Documents de travail de l'OCDE sur l'économie numérique No. 138

L'idenfication par radiofréquence (RFID)

SÉCURITÉ DE L'INFORMATION ET PROTECTION DE LA VIE PRIVÉE

OCDE

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

29-Apr-2008

Français - Or. Anglais

DIRECTION DE LA SCIENCE, DE LA TECHNOLOGIE ET DE L'INDUSTRIE
COMITE DE LA POLITIQUE DE L'INFORMATION, DE L'INFORMATIQUE ET DES COMMUNICATIONS

Groupe de travail sur la sécurité de l'information et la vie privée

L'IDENTIFICATION PAR RADIOFRÉQUENCE (RFID) : SÉCURITÉ DE L'INFORMATION ET PROTECTION DE LA VIE PRIVÉE

www.oecd.org/sti/securitevieprivee

JT03244945

AVANT-PROPOS

Ce rapport a été préparé par le Secrétariat avec l'assistance de Nick Mansfield et Francis Aldhouse, consultants pour l'OCDE. Il tient compte des commentaires et éléments en provenance des pays membres de l'OCDE, des entreprises et de la société civile.

Le rapport a été discuté par le Groupe de travail sur la sécurité de l'information et la vie privée en octobre 2007 et a été déclassifié par le Comité de la politique de l'information, de l'informatique et des communications le 17 décembre 2007. Il est publié sous la responsabilité du Secrétaire Général de l'OCDE.

TABLE DES MATIÈRES

L'IDENTIFICATION PAR RADIOFRÉQUENCE (RFID) : SÉCURITÉ DE L'INFORMATION ET PROTECTION DE LA VIE PRIVÉE

SYNTHÈSE

Le déploiement de l'identification par radiofréquence (RFID) dans un grand nombre de domaines d'application paraît prometteur. Le présent document décrit les principales caractéristiques de la RFID et traite plus particulièrement de ce que ces technologies impliquent à court terme sur les plans de la sécurité de l'information et de la vie privée. Il sera complété par une présentation générale des applications de la RFID et une analyse des aspects économiques de cette technologie par le Groupe de travail de l'OCDE sur l'économie de l'information (GTEI)[1]. Par la suite, et sur la base de ces deux séries de travaux, un ensemble de principes sur la RFID sera mis au point[2].

Le présent rapport constitue la première étape d'une série de travaux de l'OCDE consacrés aux environnements à base de capteurs. Dans un second temps, ces travaux s'intéresseront également aux questions de sécurité et de vie privée soulevées par un certain nombre de tendances susceptibles d'apparaître à plus long terme, comme par exemple la généralisation du marquage des objets (RFID ubiquitaire), les applications de RFID en boucle ouverte, ainsi que la mise en œuvre d'autres capteurs et réseaux de capteurs permettant d'exercer un contrôle sur l'environnement.

Une technologie complexe et variée

L'acronyme RFID est une expression simple et populaire qui désigne une technologie aux **contours vagues** et aux **nombreuses facettes**. Contrairement à ce que son nom indique, l'identification par radiofréquence ne s'appuie pas toujours sur des communications radio, et l'identification n'est que l'une des nombreuses fonctions pouvant être assurées par cette technologie. En fait, la RFID permet de recueillir des données à l'aide de puces (ou étiquettes ou marqueurs) électroniques sans contact (« *RFID tags* ») et de transmetteurs sans fil (lecteurs), pour des besoins d'identification ou autres. Elle peut être considérée comme une première étape vers les environnements à base de capteurs.

Il est indispensable de comprendre les possibilités et les limites de cette technologie, car les divers risques qu'elle peut présenter sur le plan de la sécurité et de la vie privée dépendent aussi bien du type de RFID utilisée que du contexte dans lequel elle est mise en œuvre. Le présent document fournit donc des **informations de base** sur cette technologie, notamment sur les normes, les composants matériels et logiciels, les bandes de fréquence, les modes de fonctionnement (induction électromagnétique ou ondes radio) et les distances de fonctionnement.

Considérations sur la sécurité de l'information

Les puces, les lecteurs RFID ainsi que la communication entre eux sont exposés à un **grand nombre de risques** qui impliquent les trois dimensions traditionnelles de la sécurité : disponibilité, intégrité et confidentialité. Ces risques sont par exemple le déni de service, le brouillage, le clonage, l'interception des données et la lecture non-autorisée (*skimming*). Les logiciels malveillants utilisant des étiquettes RFID comme vecteurs de diffusion ont également été répertoriés parmi les risques potentiels. Les étiquettes et les

1. Voir OCDE(2007b,c).

2. DSTI/ICCP/IE/REG(2007)1.

lecteurs ne sont pas les seuls composants des systèmes RFID qui nécessitent une protection. Les logiciels (intergiciels ou *middleware*), les composants réseau et les bases de données peuvent eux aussi être attaqués. Les risques de sécurité encourus par les technologies RFID ne sont pas imaginaires : de nombreux produits et systèmes, parfois déployés à très grande échelle, ont été signalés par des scientifiques ou dans la presse comme étant vulnérables. Toutefois, ces risques potentiels sont, pour nombre d'entre eux, plus ou moins liés au type de technologie RFID utilisée (par exemple, l'interception des données est moins probable avec les étiquettes RFID à induction magnétique car leur portée est très faible).

