# RFID et Administration publique: Le citoyen sous surveillance?

**Anthony Hémond** †

*La préoccupation principale à l'égard du respect de la protection de la vie privée dans les environnements électroniques a trait à la vie privée informationnelle, c'est-à-dire à l'intérêt des personnes à l'égard des informations qui les concernent ou qui sont divulguées.* Professeur Pierre Trudel.[1]

## Introduction

Comme le souligne le Professeur Trudel, la vie privée informationnelle tient une place centrale dans les environnements électroniques.

Nous pouvons intégrer les puces RFID dans ces environnements.[2]

L'apparition de la technologie RFID remonte à la fin de la seconde guerre mondiale. Elle repose sur le principe physique d'une communication par voie électromagnétique.[3] La première application de cette technologie fut militaire, au sein de l'aviation, afin de pouvoir différencier les appareils alliés de ceux ennemis. Ce système était dénommé IFF[4] et il est toujours utilisé.

Dans les années 60, les puces RFID ont connu un nouvel essor avec leur utilisation commerciale dans la prévention des vols. Il s'agissait alors du système Electronic Article Surveillance ou EAS. Cette technologie continua d'évoluer progressivement.

Il fallu attendre les années 90 pour voir le véritable envol de ces puces RFID.

Depuis, l'intérêt pour ces puces n'a cessé de s'affirmer, à un tel point que très prochainement, des documents de l'Administration en seront dotés. Après l'e-administration,[5] nous allons connaître les e-passeports. Les États disposent du pouvoir d'établir les documents relatifs à l'identité des personnes.[6] Le passeport est un document d'identité officiel délivré par le gouvernement d'un État qui identifie son citoyen dans un autre pays. Lorsque ce citoyen voyage, il doit établir son identité aux frontières lors du passage des douanes. En effet, sous l'influence américaine les passeports vont prochainement être équipés de puces RFID.

Au-delà de la question de savoir si l'utilisation de cette technologie est nécessaire, il faut plutôt et en priorité s'intéresser aux interrogations que soulève la protection des données personnelles contenues dans les différents documents de l'Administration qui utilisent ces puces RFID. En l'occurrence, ces puces RFID ne vont-elles pas porter atteinte à la vie privée des citoyens? Les lois protégeant les données personnelles sont-elles suffisamment efficaces?

Il ne s'agit pas d'un roman de science fiction comme certains peuvent le croire. Le déploiement de ces e-passeports a bel et bien commencé, notamment en Malaisie depuis 1998. En 2003, une nouvelle génération de passeports a vu le jour avec l'intégration d'empreintes digitales.

Lorsque les gouvernements et l'Administration se lancent dans la mise en place d'une nouvelle technologie, il leur faut, au préalable, analyser les enjeux et les risques de ce déploiement.

Tel sera l'essentiel de nos développements. Nous verrons comment, notamment à travers la mise en place du e-passeport, la technologie RFID peut être intégrée au sein de l'Administration. Le choix de cette nouvelle génération de passeports n'est pas anodin : si dans certains domaines les données qu'ils contiennent sont précieuses, dans d'autres, notamment celui de la santé, les informations sur les personnes sont très sensibles. Il faut donc maîtriser les risques liés à la diffusion ou à la non diffusion de ces informations.

Ainsi, nous verrons dans un premier temps où en est la technologie RFID aujourd'hui (I), avant de voir que cette technologie peut être dangereuse pour la vie privée (II).

## I. La technologie RFID aujourd'hui

Pour bien comprendre la technologie RFID, nous devons commencer par en expliquer les principes de fonctionnement (A) afin de mesurer ses implications présentes et futures sur la protection de la vie privée. Ensuite, nous nous intéresserons aux lois protégeant les données personnelles (B) pour saisir les limites de cette technologie RFID sur la collecte d'informations nomina-

†Anthony Hémond has a French Master's degree in Law in Immaterial Creations at the University of Montpellier, and an LL.M. in Information Technology at the University of Montreal. 

tives, ce qui nous amènera à voir quels sont les enjeux de cette technologie naissante.

## A. Les principes de fonctionnement de la technologie RFID

Cette technologie propose diverses options techniques.

Aussi, nous verrons quelles sont les composantes de cette technologie (1), puis les choix qui s'offrent à l'Administration pour l'utilisation de cette technologie (2).

### 1. Les composants de la technologie RFID

En premier lieu, dévoilons le fonctionnement de la technologie RFID.[7]

La technologie RFID en elle-même repose sur l'utilisation de trois composantes : une *puce* qui est insérée dans l'objet, une *antenne* et un *lecteur* capable de lire les informations contenues dans la puce.

La puce peut contenir des informations, voire des données sur le document ou l'objet dans lequel elle est intégrée. Dans le cadre de l'utilisation commerciale de ces puces, celles-ci s'apparentent au code barre. Toutefois, les données contenues dans ces puces peuvent être d'une toute autre nature, par exemple, de nature biométrique.[8]

L'antenne se situe sur la puce et transmet les données de cette puce au lecteur sous forme d'ondes radio. La combinaison antenne/puce est généralement appelée marqueur.

Le lecteur[9] dispose également de sa propre antenne pour communiquer avec le marqueur. Il faut noter que toute personne disposant du lecteur adéquat peut scanner les informations sur les marqueurs. Par contre, cette technologie peut utiliser la cryptographie[10] pour rendre les données plus sûres. L'avantage de la technologie RFID repose sur le fait que le lecteur n'a pas besoin de contact physique avec le marqueur. De plus, un seul lecteur peut lire tous les marqueurs situés dans son rayon d'action.

Le lecteur est relié à un ordinateur qui comprend une base de données pour identifier les informations.[11]

Figure: Structure of an RFID System

Les puces insérées dans les objets peuvent être de trois catégories différentes : passives, semi-passives ou actives.

### 2. Les choix possibles de cette technologie

— Les puces dites passives :[12]

L'énergie indispensable à la transmission des données devra être fournie à ce type de puce. Autrement dit, si ces puces ne sont pas activées par le lecteur, elles n'émettent aucun signal. Le lecteur émet un champ électromagnétique qui les rend actives. L'intensité de ce champ est limitée par des lois nationales ou internationales.[13] Ce qu'il faut retenir de la technologie dite passive, c'est que ces puces restent muettes tant qu'elles n'entrent pas dans un champ électromagnétique émis par le lecteur. En outre, plus on s'éloigne du lecteur, plus l'intensité du champ diminue. Ainsi, si ces puces ont besoin de peu d'énergie pour être activées et lues, alors la distance de fonctionnement par rapport au lecteur peut être plus grande. La taille de l'antenne se trouvant sur ces puces détermine leur distance de fonctionnement et leur puissance, mais il faut également tenir compte de la sensibilité de l'antenne ou du lecteur. La distance de fonctionnement théorique pour les puces dites passives est d'environ 20 mètres entre elles et le lecteur.[14] Il semblerait toutefois que ces prévisions soient optimistes ou du moins très théoriques. En pratique, la distance de fonctionnement serait plutôt de l'ordre de 10 mètres dans le meilleur scénario, l'idéal se situant entre 3 et 5 mètres.[15] Le prix moyen de ces puces (en tenant compte du fait que celui-ci peut varier en fonction de la mémoire des puces, et de leur capacité de cryptage des données) est de l'ordre de 20 cents U.S.[16]

— Les puces dites semi passives :

À la différence des puces passives, celles-ci disposent d'une batterie permettant de stocker certaines informations comme par exemple la température ambiante.

