett

[173] Pour rappel la base de donnée EPC contient toutes les références des objets produits dans le monde, en douane (ou autre) il suffirait de contrôler les numéros pour voir si le code est valable ou s'il a été falsifié (il pourrait correspondre à des produits d'un lot ancien qui ont déjà été vendus).

[174] Ces mécanismes permettant de concilier les besoins de l'industrie en matière de gestion des stocks et le respect de la vie privée des individus ont été abordés supra p. 34.

Il faut noter que ces dispositions sont en cours de transposition dans l'ordre juridique français au travers du projet de loi relatif au droit d'auteur et aux droits voisins dans la société de l'information déposé devant l'Assemblée Nationale[175]. L'adoption de cette loi conduira à

[175] Le texte du projet prévoit notamment d'insérer dans le code de la propriété intellectuelle les articles suivants :

Art. L. 331-5.- Les mesures techniques efficaces destinées à empêcher ou limiter les utilisations non autorisées par le titulaire d'un droit d'auteur ou d'un droit voisin du droit d'auteur, d'une œuvre, d'une interprétation, d'un phonogramme, d'un vidéogramme ou d'un programme, sont protégées dans les conditions prévues au présent titre. Ces dispositions ne sont pas applicables aux logiciels ;

On entend par mesure technique au sens de l'alinéa précédent, toute technologie, dispositif, composant, qui, dans le cadre normal de son fonctionnement, accomplit la fonction prévue à l'alinéa précédent. Ces mesures techniques sont réputées efficaces lorsqu'une utilisation visée à l'alinéa précédent est contrôlée grâce à l'application d'un code d'accès, d'un procédé de protection, tel que le cryptage, le brouillage ou toute autre transformation de l'objet de la protection, ou d'un mécanisme de contrôle de la copie qui atteint cet objectif de protection.

Art. L. 335-3-1.- Est assimilé à un délit de contrefaçon :

1° Le fait pour une personne de porter atteinte, en connaissance de cause, à une mesure technique mentionnée à l'article L. 331-5 afin d'altérer la protection, assurée par cette mesure, portant sur une œuvre ;

2° Le fait, en connaissance de cause, de fabriquer ou d'importer une application technologique, un dispositif ou un composant ou de fournir un service, destinés à faciliter ou à permettre la réalisation, en tout ou en partie, du fait mentionné au 1° ci-dessus ;

3° Le fait, en connaissance de cause, de détenir en vue de la vente, du prêt ou de la location, d'offrir à la vente, au prêt ou à la location, de mettre à disposition sous quelque forme que ce soit une application technologique, un dispositif ou un composant ou de fournir un service destinés à faciliter ou à permettre la réalisation, en tout ou en partie, du fait mentionné au 1° ci-dessus ;

4° Le fait, en connaissance de cause, de commander, de concevoir, d'organiser, de reproduire, de distribuer ou de diffuser une publicité, de faire connaître, directement ou indirectement, une application technologique, un dispositif, un composant ou un service destinés à faciliter ou à permettre la réalisation, en tout ou en partie, de l'un des faits mentionnés au 1° ou au 2° ci-dessus.

Art. L. 335-3-2.- Est également assimilé à un délit de contrefaçon le fait d'accomplir, en connaissance de cause, l'un des faits suivants lorsqu'il entraîne, permet, facilite ou dissimule une atteinte à un droit d'auteur :

1° Supprimer ou modifier tout élément d'information visé à l'article L. 331-10 lorsqu'il porte sur une œuvre ;

2° Distribuer, importer, mettre à disposition sous quelque forme que ce soit ou communiquer au public, directement ou indirectement, une œuvre dont un élément d'information mentionné à l'article L. 331-10 a été supprimé ou modifié ;

3° Fabriquer ou importer une application technologique, un dispositif ou un composant ou fournir un service ou une information destinés à faciliter ou à permettre la réalisation, en tout ou en partie, de l'un des faits mentionnés au 1° ou au 2° ci-dessus ;

4° Détenir en vue de la vente, du prêt ou de la location, offrir à la vente, au prêt ou à la location, mettre à disposition sous quelque forme que ce soit ou communiquer au public, directement ou indirectement, une application technologique, un dispositif ou un composant ou fournir un service destinés à faciliter ou à permettre la réalisation, en tout ou en partie, de l'un des faits mentionnés au 1° ou au 2° ci-dessus ;