Assurer la sécurité de l'identification par radiofréquence nécessite tout un ensemble de dispositions techniques et non techniques pour prévenir et atténuer les risques. Un certain nombre de **moyens techniques** existent, mais leur degré de sophistication, robustesse, complexité et coût sont variables. On ne dispose donc pas de solution de sécurité universelle pouvant apporter une réponse efficace à un type de risques donné, dans toutes les situations et à faible coût. Par conséquent, l'élaboration de mesures techniques de sécurité à la fois novatrices et bien adaptées à la RFID pourraient être un facteur critique de succès du déploiement à grande échelle de cette technologie dans de nombreux domaines.

Comme cela a été indiqué ci-dessus, les risques encourus par les systèmes RFID varient considérablement, non seulement en fonction de la technologie utilisée, mais aussi selon le contexte et le scénario d'application. En accord avec les *Lignes directrices de l'OCDE sur la sécurité*, l'évaluation et la gestion des risques peuvent contribuer à traiter la sécurité des systèmes RFID. Une **approche holistique** du risque (c'est-à-dire qui considère chaque étape de la vie du système – planification, déploiement, fonctionnement, traitement des données et fin de vie – et chaque composant du système – étiquettes et lecteurs, intergiciels (*middleware*), bases de données, composants réseau et serveur) est nécessaire pour élaborer une stratégie globale en matière de sécurité. Une stratégie d'évaluation et de gestion des risques permet de déterminer s'il faut consolider certains éléments du système pour compenser des lacunes qui ne peuvent être comblées directement.

Comme pour toute technologie, définir le niveau de sécurité approprié d'un système RFID suppose de trouver le bon équilibre entre la **valeur des ressources à protéger,** les dommages qu'une attaque pourrait causer, et les risques. Les principaux facteurs à prendre en compte sont les incidences potentielles sur la vie privée lorsque des informations relatives à des personnes sont utilisées. L'investissement dans des systèmes RFID plus sûrs, la combinaison de mesures de sécurité RFID et non-RFID, ou l'utilisation de technologies autres que la RFID font partie des stratégies envisageables pour accroître le niveau de sécurité.

La technologie RFID étant encore récente et en pleine évolution, des techniques d'attaque inédites et imprévues risquent de faire leur apparition. **Un réexamen et une réévaluation** des systèmes RFID sont indispensables pour déterminer quels investissements devront être effectués en matière de sécurité pour faire face à l'évolution des risques.

Considérations sur la vie privée

Les risques éventuels pour la vie privée suscitent généralement d'**importantes inquiétudes** chez les particuliers et les organisations. Les caractéristiques et fonctionnalités clés des technologies RFID peuvent à la fois présenter des avantages (simplicité, rapidité, par exemple), susciter des conceptions erronées et avoir des incidences sur la vie privée. Les systèmes RFID qui recueillent des données relatives à des personnes identifiées ou identifiables soulèvent des problèmes particuliers de protection de la vie privée qui devraient être considérés comme un défi majeur pour la diffusion de cette technologie dans un grand nombre de domaines. Dans la plupart des cas, l'éventuelle ingérence dans la vie privée résultant de l'utilisation de la RFID dépend à la fois de la technologie utilisée et du contexte.

Le caractère **invisible** de la collecte des données est sans doute la principale caractéristique de la RFID qui suscite des inquiétudes. C'est aussi un facteur multiplicateur de risques pour les éventuels

problèmes de protection de la vie privée associés à l'utilisation de cette technologie. La RFID pourrait révéler à des tiers des informations sur des objets transportés par des individus sans que ces derniers n'en aient conscience. Elle pourrait aussi permettre d'établir des inférences concernant une personne, révélant des liens avec d'autres informations et conduisant à la constitution d'**un profil** plus précis la concernant : ces conclusions pourraient par exemple être déduites de plusieurs étiquettes portées par un individu, de données sensibles telles que les données biométriques enregistrées sur un passeport RFID non protégé ou de médicaments étiquetés avec une puce RFID. Dans ce type de scénario, il faudrait cependant que des lecteurs soient présents à proximité des étiquettes, et que la tierce partie soit en mesure de convertir en données intelligibles les informations figurant sur les étiquettes des objets.

Le **suivi** en temps réel ou *a posteriori* est peut-être la fonctionnalité principale de la RFID qui est source de préoccupations. En particulier, compte tenu de l'invisibilité de cette technologie, le suivi des individus peut avoir lieu sans que ces derniers n'en aient connaissance, par exemple s'ils sont munis d'étiquettes cachées ou pas suffisament sécurisées. Dans d'autres cas, le suivi des personnes pourrait également être l'objectif même de l'application de la RFID (par exemple, pour savoir où se trouvent des enfants dans un parc d'attractions).