— Les puces dites actives :

Celles-ci transmettent de façon continue les données, même si aucun lecteur n'est à proximité. Ces puces sont donc équipées de batteries, les rendant ainsi plus lourdes et plus onéreuses à l'achat (environ 20 dollars U.S.).[17]

Il convient d'évoquer une autre caractéristique importante de cette technologie. Un choix concernant les marqueurs s'offre également à l'utilisateur, soit les marqueurs à lecture seulement ou à lecture/écriture. Il s'agit de la capacité du marqueur de recevoir ou non des données. Si le marqueur est à lecture seulement, aucune donnée ne pourra y être ajoutée après son incorporation au support. Les données contenues ne peuvent être modifiées, ce qui en fait un marqueur sécuritaire. À la différence des marqueurs lecture/écriture, il faut changer de marqueur pour pouvoir modifier les données. Également, ils sont plus dispendieux[18] et possèdent une portée de lecture plus réduite, ce qui constituent les deux inconvénients notoires de cette technologie. Dans le cadre de son utilisation par l'Administration, les données qu'il contient peuvent être de différents ordres et peuvent toucher, par exemple, l'identité des personnes dans le cas d'une carte d'identité,[19] voir même porter sur des infor-

mations liées à la santé des personnes. Il existe des marqueurs ayant une mémoire étendue qui leur permet de contenir suffisamment d'informations pour que le lecteur n'ait pas besoin de se connecter à une base de données pour identifier les données et les reconnaître. D'autres marqueurs ont la possibilité de communiquer entre eux.[20] La capacité de mémoire de ces marqueurs varie de quelques octets[21] à des dizaines voir des centaines de kilo-octets, pour des mémoires de type EEPROM[22] pour les marqueurs passifs ou SRAM[23] pour les marqueurs actifs.[24]

Il existe également des cartes intelligentes à base de puces RFID appelées « Contactless smart-cards » équipées d'un microprocesseur, ainsi que d'un logiciel d'exploitation. Ces systèmes ont les plus grandes capacités de mémoire. En outre, des fonctionnalités complexes peuvent être intégrées dans ces cartes. Des programmes peuvent être enregistrés dans la mémoire du marqueur et exécutés par le microprocesseur. Néanmoins, à cause de la grande consommation d'énergie de ces puces, la portée de celles-ci est limitée à quelques centimètres. Ce type de cartes est envisagé pour les pièces d'identité ou les cartes de santé.

Nous voyons donc que ces puces RFID peuvent avoir des utilisations futures intéressantes pour l'Administration, notamment en matière de sécurité[25] , mais également dans le domaine médical pour informer les médecins des antécédents médicaux, dans les bibliothèques municipales pour remplacer les codes barre[26] ou bien dans les cartes étudiantes d'écoles primaires[27] afin de savoir où se trouvent les élèves.

Ces puces, en contenant des données personnelles (voir même nominatives) présentent un risque pour la vie privée des personnes.

Il nous faut donc traiter des lois spécifiques à la protection des données personnelles.

## B. Les grands principes de protection des données personnelles

Nous commencerons par évoquer les grands principes de protection des données personnelles, en appuyant notre étude sur les similitudes entre les droits canadien, européen, français et américain (1). Puis, nous mettrons en correlation les marqueurs RFID avec les données personnelles (2).

### 1. La protection des données personnelles

Tout d'abord, qu'entend-t-on par données personnelles?

Appelées « données nominatives » en France,[28] la loi canadienne traite plutôt de « renseignements personnels ».[29] La loi américaine, quant à elle, parle d' « enregistrement » ou de « systèmes d'enregistrement »,[30] la Directive Européenne 95/46/CE[31] utilise le terme de « données personnelles » et l'Organisation de Coopération et de Développement Economiques (ci-après O.C.D.E.) parle de « données de caractère personnel ».[32]

De façon générale, la définition de données personnelles pourrait être : toute information qui permet d'identifier un individu.

Voyons désormais comment s'articule la protection de ces données personnelles.

Nous partirons de la Recommandation de l'O.C.D.E. sur les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel,[33] pour cerner quels sont les grands principes de protection des données personnelles.

Ainsi l'O.C.D.E. précise :

« Reconnaissant :

— que, bien que les législations et politiques nationales puissent différer, il est de *l'intérêt commun des pays membres de protéger la vie privée et les libertés individuelles* et de *concilier des valeurs à la fois fondamentales et antagonistes, telles que le respect de la vie privée et la libre circulation de l'information*;

— que le traitement automatique et les flux transfrontières de données de caractère personnel créent de nouvelles formes de relations entre pays et exigent l'instauration de règles et pratiques compatibles ».[34]

Il ressort que l'Administration récolte, pour ses besoins, bon nombre d'informations sur les citoyens. Nous citerons, entre autre, les informations médicales dans les hôpitaux publics, les informations des services des impôts, celles de l'état-civil avec l'établissement des pièces d'identité, comme la carte Soleil et la carte d'assuré social au Canada.

L'Administration est assujettie à des règles sur la protection de ces données. Toutefois, celles-ci doivent pouvoir circuler à l'intérieur de ses différentes branches, sans quoi l'Administration peut se retrouver bloquée. L'Administration se doit donc de gérer ces intérêts antagonistes, et d'appliquer scrupuleusement les règles concernant la vie privée tout en facilitant la circulation des données à l'interne.

Les recommandations de l'O.C.D.E. visent à harmoniser entre-elles les législations concernant la protection des données personnelles. Il ressort que la base de la protection des données personnelles, ou du moins les grands principes, sont édictés par l'O.C.D.E. Ces lignes directrices s'appliquant au secteur public,[35] elles nous sont d'autant plus utiles.

Intéressons-nous aux grands principes édictés par l'O.C.D.E. Ils sont au nombre de neuf :[36]

— limitation en matière de collecte,

— qualité des données,

— spécification des finalités,

— limitation de l'utilisation,

— garanties de sécurité,

— transparence,

— participation individuelle,

— responsabilité,

— flux transfrontières des données.

Ces principes sont la base minimale de la protection des données personnelles. Il s'avère que les pays membres de l'O.C.D.E. les ont intégrés dans leurs législations. Nous ne détaillerons pas tous ces principes, mais en privilégierons certains, en étudiant les bases communes des lois américaine, canadienne, et française.

Aux États-Unis, le *Privacy Act de 1974*[37] établit les principes de la protection des données personnelles.

Au Canada, la protection des renseignements personnels dans le secteur public s'articule autour de deux lois : la *Loi sur la protection des renseignements personnels* et la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.[38]

En France, il s'agit de la loi dite « informatique et libertés » de 1978, qui a par la suite été modifiée[39] en vue de l'intégration de la Directive Européenne 95/46/CE. Cette Directive pose, elle aussi les grands principes de protection des données personnelles. Nous traiterons du droit européen par le biais de l'étude du droit français, puisque les Directives doivent être intégrées par les États européens afin d'avoir un effet contraignant.

Attardons-nous aux similitudes des lois canadienne, française et américaine.

Si les personnes dont les données à caractère personnel sont recueillies disposent de droits, le gardien des données, quant à lui, est assujetti à certaines obligations.

Nous pouvons mentionner le droit d'accès[40] aux données recueillies, reconnu à la personne sujette à la collecte, c'est-à-dire qu'une personne peut accéder aux données qui ont été recueillies sur elle, et en connaître la teneur. Un droit de rectification lui est également reconnu.[41] La personne peut aussi s'opposer au traitement de données personnelles,[42] ce qui revient à l'obligation d'obtenir son consentement. C'est-à-dire que la personne doit consentir à la collecte d'informations la concernant. Il existe cependant des cas où la personne ne peut s'opposer à cette collecte, notamment dans le cadre d'affaires concernant la sécurité de l'État. La personne doit connaître également la finalité du traitement, c'est-à-dire la raison pour laquelle les données sont recueillies.[43] autrement dit l'utilisation qui sera faite des données.

Le gardien des données (le collecteur de données) est, quant à lui, assujetti à des obligations. Nous n'évoquerons que celles relatives à nos développements concernant les puces RFID. Ainsi, il existe une obligation quant à la *qualité* des données, à leur exactitude. Il est également nécessaire d'obtenir le *consentement* des personnes, comme nous l'avons vu. De même, il est indispensable d'informer la personne sujette à la collecte des données. Enfin, ce qui nous préoccupe le plus avec les puces RFID sont les obligations de *confidentialité* et de *sécurité* des données. Ainsi l'O.C.D.E., tout comme les différentes législations que nous venons de voir,[44] réaffirme ce besoin de sécurité pour ces données.[45]

Nous connaissons désormais les droits et obligations relatifs au traitement de données personnelles. La question est maintenant de savoir si les puces RFID sont assujetties à ces règles.