5° Commander, concevoir, organiser, reproduire, distribuer ou diffuser une publicité, faire connaître, directement ou indirectement, une application technologique, un dispositif, un composant ou un service, destinés à faciliter ou à permettre la réalisation, en tout ou en partie, de l'un des faits mentionnés au 1°, au 2° ou au 4° ci-dessus. »

Art. L. 331-10.- Les informations sous forme électronique concernant le régime des droits afférents à une œuvre, une interprétation, un phonogramme, un vidéogramme ou un programme, sont protégées dans les conditions prévues au présent titre, lorsque l'un des éléments d'information, numéros ou codes est joint à la reproduction ou apparaît en relation avec la communication au public de l'œuvre, de l'interprétation, du phonogramme, du vidéogramme ou du programme qu'il concerne. Ces dispositions ne sont pas applicables aux logiciels.

On entend par information sous forme électronique toute information fournie par un titulaire de droits qui permet d'identifier une œuvre, une interprétation, un phonogramme, un vidéogramme, un programme ou un titulaire de droit, toute information sur les conditions et modalités d'utilisation d'une œuvre, d'une interprétation, d'un phonogramme, d'un vidéogramme ou d'un programme, ainsi que tout numéro ou code représentant tout ou partie de ces informations.

assimiler au délit de contrefaçon le fait de retirer une mesure de protection ou de fournir les outils permettant de contourner cette protection.
La possibilité offerte aux consommateurs de supprimer les puces RFID des bien qu'ils ont acquis pourtant légalement pourrait donc être écartée dans de nombreux cas, on se souviendra que cette solution était pourtant prônée par les autorités en charge de la protection des données personnelles au premier rang desquelles figure la CNIL.
Lors de la 25ème conférence des commissaires à la protection des données et à la vie privée qui s'est tenue à Sidney, les commissaires ont pu noter que *« des initiatives en cours visant à interdire la modification des dispositifs couverts par le droit d'auteur pourraient empêcher les personnes concernées de neutraliser les étiquettes RFID qui ne respectent pas la vie privée (ex : après avoir payé et quitté le magasin) »*[176].

Dans une approche similaire une autre directive relative au renforcement de la propriété intellectuelle a été adoptée très récemment[177]. Celle-ci ne fait pas référence aux mesures techniques de protection dans sa version définitive, cependant on notera que le texte de la proposition de directive faisait lui aussi indirectement référence à la protection des œuvres de l'esprit, notamment grâce à la technique de radio-identification.
L'Article 21[178] qui a été supprimé par la suite disposait que :
« *1. Sans préjudice des dispositions particulières applicables dans le domaine du droit d'auteur, des droits voisins et du droit sui generis du fabricant d'une base de données, les Etats membres prévoient une protection juridique appropriée contre la fabrication, l'importation, la distribution et l'utilisation de dispositifs techniques illégitimes.*
2. Aux fins du présent chapitre, on entend par:
a) « dispositif technique », toute technologie, dispositif ou composant qui, dans le cadre normal de son fonctionnement, est destiné à fabriquer des marchandises authentiques et à permettre d'y incorporer des éléments évidents, identifiables par la clientèle ou les consommateurs, qui leur facilitent la reconnaissance de l'authenticité de ces mêmes marchandises,
b) « dispositif technique illégitime », tout dispositif technique destiné à contourner un dispositif technique et qui permet la fabrication de marchandises portant atteinte aux droits de propriété industrielle qui incorporent les éléments évidents identifiables, tels que décrits au point a) ».

Dans l'exposé des motifs attaché à la directive il était précisé que : « *L'article 21 met en place une protection juridique des dispositifs techniques dans le domaine de la propriété industrielle. Les dispositifs techniques sont utilisés pour protéger et authentifier les produits ou services. Ils sont destinés à fabriquer des marchandises authentiques et à permettre d'y incorporer des éléments évidents, identifiables par la clientèle et les consommateurs, qui leur facilitent la reconnaissance de l'authenticité de ces mêmes marchandises. Ces éléments peuvent prendre des formes diverses: hologrammes de sécurité, moyens optiques, cartes à puce, systèmes magnétiques, encres spéciales, étiquettes microscopiques, etc. Une protection similaire existe déjà dans certains domaines (article 6 de la directive 2001/29/CE sur le droit d'auteur dans la société de l'information; article 4 de la directive 98/84/CE sur les services à accès conditionnel). Le paragraphe 1 dispose que, sans préjudice des dispositions existantes dans le domaine du droit d'auteur, les Etats membres doivent interdire certains actes*

[176] 25ème Conférence Internationale des Commissaires à la protection des données et à la vie privée, Sydney, 12 septembre 2003, Résolution sur la radio-identification, version finale du 20 novembre 2003.
[177] Le 28 mars 2004.
[178] Ces articles figuraient encore dans la version du texte en date du 30 janvier 2004 avant l'adoption définitive.