L'interopérabilité des technologies RFID (« en boucle ouverte ») facilitant, et donc multipliant, les opérations de collecte et de traitement d'informations personnelles est un autre sujet de préoccupation. Une RFID omniprésente tirant avantage de son **interopérabilité** et de la possibilité de se connecter à Internet en tous lieux, tel est l'avenir qui nous est souvent décrit comme inévitable, bien qu'il n'existe actuellement que peu de systèmes en « boucle ouverte ».

Dans les cas où les systèmes RFID recueillent des données relatives à une personne identifiée ou identifiable, les ***Lignes directrices de l'OCDE sur la protection de la vie privée*** fournissent un cadre utile.

Lorsqu'un système RFID traite des données personnelles, il est indispensable que la finalité de cette opération soit communiquée en toute **transparence** et que les personnes concernées aient exprimé leur **consentement**. Outre les informations de base sur la protection des données, les notices d'information sur la protection de la vie privée pourraient faire mention des informations suivantes : *i)* l'existence de puces ou étiquettes RFID ; *ii)* leur contenu, leur utilisation, et la façon dont ils sont gérés ; *iii)* la présence de lecteurs ; *iv)* l'activité de lecture ; *v)* la possibilité de désactiver les puces ; et *vi)* les coordonnées du service d'assistance. La recherche de nouveaux moyens pour informer efficacement les personnes pourrait être envisagée. Un dialogue permanent entre l'ensemble des parties prenantes, dans tous les secteurs et tous les domaines d'application, permettrait de clarifier ou de trouver un accord sur les informations qui doivent être fournies au public, les meilleurs moyens de les communiquer pour que la transparence soit efficace, et les cas dans lesquels le consentement des personnes est ou n'est pas nécessaire.

Il va de soi que des **garanties de sécurité** sont primordiales pour assurer la protection de la vie privée à l'égard des systèmes RFID.

Compte tenu de la grande diversité des configurations techniques et des scénarios d'utilisation, **l'évaluation des incidences de la RFID sur la vie privée** (*Privacy Impact Assessment*) est une bonne pratique pour identifier et appréhender les risques en matière de protection de la vie privée, et trouver les meilleures stratégies pour les limiter dans un système donné. En ce qui concerne la sécurité, les systèmes RFID étant souvent intégrés à des dispositifs d'information de plus grande envergure, on ne peut pas s'attendre à ce que toutes les questions de protection de la vie privée soient résolues au niveau de la RFID. Une approche holistique de la gestion de la protection de la vie privée peut être considérée comme une bonne pratique. Une telle approche notamment en examinant tous les composants des systèmes d'information concernés – et pas seulement les éléments de base de la RFID – tiendrait compte du cycle de vie complet d'une puce RFID lorsque ses fonctions restent actives mais que le maître du fichier n'y a plus accès.

Le choix de l'utilisation de la technologie RFID dans un système influe sur la protection de la vie privée au même titre que sur la sécurité du système. La **protection intégrée de la vie privée** (*privacy by design)* ou l'intégration du respect de la vie privée dans la conception de la technologie et des systèmes peut faciliter de façon significative la protection de la vie privée et faire en sorte que les systèmes RFID inspirent confiance. Le développement de **technologies RFID favorisant la protection de la vie privée** (*privacy enhancing technologies*) est une tendance actuelle qui pourrait être encouragée. Des techniques comme la minimisation et l'anonymisation des données peuvent être appliquées à la RFID. Des stratégies pourraient être mises en œuvre pour inciter l'industrie et les entreprises à concevoir et utiliser des technologies RFID incluant des garanties suffisantes pour la vie privée. Quoi qu'il en soit, comme pour la sécurité, la protection de la vie privée ne doit pas reposer uniquement sur des procédés techniques mais plutôt sur une combinaison de mesures techniques et non techniques.

Certains professionnels n'associent pas les informations contenues dans les étiquettes RFID à des individus, mais leur fournissent pourtant des biens ou des produits de consommation comportant des puces RFID fonctionnelles qui pourront être lues ultérieurement par eux-mêmes ou par des tiers. Il pourrait être proposé que ces professionnels prennent la responsabilité soit de désactiver les puces, soit d'informer les personnes concernées de la présence des puces, des risques que cela présente pour la protection de la vie privée, et des moyens dont on dispose pour prévenir ou atténuer ces risques.

Enfin, et de façon plus générale, la RFID n'est pas bien comprise par le public. Accroître le niveau de **connaissance et de compréhension** de cette technologie, de ses possibilités et de ses limites ainsi que de ses avantages et ses risques, peut contribuer à améliorer ce problème d'image. Cela peut aussi aider les personnes à faire de bons choix et encourager les professionnels à mettre en place des systèmes respectueux de la vie privée.

Conclusion

Les questions de sécurité et de protection de la vie privée relatives aux infrastructures de RFID et aux logiciels correspondants devraient être examinées par l'ensemble des parties prenantes avant que cette technologie ne soit déployée à grande échelle.