## 2. Les puces RFID assujetties aux règles relatives à la protection des données personnelles

La première question à se poser est de savoir si les puces RFID peuvent contenir des données personnelles. Nous avons vu que les puces disposent de mémoire permettant le stockage de données. Dans cette hypothèse, il faut que les données permettent d'identifier les individus pour que les puces soient sujettes aux dispositions que nous venons de voir. Des informations comme le nom patronymique entrent dans cette catégorie, tout comme l'âge, la race, la couleur des yeux, mais également des numéros tels que celui d'assuré social.

Les utilisations souhaitées ou requises par l'Administration nous amènent à nous interroger. En effet, que ce soit en France avec l'instauration de cartes d'identité à puces[46] ou aux États-unis avec le passeport électronique,[47] les données insérées dans ces documents munis de puces RFID sont des données nominatives relevant du régime de protection des diverses législations. Il faut donc que l'Administration veille à respecter les règles relatives à la protection des données personnelles.

D'autres projets sont en cours d'élaboration pour ces puces RFID, notamment leur utilisation dans le domaine de la santé. Des puces pourraient être placées sous la peau du patient et pourraient contenir des informations médicales le concernant, par exemple, les antécédents allergiques d'un patient.[48] Nous pouvons d'ailleurs noter que l'Administration américaine s'est déjà prononcée sur l'incorporation de telles puces dans le corps humain, en autorisant leur insertion sous la peau.[49]

Les puces pourraient également servir à la localisation de personnes. Pensons au cas d'épidémie de type Syndrome Respiratoire Aigu Sévère (ci-après SRAS) qui a sévit en Asie. Tout le personnel médical serait équipé de puces permettant de savoir quelles personnes ont été en contact avec les malades. Il serait alors possible d'éviter les contaminations futures, en connaissant les déplacements des membres du personnel médical.

Dans ces différents exemples, les informations contenues dans les puces concernent les individus porteurs de ces puces.

Or, l'Administration peut décider d'insérer les puces dans des objets, par exemple, des livres. Dans cette hypothèse, les informations ne seraient pas personnelles,

mais pourraient tout de même être intrusives pour la vie privée. Ceci pourrait survenir, notamment par l'incorporation de puces RFID dans des billets de banque. Dès lors, il pourrait être possible de savoir quelles utilisations ont été faites des billets de banque par la personne possédant ces billets « marqués ».[50] Ici, l'intérêt d'utiliser des puces n'est pas de porter atteinte à la vie privée des gens, mais plutôt d'éviter la contrefaçon de monnaie en la rendant plus sécuritaire.

L'intérêt pour ces puces se fait grandissant. Cependant, beaucoup d'organisations mettent de l'avant les risques pour la vie privée d'un abus éventuel de l'utilisation de ces puces. Nos propos ne viseront pas à accompagner cette vision Orwellienne d'un monde sous surveillance. Ces puces peuvent être utiles, mais doivent respecter les lois protégeant la vie privée. Voyons donc les risques que représentent ces puces pour la vie privée.

## II. Une technologie dangereuse pour la vie privée

Nous avons vu que les puces RFID relèvent de la législation sur la protection des données personnelles si elles renferment des données permettant d'identifier un individu. Nous allons envisager les risques de cette technologie (A), puis voir quelles sont les solutions possibles pour éviter la paranoïa entourant ces puces RFID (B).

### A. Les risques de la technologie RFID

Lorsque l'Administration envisage la mise en place d'un nouveau passeport électronique, elle se doit de procéder, au préalable, à une analyse de la gestion des risques inhérents à ce nouveau passeport. Nous verrons, à travers la méthodologie développée par le Professeur Trudel,[51] comment l'Administration, qu'elles soient américaine, canadienne ou européenne peut intégrer ce passeport électronique. Comment gérer les risques d'atteintes au droit des personnes? Nous préciserons donc que la sécurisation des données est l'enjeu principal à la mise en place des puces RFID (1), avant de dresser un bilan des risques de cette technologie applicables à tous les secteurs de l'Administration (2).

#### 1. La sécurité des données : l'enjeu principal des puces RFID

La sécurisation des données doit être l'enjeu principal de cette technologie pour que les administrés aient confiance aux RFID.

Néanmoins, un autre enjeu capital pour l'Administration est celui de la transparence dans l'utilisation de ces puces. En effet, ces puces sont principalement utilisées pour garantir l'authenticité des e-passeports, en d'empêchant ou en réduisant la contrefaçon. Cependant, la finalité de cette technologie ne doit pas être détournée pour servir d'autres intérêts comme la « traçabilité » des administrés.

Il est indispensable que ce passeport soit en conformité avec les exigences de la loi, autrement dit, que l'Administration assure la qualité de l'information liée à ce document,[52] mais aussi que les intéressés bénéficient des lois sur la protection des renseignements personnels, ce qui signifie que le passeport électronique doit être conforme aux règles et principes édictés par les lois sur la protection des données personnelles.

Ainsi, sans revenir sur les grands principes qui ont été présentés précédemment, le risque majeur soulevé par le passeport électronique est la *sécurité* des données qu'il contient, donc les données doivent impérativement être protégées. Il s'agit là d'une obligation légale.[53]

Nous mentionnerons également, à ce stade de nos développements le principe de précaution. En effet, ce principe impose que les informations contenues dans le passeport soient protégées, par exemple au moyen de la cryptographie.

Précédemment, nous avons évoqué le choix possible qui s'offre à l'Administration d'opter pour des puces à lecture seulement ou lecture/écriture. Or, il nous semble important de souligner que si l'Administration choisit les puces à lecture seulement, elle s'expose à des risques d'atteintes à la vie privée bien moins importants que si elle choisit des puces à lecture/écriture, puisque dans le deuxième cas, un « pirate » peut potentiellement procéder à l'inscription de données sur le passeport, voire le falsifier complètement.

Une des failles existantes est l'accès aux informations contenues dans le passeport, à l'insu de l'individu porteur du passeport. Il s'agit d'un accès clandestin aux informations ou « clandestine skimming »[54] et ce risque se trouve accentué lors de l'utilisation de puces de type lecture/écriture. On peut envisager que cet accès frauduleux puisse s'accompagner d'atteintes additionnelles, telles que le suivi des déplacements d'une personne grâce au numéro unique contenu dans le passeport,[55] le clonage du passeport,[56] l'interception des communications entre la puce et le lecteur (« eavesdropping on authorized transactions »),[57] et l'utilisation des données biométriques[58] sensibles contenues dans le passeport.[59]

Attardons-nous un instant à envisager ces menaces.

— L'accès clandestin aux données

Il existe en effet un risque que toute personne équipée d'un lecteur puisse avoir accès aux données contenues dans le passeport sans que le porteur de ce passeport n'en soit informé. Le porteur ne peut donc consentir à ce que ses données soient transmises. Ceci est contraire aux principes des différentes lois en matière de protection des données personnelles. Pour réfuter cette possibilité de lecture à distance des données par un tiers

non autorisé, l'Administration américaine a avancé l'argument que les porteurs de lecteurs de puces seraient identifiés, puisque l'équipement nécessaire à la lecture des puces est trop encombrant pour passer inaperçu. Néanmoins, selon certaines sources, il semblerait qu'un simple assistant personnel de type PDA avec un logiciel puisse suffire à lire des puces RFID.[60]

— Le suivi des déplacements d'une personne

Les passeports électroniques seront munis d'un identifiant unique, un numéro attribué à la puce contenue dans le passeport. Ainsi, chaque porteur d'une puce RFID sera identifiable. Le problème restera entier quant à ce numéro qui pourra permettre de suivre les déplacements de cette puce et donc, par extension, de la personne porteuse du passeport, puisque cela semble possible sans qu'il soit nécessaire de lire les données contenues dans la puce elle-même.