(fabrication, importation, distribution, utilisation) relatifs aux dispositifs techniques illégitimes. Le paragraphe 2 précise ce qu'il faut entendre par « dispositif technique » et par « dispositif technique illégitime » aux fins de l'application du présent article ».

Si ces dispositions ne visent pas directement l'usage des RFIDs on voit tout de même qu'elles pourraient aisément justifier l'emploi de cette technologie comme mesure de protection. Le considérant 27 de cette même directive garde la trace de cette volonté[179] lorsqu'il énonce que *« la surveillance de la production de disques optiques, particulièrement grâce à des moyens d'identification directement insérés dans les disques produits sur le territoire de la communauté, aide à limiter les atteintes à la propriété intellectuelle dans ce secteur qui souffre d'un piratage à grande échelle ».*
L'article 21, alors qu'il existait encore, avait attiré l'attention de la Délégation fédérale de protection des données (BnD) (l'équivalent Allemand de la Cnil), qui relevait qu'en mettant en place une protection juridique des dispositifs techniques utilisés pour sécuriser ou authentifier des produits ou services, cette mesure pouvait servir à légitimer la prolifération des étiquettes électroniques ou RFID (*Radio Frequency Identification*) et que le risque était qu'*« elles* [soient] *détournées de leur usage premier, pour récolter subrepticement des données sur les citoyens »*[180].

L'abandon de l'article 21 de la directive sur le renforcement de la propriété intellectuelle (qui vise principalement la propriété industrielle) semble justifié par le fait que l'article 6 de la directive 2001-29 envisageait expressément la protection des œuvres de l'esprit. Il faut noter que le considérant 27, qui justifiait une protection des mesures de protection, de la directive vise principalement la lutte contre piratage des disques dont la protection est assurée par le droit d'auteur (et donc par la directive 2001-29). Le motif semblait donc erroné pour vouloir imposer une autre mesure en faveur de l'industrie du disque[181].

Malgré ce recul de la directive sur le renforcement de la propriété intellectuelle on voit bien que déjà une large place existe pour admettre la protection contre la désactivation des radio-tags. En résumé le principe d'un droit à la désactivation, même s'il est plaidé par de nombreuses autorités de protection des données, ne pourrait subsister que si :

- l'industriel désactive lui même le tag s'il est incorporé dans le produit (à moins de devoir recourir à des moyens externes : killer tag, data privatizer,… et à condition que ceux ci ne soient pas interdits globalement comme participant au contournement d'une mesure de protection),
- pour les biens qui ne sont pas utilisés pour un traitement mis en œuvre par l'autorité publique,
- si la radio identification n'est pas utilisée dans un processus contractuel ou dans le cadre d'une relation de travail,
- ne participe pas à la protection d'une œuvre protégée par le droit d'auteur.

La place laissée à la désactivation passe donc du principe à l'exception devant la réduction drastique de son champ d'application possible.

---

[179] Curieusement il semble que ce considérant n'ait pas été modifié alors que l'article 21 lui était supprimé.
[180] Voir un article proposé par le site N juris, Critique de la proposition de directive européenne relative à la lutte contre la contrefaçon à l'adresse suivante : http://www.njuris.com/Imp_Breve.aspx?IDBreve=639
[181] On comprend bien que le fait que le rapporteur de texte, Mme Janelly Fourtou, ait été sensibilisé aux difficultés que peut rencontrer l'industrie du disque, son époux n'étant autre que le président de Vivendi Universal, M. Jean René Fourtou.