Les *Lignes directrices de l'OCDE sur la sécurité* fournissent un cadre qui permet le développement d'une culture de la sécurité pour les systèmes RFID, que ces derniers traitent ou non des données personnelles. *Les Lignes directrices de l'OCDE sur la protection de la vie privée* donnent elles aussi des indications utiles pour mettre en œuvre des systèmes RFID qui recueillent ou traitent des données personnelles.

Toutefois, un dialogue reste nécessaire pour clarifier ou pour trouver un accord sur plusieurs points, comme par exemple : *i)* comment appliquer les concepts de données personnelles et de maître du fichier ; *ii)* la nature des informations à fournir aux individus et les meilleurs moyens de les communiquer pour que la transparence soit efficace ; *iii)* les cas dans lesquels le consentement des personnes est nécessaire.

Certains des concepts et approches qui sont énoncés dans les *Lignes directrices sur la sécurité* de 2002 pourraient être adaptés de façon à faciliter la mise en œuvre des principes de l'OCDE sur la protection de la vie privée, à renforcer leur efficacité et à permettre le développement d'une culture de la protection de la vie privée vis-à-vis des systèmes RFID. Il est question notamment d'activités de sensibilisation, de méthodologies de réduction des risques (par exemple, de la pratique de l'évaluation de l'incidence sur la vie privée) et de travaux visant à intégrer les questions de sécurité et de protection de la vie privée dans la conception des technologies et des systèmes RFID.

INTRODUCTION

Contexte

Le Forum de prospective sur la RFID du Comité PIIC de l'OCDE – intitulé « Radio Frequency Identification (RFID) Applications and Public Policy Considerations » – qui a eu lieu en octobre 2005, a mis en relief le potentiel économique que représentent les technologies RFID ainsi que les nouveaux défis qu'elles suscitent en matière de sécurité de l'information et de protection de la vie privée. Il a également souligné que la RFID pouvait être considérée comme la première illustration d'une technologie faisant appel à un réseau de capteurs intelligents, qui pourrait permettre la création de « l'Internet des choses ». L'utilisation de la RFID devrait faciliter la convergence des technologies de communication et contribuer à terme à créer des « sociétés de réseaux ubiquitaires », où quasiment chaque aspect de l'environnement de vie et de travail d'un individu serait relié à un réseau global omniprésent, 24 heures sur 24, 7 jours sur 7.

En s'appuyant sur l'intérêt généré par ce forum, d'autres activités sur la RFID ont été incluses dans le programme de travail 2007-2008 de l'OCDE :

- Le Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP) a engagé des travaux sur la RFID et l'informatique à base de capteurs dans le contexte plus général des capteurs et des réseaux ubiquitaires, afin de déterminer si les *Lignes directrices de l'OCDE sur la sécurité et sur la protection de la vie privée* seraient remises en question par ces nouvelles tendances technologiques.

- Le Groupe de travail sur l'économie de l'information (GTEI) a entrepris des travaux sur les aspects économiques de la RFID[3].

En octobre 2006, le GTSIVP a examiné un rapport préliminaire du Secrétariat qui passe en revue les problèmes de sécurité de l'information et de vie privée suscités par la RFID, les capteurs et les technologies réseau ubiquitaires. Il a constaté que la RFID et la technologie des capteurs se trouvaient à deux stades différents en matière de développement et de déploiement. Les technologies RFID connaissent déjà une évolution et une progression rapides, elles sont arrivées à un certain niveau de maturité et sont en train d'être déployées à petite, moyenne et grande échelles dans de nombreux pays, dans plusieurs secteurs et pour des applications diverses. Des problèmes de sécurité et de protection de la vie privée leur sont déjà associés. En revanche, les autres capteurs et technologies capteurs en réseau qui enregistrent les paramètres de l'environnement et communiquent les données enregistrées à d'autres dispositifs auxquels ils sont connectés sont moins avancés et généralement déployés à beaucoup plus petite échelle, pour des applications qui ont rarement des répercussions sur les personnes. Leur généralisation n'est pas encore effective, les applications et les secteurs demandeurs ne sont pas encore connus, et les problèmes spécifiques qui risquent d'apparaître au niveau de la sécurité et de la vie privée sont hypothétiques. On ne connaît pas non plus les répercussions qu'aura à cet égard la RFID ubiquitaire. Le GTSIVP a donc décidé que les travaux menés en 2007 seraient consacrés aux problèmes causés par l'utilisation de la RFID à court terme. Les problèmes engendrés à long terme par la RFID ubiquitaire et d'autres technologies à base de capteurs feront l'objet d'une étude ultérieure.

3. OCDE, 2007b et 2007c.

Le présent rapport sur la RFID, la sécurité de l'information et la vie privée souligne l'importance de la dimension transversale des travaux du GTSIVP sur la sécurité et la protection de la vie privée. La gestion des identités, l'authentification et les logiciels malveillants ont tous des conséquences sur la RFID et les technologies similaires. À titre d'exemple, les puces RFID peuvent stocker des données personnelles importantes et être reliés à des bases de données contenant des informations à caractère personnel. Ces puces, qui sont de plus en plus utilisés pour authentifier les personnes, peuvent contenir des données biométriques ou d'autres informations d'authentification, par exemple dans les systèmes d'identification à grande échelle que sont les passeports ou les cartes d'identité nationales. Par ailleurs, des puces RFID pourraient être utilisées comme vecteurs d'une attaque par un logiciel hostile ou malveillant. D'où la conclusion qu'il demeure important de traiter les problèmes de sécurité et de vie privée de façon conjointe et en suivant de près l'évolution des nouvelles technologies et applications en matière de communications.