— L'interception des données

Les données transmises par la puce au lecteur pendant la phase de lecture peuvent être interceptées par un tiers. Il est donc nécessaire de rendre cette phase sécuritaire.[61]

— Le vol des données biométriques

Il s'agit là, à notre avis, d'un faux problème, mais nous tenterons tout de même de l'expliquer. Ces données servent à vérifier si le porteur du passeport est bien la personne dont les données biométriques sont contenues dans le passeport.[62] Ces données sont principalement la reconnaissance faciale, l'iris de l'œil ou encore les empreintes digitales. Nous sommes donc encore bien loin des romans de science fiction de Philip K. Dick[63] où il est question de greffe d'iris permettant ensuite l'accès à ces données. [Dans cette hypothèse, il nous semble que pour réduire les risques, il faudrait que l'utilisation des données biométriques soit couplée avec des bases de données regroupant toutes les données biométriques pour pouvoir identifier les personnes. Ainsi la lecture seule des données ne permettraient pas d'identifier une personne, il serait nécessaire d'accéder à un outil externe : la base de données.]

Dressons maintenant le bilan des risques potentiels occasionnés par les puces RFID.

## 2. Bilan général des risques présentés par les puces RFID

On peut identifier, à notre avis, quatre risques liés au passeport électronique et, de manière générale, à l'utilisation des puces RFID. Nous pensons d'abord aux risques liés à la *sécurité* des informations contenues dans les passeports. En effet, les informations contenues dans les puces RFID doivent être protégées afin d'éviter toute lecture des données par une personne non autorisée. Le caractère « sensible » des informations récoltées dans certains domaines (le champ médical notamment), risque de mener au développement de systèmes sécuritaires pour ces données,[64] puisque, par exemple, l'utilisation d'une puce sous-cutanée permettrait d'obtenir toutes les informations relatives à la santé d'une personne, domaine qui relève bien du domaine de la vie privée.

De plus, si l'on revient aux grands principes de protection des données personnelles, le *consentement de la personne* pour la collecte des données est un élément primordial. Or, les puces peuvent communiquer avec les lecteurs sans que le porteur de la puce ne soit au courant de l'accès aux données. Ainsi, un manque de transparence existe quant à la collecte de ces données. Il faut donc prévoir un dispositif permettant au porteur de donner son consentement préalablement à la lecture des données ou, dans les cas où le consentement n'est pas obligatoire, informer le porteur que les données seront lues.

Un autre risque est relié au consentement de la personne s'avère être la *finalité* de la collecte.[65] En effet, pour exprimer un consentement éclairé encore faut-il savoir pourquoi les données sont récoltées?

Dans le cadre des contrôles liés à la lecture des passeports par les agents des douanes, il semble que la finalité du traitement soit de s'assurer que la personne titulaire du passeport est la bonne. Cependant, les données pouvant parfois être récoltées à l'insu de la personne, la finalité de la collecte peut ne pas être révélée. Nous nous retrouvons dans l'hypothèse où des personnes malveillantes peuvent rassembler des informations pour leur propre intérêt. Cela peut devenir dangereux et se rapprocher de « l'État policier » décrit dans le célèbre roman *1984* de George Orwell.[66] En effet, le principe de finalité repose sur la connaissance de l'utilisation des données. Toute personne doit savoir dans quel but les informations la concernant sont récoltées, cela afin d'éviter que des informations ne soient transmises à des tiers, ou ne desservent des objectifs autres que ceux pour lesquels le consentement a été donné. Ce principe vise à protéger les individus contre l'utilisation abusive de leurs données personnelles.

Nous allons évoquer une particularité du droit canadien : les administrés sont moins bien protégés contre l'Administration que contre les entreprises privées pouvant faire la collecte d'informations. En cela, nous faisons référence aux paroles du Commissaire à la vie privée du Canada qui a précisé :

> «Enfin, il existe une certaine différence en ce qui concerne les limites imposées à la collecte de renseignements personnels. La *Loi sur la protection des renseignements personnels* limite les institutions gouvernementales à la collecte de renseignements personnels directement liés aux programmes qu'elles mettent en oeuvre. « Directement liés » ne veut pas dire la même chose que « nécessaires ». Par contre, la *Loi sur la protection des renseignements personnels et les documents électroniques* exige que les organismes ne recueillent des renseignements personnels « qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. À notre avis, voilà une affirmation beaucoup plus forte de notre droit fondamental à la vie privée ».[67]

En effet, cette disposition de la loi canadienne offre à l'Administration une grande facilité d'intrusion dans la vie privée des personnes. Le terme « directement lié » dans la loi canadienne est beaucoup trop vague. Bon nombre de renseignements peuvent être directement liés aux programmes mis en place et il existe un risque accru avec la mise en place de systèmes tels que les puces RFID. L'Administration pourrait demander nombre d'informations liées au service mis en place et ces informations pourraient être utilisées, voire détournées de leur finalité. Ces risques sont relatifs et il n'est pas de l'intérêt de l'Administration de détourner les renseignements, puisque ceci engendrerait une perte de confiance non seulement dans l'Administration mais également dans l'État.

Enfin un autre risque découlant de l'utilisation de ces puces RFID est qu'il est désormais *possible de suivre un citoyen*. Si l'on prend l'exemple de la France, l'État dispose du droit de délivrance des titres d'identité comme celui du contrôle de l'identité. Il s'agit de prérogatives régaliennes. La France connaît, comme d'autres pays européens, la carte d'identité. Dans l'avenir, celle-ci pourra être munie de puces RFID. Sachant qu'un individu doit pouvoir démontrer son identité en tout temps à la demande de la police en fournissant sa carte d'identité, il sera possible de suivre les déplacements de chaque individu si les cartes sont munies d'une puce RFID. Devant cette hypothèse, le droit de chaque citoyen au respect de sa vie privée doit être protégé. Ainsi, les informations contenues dans la carte d'identité ou la puce RFID ne doivent être activées que sous le contrôle du titulaire de cette carte.

Par ailleurs, le suivi des déplacements d'une personne peut être l'objet même de l'utilisation des puces RFID. En effet, dans le cadre d'épidémies, comme nous l'avons vu précédemment avec le SRAS, il peut être utile de savoir quelles personnes ont été en contact avec les malades. Dans ce cas précis, la « traçabilité » n'est pas un risque afférent mais est le but poursuivi. Cependant, il faut tenir compte de la *finalité* de la collecte. Ainsi, l'accès aux informations permettant de retracer le parcours d'une personne ne devra s'appliquer que pour prévenir un risque d'épidémie, et non pour surveiller les personnes.

Voyons désormais quelles sont les solutions à apporter pour encadrer l'utilisation de ces puces RFID.

## B. Des solutions aux problématiques soulevées par les puces RFID

Nous voyons deux types de solutions visant un objectif commun : celui de l'amélioration de l'efficacité de la sanction lors d'atteintes à la vie privée et non l'accroissement de la vie privée. Les solutions envisageables sont donc d'une part, une intervention législative pour encadrer l'utilisation des puces RFID (1) et d'autre part, l'utilisation de solutions techniques (2).

### 1. Un encadrement de l'utilisation des puces RFID par la loi

Une réponse possible à l'utilisation des puces RFID est l'encadrement de ces puces par des mesures législatives appropriées. Cela passe par un renforcement des règles existantes en matière de consentement et de divulgation d'information à la personne visée par la collecte, de même qu'une garantie accrue en matière de sécurité des données, ainsi qu'une reconnaissance du droit de l'administré de s'opposer à la collecte.

Les Directives[68] européennes, tout comme la loi française, n'ont pas besoin d'être modifiées pour répondre au défi de la technologie RFID. Si l'on regarde attentivement le document fourni par le groupe de travail sur l'Article 29,[69] on s'aperçoit qu'il procède à l'examen des puces au regard des différentes Directives en matière de protection de la vie privée. Il ressort de ce document que les puces RFID n'amènent pas de nouvelle problématique à la protection des données personnelles.