On peut tout de même s'interroger sur la validité d'une telle restriction au droit de désactivation des tags, principalement dans le cas des biens de consommation. En effet la personne qui acquiert (dans le cas de la vente) un produit dispose d'un droit de propriété sur celui-ci. L'article 544 du code civil dispose d'ailleurs que *« la propriété est le droit de jouir et de disposer de la chose de la manière la plus absolue,… »*. Ce droit s'est même vu reconnaître une valeur constitutionnelle (article 2 de la Déclaration des Droits de l'Homme et du Citoyen de 1789)[182]. L'interdiction de désactivation des puces sur les produits achetés constitue à n'en point douter une restriction au droit de propriété. Le droit de propriété se démembre en trois droits complémentaires : l'*usus*, le *fructus* et l'*abusus*. L'*usus* est le droit d'utiliser la chose, le *fructus* le droit d'en retirer les fruits et l'*abusus* le droit de la céder, de la nantir ou pourquoi pas de la détruire en tout ou en partie. Rien ne pourrait alors s'opposer à ce que l'acquéreur légitime d'un bien détruise le tag inséré dans le produit qu'il vient d'acheter. En effet l'existence de droits concurrents reconnus par le code de la propriété intellectuelle ne doit aucunement limiter le droit de propriété pour le faire ressembler à un simple droit d'usage[183].

L'utilisation de la radio-identification suscite, donc comme il est fréquent face aux évolutions techniques de nouvelles questions auxquelles le droit se devra de répondre sous peine de laisser se développer l'insécurité juridique.

[182] Le droit de propriété ne connaît que de rares exceptions à son caractère absolu : expropriation pour cause d'utilité publique, abus de droit,… quoi qu'il en soit ces exceptions doivent répondre à des impératifs supérieurs pour justifier l'atteinte à un droit reconnu comme ayant une valeur constitutionnelle. Il n'est pas certain que la lutte contre le piratage soit un juste motif autorisant le législateur à empiéter sur le droit de propriété. En dernier recours il pourrait appartenir au Conseil Constitutionnel de trancher ce point lors de l'adoption de la loi transposant la directive 2001-29.

[183] Dans un domaine distinct mais dont la problématique est fortement similaire, principalement quant aux interférences entre droit d'auteur et droit de propriété. voir J. Huet, De la "vente" de logiciel in Mélange Catala 2001.

Conclusion

Alors que la bataille contre l'immixtion dans la vie personnelle que constituent les RFIDs n'en est qu'à ses débuts, déjà les ingénieurs ont créé de nouveaux moyens permettant d'assurer la traçabilité des individus avec des implications encore plus importantes pour les libertés individuelles. La technologie permet déjà de « sniffer » l'ADN. *« Les renifleurs d'ADN sont considérés comme étant le futur des systèmes d'identification (...). Ces* [appareils] *combinent les aspects d'identification sans contact comme les RFIDs et des processus d'identification biométriques. Le renifleur pourrait être comparé au lecteur RFID et les cellules humaines aux tags. Parce que l'ADN est unique, il pourrait aussi être considéré comme une identification biométrique.* [Ces systèmes] *hériteront sans doute des difficultés inhérentes, en matière de vie privée et de sécurité, à ces deux plateformes d'identification »*[184].

On voit dans ce domaine que l'évolution des technologies provoque sans cesse des heurts avec le droit au respect de la vie privée reconnu aux individus. La technique permettant de tracer toujours plus précisément les habitudes de chacun, il convient d'adapter notre droit aux évolutions de cette dernière. Le juriste intervient alors *a posteriori* tentant de redonner à l'individu une part de liberté que les ingénieurs, par les progrès qu'ils permettent, lui ont pris. L'évolution de droit est conduite par celle de la technique et *« ce ne sont pas les philosophes avec leurs théories, ni les juristes avec leurs formules mais les ingénieurs avec leurs inventions qui font le droit et le progrès du droit »*[185].

Tel serait donc le rôle du droit dans nos sociétés modernes, agir comme un garde fou aux immixtions sans cesse plus présentes de la technologie dans notre vie quotidienne. Le juriste devenu garant des libertés doit donc rester vigilant !

« Le prix de la liberté c'est la vigilance éternelle »
Thomas Jefferson.

[184] Rapport final de l'IST (Information Society Technology), *The opportunities ahead*, 2-4 octobre 2003, Milan Italie, p. 51 et 52.
[185] Cette citation de De la Pradelle datant de près d'un siècle (1908) garde un note tout à fait contemporaine.

Bibliographie

Documents techniques

- S. Hodges et M. Harrison, White *paper : Demystifying RFID : principles and practicabilities*, octobre 2003 disponible sur le site http://www.autoidlabs.org/.

- The Association for the Automatic Identification and Data Capture Industry (AIM), *Draft paper on the characteristics of RFID-sytems*, juillet 2000 disponible sur le site http://www.aimglobal.org.