Bien que leur création remonte à la Seconde Guerre mondiale, les technologies RFID ont connu ces dernières années une évolution rapide et ont été mises en œuvre dans tous les secteurs de l'économie. Tandis que les technologies à base de capteurs intelligents continuent de se développer et pourraient conduire, en association avec la RFID, à la création d'un « Internet des choses », il est important que l'on prenne conscience de l'incidence qu'ont ces technologies sur l'Internet et sur la société. À cet égard, les résultats de la présente étude serviront de support à la réunion ministérielle de l'OCDE en 2008, dont le thème est « L'avenir de l'économie de l'Internet ».

Objectifs et portée de l'étude

Le présent rapport a pour but de faire le point sur les capacités de la RFID à court terme, et de mettre en évidence les problèmes suscités par cette technologie en matière de sécurité de l'information et de protection de la vie privée, dont les implications ne sont pas toujours prises en compte dans les instruments ou politiques existants. Les *Lignes directrices de l'OCDE sur la sécurité des systèmes d'information et des réseaux : vers une culture de la sécurité* (*Lignes directrices sur la sécurité*) et les *Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel* (*Lignes directrices sur la vie privée*) servent de référence tout au long de l'analyse. Ce rapport a pour objectif de servir de base de travail pour le développement d'orientations pour la sécurité de l'information et la protection de la vie privée par le GTSIVP qui seront proposées dans un document séparé de façon conjointe avec les conclusions des travaux du GTEI concernant les applications de la RFID dans les secteurs public et privé, les conséquences économiques et les politiques mises en œuvre par les gouvernements pour développer et diffuser la RFID et les technologies associées[4].

La première section du présent rapport a pour objectif de mieux faire comprendre ce qu'est la RFID, sigle qui recouvre un concept général et, dans une certaine mesure, peu précis qui fait référence aux technologies permettant la collecte de données à l'aide de puces électroniques sans contact et de transmetteurs sans fil (lecteurs), à des fins d'identification ou autres. La seconde section est consacrée aux problèmes de sécurité de l'information et de protection de la vie privée que soulève déjà la RFID ou qui risquent d'apparaître d'ici trois à quatre ans, en proposant d'éventuelles solutions pour les résoudre.

Bien que la RFID soit considérée comme un sous-ensemble de l'informatique à base de capteurs, cette catégorie plus vaste – qui regroupe aussi des technologies de collecte d'informations qui n'utilisent pas de puces RFID – n'est pas examinée ici. Le présent rapport n'aborde pas non plus les problèmes qui pourront survenir lorsque la RFID deviendra ubiquitaire, qu'elle sera utilisée de manière non anticipée, ou associée avec d'autres technologies à base de capteurs. Ces questions feront l'objet de travaux ultérieurs.

4. Voir DSTI/ICCP/IE(2007)6 et 7, présentés à la réunion du GTEI en mai 2007.

1. MIEUX COMPRENDRE LA RFID

La RFID a été décrite comme « la plus ancienne nouvelle technologie du monde ». Son invention remonte aux années 1940, avec des applications relatives à l'identification « ami/ennemi » des avions militaires. Les premières utilisations commerciales sont apparues dans les années 1960 avec la surveillance électronique des articles pour lutter contre le vol, une application qui est toujours très répandue aujourd'hui. Les progrès accomplis dans le domaine des semi-conducteurs ont permis des améliorations importantes de cette technologie. Parallèlement, le succès commercial des applications mises sur le marché a entraîné une baisse considérable des coûts et un intérêt croissant des entreprises.

De nombreux éléments indiquent que le foisonnement des applications faisant appel à la technologie RFID n'en est qu'à ses débuts. Les chiffres fournis par les analystes du marché prédisent l'essor commercial de cette technologie au cours des dix prochaines années. Selon une étude de la société Gartner (2005), le chiffre d'affaires du marché de la RFID (achats de matériel et de logiciels) a augmenté de plus de 33 % entre 2004 et 2005 (il s'élevait cette année-là à USD 504 millions), et il atteindra USD 3 milliards d'ici à 2010. Le cabinet d'étude IDTechEx (2006a) prévoit que le marché global de la RFID, incluant à la fois les systèmes et les services, sera de USD 26.23 milliards en 2016 (contre environ USD 2.71 milliards en 2006), et que le nombre total de puces s'élèvera à 585 milliards, soit 450 fois plus qu'en 2006. Les avantages que présente la technologie RFID pour les entreprises et les particuliers sont très prometteurs (OCDE, 2006a).