Nous nous devons de noter que dans le cas du Canada, il est question de modifier la *Loi sur la protection des renseignements personnels* pour la rapprocher de son homologue du secteur privé, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Cette dernière a bénéficié de l'expérience acquise lors de l'application de la *Loi sur la protection des renseignements personnels*. Bref, la vie privée des Canadiens et Canadiennes ainsi que leurs renseignements personnels sont mieux protégés dans le secteur privé que dans le secteur public selon la Commissaire à la vie privée du Canada.[70]

Les États-Unis vont également renforcer leur législation [fédérale], mais cette fois, en ce qui concerne les collectes de données par les entreprises privées. En effet, il existe un projet de réforme du *Privacy Act* dans lequel certaines modifications doivent être apportées. Il y est notamment question de redéfinir les informations personnelles identifiantes,[71] de renforcer la protection des données médicales,[72] tout comme celle du numéro d'assuré social.[73] Les États envisagent eux aussi d'encadrer l'utilisation de cette technologie. Celle-ci ne doit pas se retrouver dans tous les secteurs de l'Administration. Ainsi, il est même envisagé, en Californie, d'interdire l'utilisation des puces RFID pour tout document permettant l'identification des personnes.[74] Il s'agit là d'une solution extrême, mais l'on peut rappeler qu'un projet similaire avait été déposé pour empêcher l'établissement de puces RFID dans le secteur privé, projet ayant vite été avorté sous la pression du secteur industriel.[75]

La doctrine américaine avance également de nouvelles pistes pour la protection des données personnelles. Le Professeur Solove propose la mise en place d'une nouvelle architecture pour la protection des don-

nées personnelles :[76] la participation et la responsabilité. Cette théorie se fonde sur les *Fair Information Practices* apparues en 1973.[77] La proposition du Professeur Solove consiste d'une part à accroître la participation des personnes à la collecte des données, et d'autre part, à accentuer la responsabilité des organismes qui recueillent les informations.

En somme, il nous semble que l'utilisation des puces RFID amène l'administré à prendre conscience de ses droits quant à ses données personnelles et à les exercer. Mais, si un droit n'est plus utilisé, devient-il pour autant désuet?

Une meilleure information du citoyen est nécessaire pour lui faire prendre conscience des risques potentiels de cette technologie sans pour autant le faire succomber à une paranoïa certaine. Nous rejoignons les idées du Professeur Solove sur ce point.

En ce sens, il nous semble que le groupe de travail sur l'Article 29 en Europe peut jouer un rôle de catalyseur pour la prise de conscience des droits existants.

En outre, les organisations de protection de la vie privée ont également un rôle à jouer dans l'information du citoyen.[78] En effet, le citoyen ignore bien souvent ses droits en ce domaine. Or, nul n'est censé ignorer la loi. La mise en place du passeport électronique aux États-Unis est un exemple d'initiative dans laquelle les organisations de protection de la vie privée ont un rôle décisif à jouer quant à l'éducation des citoyens, tout en les informant également que la loi actuelle, notamment aux États-Unis, offre une protection suffisante.

L'International Civil Aviation Organization (ci-après ICAO) a donné des indications quant aux spécifications techniques requises pour les puces RFID utilisées dans les passeports électroniques.[79] L'ICAO a par la suite fourni un nouveau document, beaucoup plus complet, sur les spécifications techniques des documents de voyage munis de puces RFID.[80]

Il s'avère que l'Administration américaine, dans sa volonté d'implantation du passeport électronique, n'a pas suivi les recommandations de l'ICAO. Par conséquent, le Département d'État qui est à la base de ce projet a vu s'élever bon nombre de critiques, notamment sur l'existence de failles de sécurité et sur l'absence de cryptographie pour la sécurisation des données.[81] Devant l'affluence des critiques, le Département d'État américain a dû, d'urgence, modifier son projet.[82] Cette affaire illustre bien l'importance que peuvent avoir les organisations de protection de la vie privée.

De plus, nous pensons qu'il existe une certaine neutralité technologique dans les lois protégeant la vie privée. Les modifications législatives apportées pour englober l'Internet et les réseaux de communication de façon générale, prévoient une protection suffisante pour toutes les nouvelles technologies comme celles des puces RFID. S'il advenait que l'utilisation de cette technologie devait être encadrée spécifiquement par la loi, cela mettrait fin à la neutralité technologique des lois protégeant la vie privée. Il faudrait alors légiférer sur chaque technologie intrusive à la vie privée. Or, il nous semble que ce sont aux technologies à s'adapter aux règles sur la protection des données personnelles et non l'inverse.

Il ressort de nos développements qu'il n'est nul besoin de légiférer pour encadrer les puces RFID, à condition que les lois spécifiques en matière de protection des données personnelles aient été modifiées avec l'avènement d'Internet, ce qui n'est pas le cas avec les législations canadienne et américaine pour lesquelles, sans nul doute, un besoin d'actualisation se fait ressentir, sans pour autant qu'il soit nécessaire de les modifier complètement. Il nous semble que la réponse apportée pour la sécurisation des données des puces RFID sera une réponse d'ordre technique.

## 2. Des solutions techniques aux puces RFID

Nous ferons ici référence à la célèbre phrase de Charles Clark : « The answer to the machine is in the machine ».[83] Autrement dit, les puces RFID posent un problème technique mais ne remettent pas en cause les lois relatives à la protection des données personnelles. Ainsi, la technologie doit se conformer aux règles en vigueur. Il est donc nécessaire d'apporter des solutions techniques et non législatives au problème de la mise en place des puces RFID.

Comme le préconise l'ICAO pour les passeports, il existe des moyens efficaces pour permettre aux personnes d'exercer leurs droits relatifs à la protection des données personnelles.

Prenons l'exemple de la nécessité d'informer les personnes quant à la lecture des données. Nous savons que les puces RFID peuvent être lues à distance. Or la lecture de ces données ne devrait pouvoir s'effectuer que si la personne consent à présenter son passeport. Même si la personne ne peut faire valoir son droit d'opposition, elle devrait toutefois être informée que ses informations vont être lues par un lecteur.

L'ICAO préconise donc l'utilisation d'une nouvelle technologie dénommée Basic Access Control (BAC),[84] dans laquelle les données contenues dans les puces sont « verrouillées » et indisponibles pour tous les lecteurs qui ne disposent pas d'une clef spéciale ou d'un mot de passe « déverrouillant » l'accès aux informations. Or, pour obtenir une clef, le douanier, par exemple, devra « scanner » la page du passeport où se trouve la photo de l'individu. On assiste donc ici à l'abandon de la lecture à distance des données. Par la suite, les données seront « hachées »[85] pour créer une clef unique permettant l'identification du lecteur et le déverrouillage des données contenues sur le passeport.

Cette solution technique présente de nombreux avantages, comme l'impossibilité de lire des données sans que la personne n'en soit informée (ou n'y ait consenti), ce qui comme nous l'avons vu, serait contraire à

son droit à l'information. En outre, un autre avantage de cette solution est d'interdire l'interception des données par tout autre lecteur pendant la lecture par le lecteur autorisé. En effet la cryptographie rend illisible les données qui seraient interceptées par un lecteur non autorisé.

Comme toute solution technique, celle-ci n'est pas non plus sûre à 100%. Tel est le risque de toute nouvelle technologie.[86] En effet, il existera toujours un pirate informatique ingénieux qui réussira à contourner les protections. La question est de savoir ce que l'on recherche avec la mise en place d'un passeport électronique. Est-ce un contrôle plus sûr des passagers? Est-ce empêcher la contrefaçon de documents dont l'État est garant?

Toutefois, même dans l'univers physique, précisons que dans le monde du papier, les risques de contrefaçon nous semblent bien supérieurs. Les États-Unis brandissent le passeport électronique comme un moyen de lutter contre le terrorisme.[87] Cependant, nous devons nous garder de telles affirmations, car si la technologie peut restreindre les capacités de contrefaçon, cela ne reste valable qu'un certain temps. De plus, si l'on se remémore les évènements tragiques du 11 septembre 2001, il ressort que les pirates de l'air avaient utilisé de vrais passeports. S'il est vrai que la technologie pourrait permettre d'identifier plus facilement, grâce aux bases de données avec lesquelles sont couplées les passeports, les personnes dangereuses, là encore faudrait-il que ces personnes aient été, au préalable, identifiées comme telles.