- K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification.*

- Harnessing Technology Project Phase I – *Research, RFID, a week long survey on the technology and its potential, Radio Frequency Identification*, Interaction Design Institute Ivrea Monday, March 04, 2002,http://www.interaction-ivrea.it

- Dr. Jeremy Landt, *Shrouds of Time*, *The history of RFID,* AIM Publication, 1er octobre 2001.

- AIM Inc. Frequency Forum White Paper Document, *Draft Paper on the Characteristics of RFID-Systems*, Juillet 2000, AIM Frequency Forums.

- Intermec, White paper, *The Write stuff: understanding the value of read/write functionality of RFID*.

- AutoID labs, différents documents techniques tous disponibles sur le site de l'AutoId center : http://www.autoidcenter.org

Documents juridiques

Ouvrages

- Sedallian Valérie, *Droit de l'internet,* collection AUI, Editions Net Press, Paris janvier 1997.

- Lamy, *Droit de l'informatique et des réseaux*, Editions Lamy, avril 2003.

- Bensoussan Alain, *Informatique, télécoms, internet*, Editions Francis Lefebvre, août 2001.

- Pedrot Philippe, *Traçabilité et responsabilité*, Editions Economica, mars 2003.

- Tabatoni Pierre, La protection de la vie privée dans la société d'information, Toms 1, 3, 4 et 5, Cahier des sciences morales et politiques, Editions Presse Universitaires de France, octobre 2000 (tome 1) et janvier 2002 (tomes3,4 et 5)

- Législation et réglementation, *Informatique et libertés*, Journaux Officiels, décembre 2003

Rapports

Rapport final de l'IST (Information Society Technology), *The opportunities ahead*, 2-4 octobre 2003, Milan Italie.

Rapport EUR 20823 EN, *Security and Privacy for the Citizen in the Post September 11 Digital Age: A Prospective Overview*

Technology Information and Privacy Commissioner Ontario, *Tag, You're It: Privacy Implications of RadioFrequency Identification (RFID)*, Ann Cavoukian, Ph.D.Commissioner February 2004.

CASPIAN, *Privacy and Societal Implications of RFID*, Katherine Albrecht, Consumers Against Supermarket Privacy Invasion and Numbering.

Global Business Dialogue on Electronic Commerce, *New York Recommendations 2003*, Summit 2003.

Conseil d'Etat, *internet et les réseaux numériques,* Les études du Conseil d'Etat, La Documentation Française, 2 juillet 1998

CNIL, *Rapport d'étude et de consultation publique, la cybersurveillance des salariés dans l'entreprise,* Mars 2001 disponible sur www.cnil.fr

CNIL, *Rapport la cybersurveillance sur les lieux de travail,* 5 février 2002 disponible sur www.cnil.fr.

CNIL, *21ème rapport d'activité*, la documentation Française, Paris 2001.

CNIL, *22ème rapport d'activité*, la documentation Française, Paris 2002.

CNIL, *23ème rapport d'activité*, la documentation Française, Paris 2003.

CNIL, Rapport sur les listes noires.

CNIL, Communication de M. Philippe Lemoine relative à la Radio-Identification (Radio-Tags ou RFIds).

23ème conférence internationale des commissaires à la protection des données, *Vie privée – Droits de l'homme*, Paris 24/26 septembre 2001, CNIL, éditions la documentation française, 2ème trimestre 2002.

Périodiques

Guide permanent droit et internet, éditions F. Lefebvre

Textes législatifs

Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Directive 95-46 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.

Directive 2002-58 du 12 juillet 2002 relative à la vie privée et aux communications électroniques.

Loi relative au traitement des données à caractère personnel du 6 août 2004 (2004-801) modifiant la loi du 6 janvier 1978 (transposant la directive 95-46).

Sites internet généralistes

www.juriscom.net

www.droit-ntic.org

www.droit-technologie.org

www.telecom.gouv.fr

www.internet.gouv.fr

www.legifrance.fr

www.clic-droit.com

www.europa.eu.int

Sites internet spécialisés

www.fing.org

www.aim.org

www.epcglobalinc.org

www.autoidcenter.org

www.rfidjournal.com

www.cnil.fr

www.epic.org

www.eff.org

www.spychips.com

www.wired.com

www.slashdot.org

www.zdnet.fr

www.tracenews.net

www.poletracabilite.com

www.rfidjournallive.com

www.contactlessnews.com