Un moteur important de la croissance actuelle du marché est la possibilité d'améliorer la traçabilité des marchandises dans la chaîne logistique, ce qui permet d'accroître la rentabilité de cette chaîne, de réduire les vols et les fraudes, et de réaliser de substantielles économies. De nombreux autres types d'applications de la RFID ont en outre été répertoriés, et cette technologie est désormais courante dans des domaines comme les passeports, les hôpitaux, les transports, les billetteries, les bibliothèques, les musées, la lutte contre la contrefaçon, le suivi des bagages dans les aéroports et le marquage du bétail. Au vu de ce succès, il est probable que la RFID aura des incidences sur les processus de gestion des entreprises et des administrations, ainsi que sur la vie des particuliers et des consommateurs. Comme l'a indiqué le Groupe de travail Article 29[5] (2005), « les fonctions spécifiques que peuvent assurer les tags RFID dans les différents secteurs sont elles aussi en augmentation et leurs possibilités commencent tout juste à se dégager ».

L'utilisation de la RFID dans l'ensemble de la chaîne logistique requiert un réaménagement en profondeur de processus de gestion complexes, et il ne faut pas s'attendre à ce que cette technologie devienne ubiquitaire à court terme, à un niveau tel que la société en soit considérablement bouleversée (par exemple, marquage de chaque article ou utilisation généralisée de la RFID en dehors du point de vente). Cela étant, il est probable que le nombre d'applications de la RFID augmentera dans de nombreux secteurs – comme le suggèrent les chiffres énoncés plus haut – et que la technologie évoluera, ouvrant la voie à de nouvelles applications.

5. Le Groupe de travail Article 29 est un organe consultatif indépendant chargé d'étudier la protection des données et de la vie privée des personnes au sein de l'Union européenne. Il regroupe les représentants des autorités de protection des données européennes. Il a été créé en vertu de l'article 29 de la Directive européenne 95/46/CE.

L'une des principales conclusions du Forum de prospective sur la RFID organisé par le Comité PIIC en octobre 2005 était que la protection de la vie privée et la sécurité sont deux grands obstacles au développement à grande échelle de la RFID, et que des solutions doivent être trouvées. Comprendre cette technologie, ses possibilités et ses limites, permet d'éviter de sous-estimer ou surestimer ces risques. La présente section donne un aperçu général et conceptuel de la RFID, en décrivant les étiquettes RFID, les lecteurs et l'environnement dans lequel fonctionne cette technologie[6].

1.1. Un concept général pour une technologie complexe

La RFID est un concept commode et populaire pour désigner une technologie aux multiples facettes. L'expression « identification par radiofréquence » fait référence à deux dimensions de cette technologie : *i)* l'aspect technique : les radiofréquences ; *ii)* la fonction particulière de cette technologie : identifier des objets, des animaux ou des personnes qui portent, ou sur lesquels est insérée ou implantée, une puce. La signification de l'acronyme RFID peut donc être trompeuse : les communications établies à l'aide de cette technologie ne reposent pas toujours sur les radiofréquences (elles peuvent avoir lieu par induction électromagnétique), et la RFID peut être utilisée dans des contextes où l'identification n'est qu'une fonction parmi d'autres. Cette technologie permet par exemple d'effectuer des tâches de suivi, dont les incidences sont considérables sur le plan économique et social. Par ailleurs, certaines puces RFID peuvent enregistrer dans leur mémoire des données provenant d'un lecteur, à l'instar des puces équipées de capteurs qui mesurent les paramètres de l'environnement (lumière, bruits, température, etc.).

Il serait plus approprié de décrire la RFID comme une technologie permettant de collecter des données à l'aide de puces ou étiquettes électroniques sans contact et de transmetteurs sans fil (lecteurs), à des fins d'identification ou autres. Cette définition générale ne reprend pas nécessairement la terminologie employée dans les normes internationales. Elle a néanmoins le mérite d'englober toute la gamme des technologies RFID[7].

Comme nous le verrons plus avant, d'autres facteurs empêchent de donner une définition claire de la RFID. Par exemple, différents types de technologies peuvent être désignées sous l'acronyme RFID, soit parce qu'elles s'appuient sur des communications radio, qu'elles fonctionnent dans la bande de fréquence habituelle de la RFID, ou qu'elles remplissent les mêmes fonctions. Il arrive que des entreprises associent la technologie, les produits ou les services qu'elles proposent à l'acronyme « RFID » pour des raisons d'image ou de marketing et cela peut parfois semer la confusion dans l'esprit du public.

Comprendre les possibilités ou les limites de cette technologie évite d'avoir des craintes injustifiées ou des attentes irréalistes à son égard.

La RFID possède une dimension logicielle qui inclut, par exemple, les composants intermédiaires (*middleware*), des applications d'arrière-plan, et protocoles de communication, etc. Cette dimension ne saurait être négligée si l'on veut comprendre réellement cette technologie. Cependant, la spécificité et la nouveauté de la RFID résident dans ses éléments matériels (puces, lecteurs et communication électromagnétique) qui sont régis par les lois de la physique, comme n'importe quel dispositif matériel. C'est là une différence majeure par rapport aux technologies logicielles (comme par exemple l'extraction

6. Pour une présentation plus détaillée du fonctionnement de cette technologie, voir par exemple Finkenzeller (2003) et Lahiri (2005).