## Conclusion

De façon générale, la question qui se pose ici est celle des risques de la mise en place d'une nouvelle technologie. Cela n'a, en soit, rien de nouveau. La révolution numérique a entraîné de nombreux changements au sein de l'Administration, comme par exemple, la numérisation des documents, et leur diffusion.

Nous retrouvons toujours d'un côté les opposants à la transformation technologique de l'Administration et de l'autre, ses fervents. Mais ici, la question est plus sensible dès que l'on ajoute le spectre de la vie privée. En effet, dès lors qu'il est question de données personnelles, deux autres clans s'affrontent : les partisans du protectionnisme de la vie privée et ceux prônant la libre circulation des informations.

Nos développements nous amènent à formuler notre conclusion sous la forme de deux remarques.

Tout d'abord, personne ne peut s'opposer à la mise en place de passeports électroniques, l'État étant seul maître de ces décisions. À preuve, les États-Unis et l'Europe ont décidé conjointement de la mise en place de ceux-ci. Aussi, la question n'est plus celle de la façon d'empêcher la mise en place des passeports munis de puces RFID, mais au contraire de la manière par laquelle ces passeports doivent s'adapter aux lois protégeant la vie privée. Les citoyens doivent prendre conscience que les « fuites » de données ou d'informations les concernant sont un risque majeur. Une fois ce risque reconnu, il faut veiller à la mise en place de solutions protégeant les données et, à fortiori, la vie privée des personnes.

Ensuite, nous remarquons qu'à l'heure de la révolution technologique de la planète, Internet pourrait jouer un rôle majeur dans l'information des personnes quant aux risques lui étant reliées. Ce récent vecteur d'information permettrait de sensibiliser un public plus nombreux qu'il ne l'était possible auparavant dans le monde du papier. Ainsi, sur la question de la sécurisation du passeport, le Département d'État américain a reçu plus de 2 400 commentaires de citoyens sur la mise en place de tel passeport.[88]

Finalement, il nous semble que la réponse à la technologie se trouve bien dans la technologie.

## Notes:

[1] Professeur Pierre Trudel, «Le droit d'Internet au Canada», Rapport présenté au colloque international sur l'Internet et le droit européen et comparé de l'Internet; Paris, 25-26 septembre 2000, disponible sur: <http://www.droit-internet-2000.univ-paris1.fr/dossier4/Pierre-Trudel.doc> (dernière visite le 28/04/2005).

[2] RFID : acronyme de Radio Frequency Identification Device.

[3] Harry Stockman, *Communication by Means of Reflected Power*, Proceedings of the IRE, 1948, p. 1196–1204.

[4] Identify: Friend or Foe.

[5] Voir notamment sur l'e-administration, le dossier du gouvernement français, l'e-administration, au service des citoyens.Voir <http://www.internet.gouv.fr/rubrique.php3?id_rubrique=253> (dernière visite le 28/04/2005).

[6] Voir notamment *Décret n° 2001-185 du 26 février 2001 relatif aux conditions de délivrance et de renouvellement des passeports*. Voir <http://www.legifrance.gouv.fr/texteconsolide/ARHCF.htm> (dernière visite le 28/04/2005).

[7] Document de travail sur les questions de protection des données liées à la technologie RFID 19/01/2005 WP 105. Voir <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/wp105_en.pdf> (dernière visite le 12/04/2005). Voir également le site <http://rapidttp.com/transponder/newswork.html> (dernière visite le 12/04/2005).

[8] Pour l'utilisation de ces puces dans un passeport, ce que nous développerons par la suite, voir John Carrey, "Big Brother's passport to try" *Business Week*, 5 novembre 2004, <http://www.businessweek.com/bwdaily/dnflash/nov2004/nf2004115_1663_db016.htm> (dernière visite le 12/04/2005).

[9] Voir sur les questions techniques des lecteurs : Committee on Radio Frequency Identification Technologies, *Radio Frequency Identification Technologies: A Workshop Summary*, National Research Council, 2004, <http://www.nap.edu/catalog/11189.html> (dernière visite le 15/04/2005).

[10] La cryptographie est une des disciplines de la cryptologie, s'attachant à protéger des messages (assurant confidentialité et/ou authenticité), en s'aidant souvent de secrets ou clés. Elle est utilisée depuis l'antiquité, mais

certaines de ses méthodes les plus importantes, comme la cryptographie asymétrique, n'ont que quelques dizaines d'années d'existence. Voir <http://fr.wikipedia.org/wiki/Cryptographie> (dernière visite le 12/04/2005).

[11] Schéma emprunté au rapport du groupe de travail sur l'Article 29, *supra*, note 5.

[12] Pour des spécifications techniques sur les puces actives et passives, voir : <http://www.autoid.org/2002_Documents/sc31_wg4/docs_501-520/520_18000-7_WhitePaper.pdf> (dernière visite le 26/04/2005).

[13] En l'occurrence en France, la réglementation concernant la protection du public contre les champs électromagnétiques repose sur le décret du 3 mai 2002 (n° 2002-775) qui fait acte de transposition de la *Recommandation européenne (1999/519/CE)* du 12 juillet 1999 relative à la limitation de l'exposition du public aux champs électromagnétiques (de 0 Hz à 300 GHz). Il s'avère que la technologie RFID utilise des fréquences comprises entre 135 kHz et 5.8 GHz, cette technologie entre donc bien dans le champ d'application de cette recommandation et du décret. Des questions restent pendantes sur l'effet de cette technologie sur la santé et des restrictions peuvent être envisagées, notamment en se référant à la *Directive 2004/40/CE* du parlement et du conseil en date du 29 avril 2004, dont la transposition doit être effectuée avant 2008. Pour plus d'informations sur cette question, voir : <http://www.anfr.fr/index.php?cat=sante&page=reglementation#2004_40> (dernière visite le 12/04/2005).

[14] Voir Matt Reynolds, «The physics of RFID», <http://www.rfidprivacy.org/papers/physicsofrfid.pdf> (dernière visite le 12/04/2005).

[15] Sur la question de la distance de fonctionnement des puces voir : *Radio Frequency identification Applications and Implications for Consumers*. Auditions devant la « Federal Trade Commission » du 21 juin 2004, notamment les témoignages de Daniel Engels p. 23–34, et de Jim Waldo p. 247. De plus, les éléments naturels comme le vent, la pluie peuvent venir perturber le champ électromagnétique.

[16] Pour le prix des puces RFID voir : <http://www.rfidjournal.com/article/glossary/3> (dernière visite le 12/04/2005).

[17] *Id*., note 16.

[18] *Id*., note 16.

[19] Voir notamment Marc Olanie, «RFID et cartes d'identité électronique, welcome big brother», <http://www.reseaux-telecoms.com/cso_btree/05_04_14_000240_710/CSO/Newscso_view> (dernière visite le 15/04/2005).

[20] Voir National Research Council, *Embedded, Everywhere : A Research Agenda for Networked Systems of Embedded Computers*, 2001, Washington D.C., National Academy Press, <http://books.nap.edu/html/embedded_everywhere/> (dernière visite le 15/04/2005).

[21] L'octet est une unité de mesure informatique. Un octet est composé de 8 bits. L'octet est la traduction du terme anglais byte. L'octet sert à mesurer les éléments relatifs à la mémoire d'un ordinateur, mais de façon plus générale la mémoire informatique. Le kilo-octet correspond quant à lui à $2^{10}$ octets soit 1024 octets. Voir <http://fr.wikipedia.org/wiki/Octet> (dernière visite le 15/04/2005).

[22] Electrically Erasable Programmable Read Only Memory : composante de stockage non volatile utilisée dans les ordinateurs et autres équipements. Cette mémoire peut être programmée et effacée plusieurs fois, elle peut être lue à l'infini. <http://fr.wikipedia.org/wiki/Electrically-erasable_programmable_read-only_memory> (dernière visite le 15/04/2005).