7. À titre d'exemple, les systèmes répondant aux normes ISO 14443 sont rarement désignés par les experts sous l'appellation de systèmes RFID, mais plutôt sous celle de « cartes à circuit intégré sans contact », qui est la terminologie employée dans les normes ISO. Or, ce que l'homme de la rue appelle aujourd'hui un « passeport RFID » est un système conforme à la norme ISO 14443. Ces nuances sont très subtiles pour le grand public.

de données), qui fonctionnent selon des règles établies par les ingénieurs sous forme de normes, et qui sont, par nature, principalement limitées par l'imagination de leurs concepteurs.

L'expérience montre que les limites des technologies de l'information ne sont souvent que provisoires et sont généralement dépassées par de nouvelles avancées technologiques. Pour la plupart des technologies de l'information, les limites théoriques sont encore loin d'être atteintes par les ingénieurs, comme on le voit par exemple avec Internet. Cela laisse donc supposer que les technologies RFID connaîtront elles aussi des progrès, que leurs lacunes actuelles seront comblées et que certaines de leurs fonctions, aujourd'hui peu étendues et donc acceptables, feront tôt ou tard l'objet de découvertes technologiques qui en repousseront les limites. La taille des puces et des lecteurs, de même que la portée des communications, sont des exemples typiques de cette logique. Certes, il continuera d'y avoir des progrès technologiques, mais les lois de la physique continueront d'imposer des limites à ce que la technologie peut et ne peut pas faire. Il est donc important de savoir où sont situées ces limites que les lois de la physique imposent à l'évolution technologique. Le fait d'indiquer clairement quelles caractéristiques de la RFID sont susceptibles d'évoluer ou non aidera à définir des politiques adaptées et permettra peut-être de rompre les résistances du public sans freiner l'innovation.

Pour les scientifiques et autres experts, la RFID est une technologie de l'information définie par plusieurs normes. Ainsi, la série de normes adoptées par l'Organisation internationale de normalisation (ISO) est considérée par certains comme la référence principale pour la RFID[8]. Plusieurs autres normes concernent également cette technologie, et leur liste se renouvelle constamment[9].

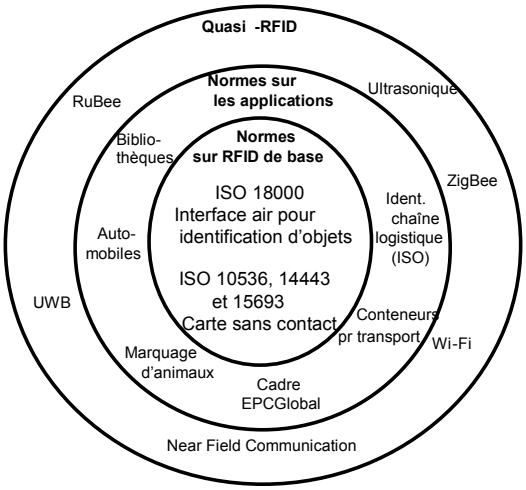
Certaines technologies sont parfois présentées comme des alternatives à la RFID. Elles pourraient être considérées comme des variantes du concept, ou des « quasi-RFID ». Il s'agit notamment des technologies NFC (« Near Field Communication »), RuBee, ZigBee, Wi-Fi et UWB (« Ultra Wide Band »), et d'innovations telles que le « Memory Spot » de HP. Certaines d'entre elles (RuBee, par exemple) ne sont pas complètement normalisées. D'autres (telles que NFC) ne sont pas désignées sous l'appellation RFID par leurs concepteurs, peut-être notamment pour ne pas porter confusion auprès du public. D'autres en revanche (comme Wi-Fi) sont assimilées à la RFID, non pas sur le plan technique mais fonctionnel[10].

8. Les normes ISO concernent notamment les paramètres de l'interface radio pour l'identification d'objets (série ISO 18000), ainsi que les cartes sans contact à couplage rapproché, de proximité et de voisinage (ISO 10536, 14443 et 15693). D'autres normes ISO couvrent des applications spécifiques, comme par exemple le marquage des animaux (ISO 11784, 11785 et 14223) ou l'identification automatique des conteneurs pour le transport de marchandises (ISO 10374). Les normes ISO définissent souvent les différentes structures de données utilisées, comme par exemple le « modèle de données utilisé pour l'identification par radiofréquence (RFID) dans les bibliothèques », en cours de développement (ISO/NP 28560), ou la norme ISO 15963 (« Identification unique des tags RF ») et d'autres normes ISO relatives à la chaîne logistique (Oehlmann, 2006 ; Rees, 2004).

9. L'annexe I donne un bref aperçu des normes relatives à la RFID.

10. L'annexe II décrit les capacités de ces technologies.

Figure 1. Normes sur la RFID, du concept de base jusqu'aux variantes de la technologie
Voir les annexes I et II pour les références des normes



1.2. Composants matériels

Les puces et les lecteurs sont les composants matériels de base d'un système RFID.