[23] Static Random Access Memory : il s'agit d'une RAM (random access memory) qui retient les informations tant et aussi longtemps qu'une source d'alimentation est fournie. <http://searchsmb.techtarget.com/sDefinition/0,,sid44_gci214231,00.html> (dernière visite le 15/04/2005).

[24] Pour de plus amples informations sur les types de mémoire, voir : Professeur Anthony Furness, «Present and Future Smart Active Label (SAL) Enabling Technologies — An Introductory Overview», p. 7-8. Voir <http://www.sal-c.org/pdfs/Overview%20on%20Current%20and%20Future%20SAL%20Technologies.pdf> (dernière visite le 26/04/2005).

[25] Voir en ce sens l'article de Mark Baard "Ridge Says RFID Boosts Security" *Wired News* 12 avril 2005, <http://www.wired.com/news/privacy/0,1848,67192,00.html> (dernière visite le 19/4/2005).

[26] Voir Ann Cavoukian, « Guidelines for using RFID Tags in Ontario Public Libraries », <http://www.ipc.on.ca/docs/rfid-lib.pdf> (dernière visite le 26/04/2005).

[27] Voir Alorie Gilbert, « Elementary school nixes IDs », *CNET News*, 17 février 2005. Online: <http://news.com.com/Elementary+school+nixes+electronic+IDs/2100-1029_3-5581275.html> (dernière visite le 26/04/2005).

[28] Article 2 : Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*. Voir <http://www.legifrance.gouv.fr/> (dernière visite le 20/04/2005).

[29] Article 3: « « renseignements personnels » Les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable » (puis suit une série d'exemples de données pouvant être un renseignement personnel). *Loi sur la protection des renseignements personnels*, L.R. 1985, ch. P-21. Voir <http://lois.justice.gc.ca/fr/P-21/index.html> (dernière visite le 20/04/2005).

[30] U.S.C. § 552a (*a*)(4) « the term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph ».

[31] Article 2 : « Toute information concernant une personne physique identifiée ou identifiable ; 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 ». J.O. des Communautés européennes n° L 281 du 23 octobre 1995 p. 0031–0050. Voir <http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=FR&numdoc=31995L0046&model=guichett> (dernière visite le 27/04/2005).

[32] Article 1(*b*) : « Données de caractère personnel, on entend toute information relative à une personne physique identifiée ou identifiable ». Organisation de coopération et de développement économiques, lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel, Paris, 23 septembre 1980, <http://www1.oecd.org/publications/e-book/9302012e.pdf>.

[33] *Id*., point 21.

[34] *Id*., note 30, p. 13

[35] *Id*., note 17, p. 15 Les présentes lignes directrices s'appliquent aux données à caractère personnel, dans les secteurs public et privé, qui, compte tenu de leur mode de traitement, de leur nature ou du contexte dans lequel elles sont utilisées comportent un danger pour la vie et les libertés individuelles.

[36] *Id*., note 30, p. 16–18.

[37] 5 U.S.C. § 552a. Voir <http://straylight.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552---a000-.html> (dernière visite le 20/04/2005).

[38] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, <http://www.iijcan.org> (dernière visite le 20/04/2005).

[39] *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*, <http://www.legifrance.gouv.fr> (dernière visite le 20/04/2005).

[40] Article 12 (1) de la *Loi sur la protection des renseignements personnels*, L.R. 1985, ch. P-21; 5 U.S.C. § 552a (*d*) (1); Article 39 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[41] Article 12 (2) de la *Loi sur la protection des renseignements personnels*, L.R. 1985, ch. P-21; 5 U.S.C. § 552a (*d*)(B)(i); Article 40 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[42] Article 5 de la *Loi sur la protection des renseignements personnels*, L.R. 1985, ch. P-21; 5 U.S.C. § 552a (*b*); Article 38 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[43] Article 5(2) de la *Loi sur la protection des renseignements personnels*, L.R. 1985, ch. P-21; 5 U.S.C. § 552a (*e*) (5); Article 6 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[44] *Id*., note 32, Recommandation de l'O.C.D.E. sur les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel : Paragraphe 11 : Principes des garanties de sécurité, § 56 « les notions de sécurité et de protection de la vie privée

n'ont pas la même signification. Cependant, les limitations imposées à l'utilisation et à la divulgation des données devraient être renforcées par des garanties de sécurité. Ces garanties comprennent des mesures d'ordre matériel (verrouillage des portes et cartes d'identification, par exemple), des mesures structurelles (telles que le chiffrement et la surveillance des activités inhabituelles susceptibles de présenter un danger et des mesures destinées à y faire face). Il conviendrait de souligner que la catégorie des mesures structurelles comprend l'obligation faite au personnel chargé du traitement de l'information de maintenir le caractère confidentiel des données ».

[45] Voir notamment : 5 U.S.C. § 552a (*e*) (10); Article 34 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[46] Voir sur cette question : Stephane Foucart, « Feu vert pour la carte d'identité électronique », Le Monde, 13 avril 2005. <http://www.lemonde.fr/web/article/0,1-0@2-3244,36-638179@51-627772,0.html> (dernière visite le 20/04/2005).

[47] Voir Ryan Singel, « Passport Chip Criticism Grows », *Wired News*, 31 mars 2005, <http://www.wired.com/news/privacy/0,1848,67066,00.html?tw=wn_story_page_prev2> (dernière visite le 20/04/2005).

[48] Voir Michael Kanellos, « The man with the RFID arm », *CNET News*, 15 février 2005. Voir <http://news.com.com/The+man+with+the+RFID+arm/2100-1029_3-5578023.html> (dernière visite le 28/04/2005).

[49] Department of Health and Human Services; Food and Drug Administration ; 21 CFR Part 880 ; Docket N°. 2004N-0477; published in Federal Register/ Vol. 69, N° 237 / Friday, December 10, 2004/Rules and Regulations.

[50] Voir Junko Yoshida, « Euro bank notes to embed RFID chips by 2005 », *EETimes*, 19 décembre 2001, <http://www.eetimes.com/story/OEG20011219S0016> (dernière visite le 27/04/2005); voir également : «Des RFID dans nos billets de banque», <http://www.jp-petit.com/Presse/RFID.htm> (dernière visite le 27/04/2005).

[51] Méthodologies d'analyses des risques développées par le Centre de Recherche en Droit public (CRDP), <http://www.crdp.umontreal.ca/cours/drt6929d/gestion%20risques.htm> (dernière visite le 26/04/2005).

[52] Pierre Trudel, « Law in Pursuit of Information Quality » dans Urs Gasser (ed.) *Information Quality Regulation : Foundations, Perspectives, and Applications*, Baden-Baden, Shulthess, 2004, p. 91–105; Jean Frayssinet, «La protection des données personnelles», dans *Droit de l'informatique et de l'Internet*, Paris, Puf Droit, 2001, p. 125–129.

[53] *Supra*, note 45.

[54] Voir EFF'S letter to the State Department regarding RFIDs in passports, <http://www.eff.org/Privacy/Surveillance/RFID/RFID_passport.pdf> (dernière visite le 26/04/2005) p. 10.

[55] *Id*., p. 9.

[56] *Id*., p. 12.

[57] *Id*., p. 9.

[58] La biométrie est le développement de méthodes statistiques et mathématiques applicables à l'analyse de données relevant de problèmes dans les sciences biologiques. Le terme biométrique vient du grec bio qui signifie vie et du terme metric qui signifie mesurer. Il s'agie de façon générale des technologies qui mesurent et analysent les caractéristiques physiologiques ou comportementales d'une personne, comme ses empreintes digitales, ses iris, le son de sa voix, la reconnaissance faciale, la reconnaissance de la main, et cela pour des besoins d'identification ou de vérification. Voir pour un historique notamment de la biométrie, <http://ctl.ncsc.dni.us/biomet%20web/BMOverview.html#definition> (dernière visite le 27/04/2005).

[59] *Id*., note 54, p. 10

[60] Voir Arik Hesseldahl, «A Hacker's guide to RFID», *Forbes*, 29 juillet 2004. Voir <http://www.forbes.com/home/commerce/2004/07/29/cx_ah_0729rfid.html> (dernière visite le 26/04/2005); voir également comment un téléphone cellulaire peut devenir un lecteur RFID, *RFID Journal*, «Nokia unveils RFID phone reader» (17 mars 2004), <http://www.rfidjournal.com/article/articleview/834/1/13/> (dernière visite le 26/04/2005).

[61] Voir sur cette question : Ziv Kfir et Avishai Wool, *Picking Virtual Pockets Using Relay Attacks on Contactless Smartcard Systems* (2005), Cryptology ePrint Archive, Report 2005/052, <http://eprint.iacr.org/2005/052> (dernière visite le 26/04/2005).

[62] En cette matière il semblerait que le Canada ait commencé l'incorporation de données biométriques dans les passeports. Voir Susan Munroe, « Canada Plans Biometric Passports », Canada Online, <http://canadaonline.about.com/od/idcards/a/biometricpssprt.htm> (dernière visite le 27/04/2005).

[63] Lire Philip K. Dick, *Minority Report*, La Flèche, Gallimard, 2004.

[64] Voir l'article 8, alinéa 1er de la Directive de 1995 qui pose le principe selon lequel : « Les États membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle. » Voir également l'article 31 d la loi de 1978 dite informatique et liberté. Cependant dans le cadre de collecte de données médicales il est possible que la personne intéressée puisse donner son accord pour que des données sur sa personne soit collectée. Dans cette hypothèse il est nécessaire d'obtenir l'accord de cet individu, un accord qui doit être exprès si l'on en croit l'article 8-2 a de la Directive de 1995. En outre, il existe d'autres exceptions comme dans le § 3 de l'article 8 de la Directive de 1995. Ainsi l'interdiction de traitement des données sensibles ne s'applique pas lorsque le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé. Néanmoins ce traitement doit être effectué par un praticien de la santé soumis au secret professionnel ou par une autre personne également soumise à une obligation de secret équivalente. Voir sur l'ensemble de cette question, Jean Frayssinet, « La protection des données personnelles », *loc. cit*., note 52, p. 137–161.

[65] « Le principe de finalité est l'un des piliers de la protection. Un traitement d'informations nominatives est créé pour atteindre un certain objectif. Son contenu 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.» site de la Commission Nationale Informatique et Liberté : <http://www.cnil.fr/index.php?id=20&print=1> (dernière visite le 27/04/2005).

[66] George Orwell, *1984*, La Flèche, Gallimard, 1991.

[67] Jennifer Stoddart, "Appui à la transparence et protection des renseignements personnels", Conférence à l'intention de la communauté de l'Accès à l'information et protection des renseignements personnels. 1er avril 2004, <http://canadaonline.about.com/gi/dynamic/offsite.htm?zi=1/XJ&sdn=canadaonline&zu=http%3A%2F%2Fwww.privcom.gc.ca%2Fspeech%2F2004%2Fsp-d_040401_e.asp> (dernière visite le 27/04/2005).

[68] *Directive 95/46/CE supra*, note 31, et *Directive 2002/58/CE 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*.

[69] Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology*, du 19 janvier 2005 10107/05/EN WP 105, p. 8–11, <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/wp105_en.pdf> (dernière visite le 27/04/2005).

[70] *Supra*, note 67.

[71] Cette nouvelle definition serait: "Any individually identifiable information including name, address, e-mail, telephone number, visual identification, birth details or any other information combined with any of the preceding". Voir projet de loi S.116, <http://thomas.loc.gov/cgi-bin/query/z?c109:S.116> (dernière visite le 28/04/2005). On peut également s'intéresser à la doctrine américaine, notamment au Professeur Daniel J. Solove et Chris J. Hoofnagle, « A model regime of privacy protection version 2.0 », GWU Law School Public Law Research Paper No. 136, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=699701> (dernière visite le 1/05/2005), p. 18-19. Article dans lequel le Professeur Solove demande l'actualisation du *Privacy Act*, avec la régulation de la collecte des données personnelles, des utilisations raisonnées, l'actualisation des données, la sécurité, et la non divulgation des informations.

[72] *Id*., Titre 4 du projet de loi.

[73] *Id*. Titre 2 du projet de loi.

[74] Voir le projet de loi californien SB 682, The act would prohibit identification documents created, mandated, purchased, or issued by various public entities from containing a contactless integrated circuit or other device that can broadcast personal information or enable personal information to be scanned remotely, except as specified. <http://leginfo.ca.gov/pub/bill/sen/sb_0651-0700/sb_682_bill_20050331_amended_sen.html> (dernière visite le 29/04/2005). Voir également Alorie Gilbert, "California bill would ban tracking chips in IDs", *CNET News*, 28 avril 2005. Voir <http://news.com.com/Cali-

fornia+bill+would+ban+RFID+chips+in+IDs/2100-1039_3-5689358.html?tag=html.alert> (dernière visite le 29/04/2005).

[75] Voir Alorie Gilbert, "California lawmaker introduces RFID bill", *CNET News*, 28 avril 2005, <http://news.com.com/California+lawmaker+introduces+RFID+bill/2100-1014_3-5164457.html?tag=nl> (dernière visite le 29/04/2005).

[76] Daniel J. Solove, « Identity Theft, Privacy, and the Architecture of Vulnerability », *Hastings Law Journal*, Vol. 54, 2003, p. 1227, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=416740> (dernière visite le 1/05/2005).

[77] Fair Information Practices : "There must be no personal-data record-keeping systems whose very existence is secret. There must be a way for an individual to find out what information about him is in a record and how it is used. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent. There must be a way for an individual to correct or amend a record of identifiable information about him. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data." U.S. Department of Health, Education, and Welfare, *Report of the secretary's advisory committee on automated personal data systems: records, computers, and the rights of citizens* xxxii (1973).

[78] Voir notamment Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC), Center for Democracy & Technology (CDT), American Civil Liberties Union (ACLU), et, au Canada, la Canadian Internet Policy and Public Interest Clinic (CIPPIC).

[79] Ce document précise les besoins d'interopérabilité des puces RFID avec les différents lecteurs existant. La capacité de mémoire des puces RFID ne doit pas être en deçà de 32K, les données doivent être protégées contre l'accès frauduleux au moyen de la cryptographie, voire de microprocesseur, ou par tout autre moyen. L'accès aux données doit se faire en moins de 10 secondes. Le lecteur doit pouvoir lire les données soit par contact physique du document ou bien à une distance n'excédant pas 10 centimètres. ICAO New technologies working group request for information, <http://www.icao.int/mrtd/download/documents/ICAO%20RFI%202004.pdf> (dernière visite le 27/04/2005).

[80] ICAO, PKI Task Force, «PKI for Machine Readable Travel Documents offering ICC Read-Only Access», <http://www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf> (dernière visite le 27/04/2005).

[81] *Supra*, note 47.

[82] Kim Zetter, « Feds Rethinking RFID Passport », *Wired.com*, 26 avril 2005. <http://www.wired.com/news/privacy/0,1848,67333,00.html?tw=wn_story_page_prev2> (dernière visite le 27/04/2005).

[83] Charles Clark, « The answer to the machine is in the machine », in P. Bernt Hugenholtz, *The future of copyright in a digital environment*, The Hague, Kluwer, 1996, p. 139.

[84] *Supra*, note 78, p. 18; voir également pour des précisions techniques sur la technologie BAC, <http://www.itsc.org.sg/tc/6th_term_compo/Summary-ofInterFest3Feb05_Final.pdf> (dernière visite le 28/04/2005).

[85] Pour une définition du hachage ou hashing en anglais voir : <http://www.webopedia.com/TERM/h/hashing.html> (dernière visite le 28/04/2005).

[86] Concernant les failles potentielles de la technologie BAC, voir Ari Juels, David Molnar et David Wagner, *Security and Privacy Issues in E-passports*, <http://eprint.iacr.org/2005/095.pdf> (dernière visite le 28/04/2005).

[87] *Supra*, note 25.

[88] *Supra*, note 80.