1.2.1. Puces

Les puces RFID, également appelées transpondeurs, peuvent être classés en plusieurs catégories selon toute une série de caractéristiques. Ainsi, on fait généralement une distinction entre les puces actives et passives. La capacité de mémoire et les fonctions de lecture-écriture sont d'autres critères de distinction. À l'avenir, les puces offriront certainement de nouvelles possibilités. Il ne faut pas les confondre avec les objets auxquels ils sont attachés ou dans lesquels ils sont insérés.

1.2.1.1. Puces actives ou passives

Les puces passives ne disposent pas d'une source d'alimentation interne et ne peuvent pas envoyer de signaux vers l'extérieur sans recevoir de l'énergie d'un lecteur. Elles utilisent un signal radio entrant pour activer un circuit intégré et transmettre une réponse. Leur antenne doit être capable à la fois de recevoir l'énergie d'un signal entrant et d'envoyer un signal de sortie (voir ci-dessous). Leur dimension peut varier de 0.15 mm (voir Figure 2, image de droite) à celles d'une carte postale, la taille de leur antenne étant le principal critère déterminant. Leur durée de vie est quasiment illimitée : elles peuvent être réactivées plusieurs années après leur fabrication. Les systèmes fonctionnant sur des basses fréquences (LF) et hautes fréquences (HF) sont passifs. Ceux opérant sur les ultra-hautes fréquences (UHF) et les microondes peuvent être passifs ou actifs.

Figure 2. Etiquettes et puces RFID

Gauche : étiquette avec puce passive destinée à un produit de consommation.
Droite : puce Hitachi disposée à côté de grains de sel (0.15 x 0.15 x 7.5 micromètres, sans l'antenne)

Source : Gauche : site Internet de Metro Group Future Store ; Droite : Hitachi[11].

Contrairement à leurs homologues passives, les puces actives disposent de leur propre source d'énergie pour alimenter le circuit intégré, qui génère un signal de sortie. Cette source d'alimentation supplémentaire procure aux puces actives plusieurs avantages par rapport aux passives, et entraîne une série de conséquences, dont les suivantes (QED Systems, 2002) :

- *Force du signal* : les puces actives peuvent recevoir du lecteur des signaux d'une très faible intensité. En revanche, les puces passives ne peuvent recevoir que des signaux très puissants – jusqu'à 1 000 fois plus que ceux nécessaires pour les puces actives – et la force du signal qu'elles renvoient est très faible.
- *Ouverture de la communication* : les puces passives ont besoin qu'un lecteur leur envoie un premier signal pour établir la communication, alors que les puces actives peuvent démarrer elles-mêmes la communication. Ces dernières peuvent ainsi être programmées pour envoyer des données (par exemple, les données sur l'environnement enregistrées par un capteur) à des moments précis ou lorsque des événements externes se produisent.
- *Distance entre la puce et le lecteur* : elle est plus faible pour les puces passives que pour les puces actives. La lecture est possible depuis quelques centimètres jusqu'à plusieurs mètres pour les puces passives, et jusqu'à plusieurs centaines de mètres pour les puces actives. La distance par rapport au lecteur dépend de plusieurs facteurs, dont la taille de l'antenne. Pour doubler la distance de lecture d'une puce passive, il faut 16 fois plus de puissance du côté du lecteur. En revanche, pour doubler cette distance dans le cas d'une puce active, il ne faut que quatre fois plus de puissance, car les puces actives possèdent une pile interne.
- *Capteurs de paramètres environnementaux* : les puces actives et passives peuvent être associées à des capteurs pour contrôler l'environnement. Les puces passives ne peuvent cependant utiliser leur capteur que si un lecteur leur envoie un signal. À l'opposé, les puces actives peuvent mesurer les paramètres environnementaux en permanence – même en l'absence de lecteur dans le périmètre – stocker les données du capteur et les informations de date et d'heure, puis les envoyer à un lecteur à un moment précis ou sur demande.
- *Capacité de lecture-écriture* : des moyens technologiques sont mis en œuvre pour permettre aux puces actives et passives de stocker les informations envoyées par le lecteur. Cependant, les contraintes d'alimentation limitent généralement les capacités de traitement des données des puces passives qui, de plus, possèdent normalement peu

11. La puce Hitachi est capable de transmettre un numéro d'identification unique de 128 bits ($3.4x10^{38}$). Elle a été utilisée pour les 22 millions de tickets qui ont été émis à l'occasion de l'Exposition universelle de 2005, avec un taux d'erreur de reconnaissance des tickets de 0.001 %. Voir : www.hitachi.com/New/cnews/060206.html.

d'espace mémoire. De leur côté, les puces actives ont notamment la capacité d'utiliser des protocoles plus complexes, ce qui réduit par exemple les erreurs de transmission.

Par ailleurs, la *durée de vie* des puces actives est conditionnée à celle de leur pile, qui dépend à son tour de la fréquence avec laquelle la puce en question est sollicitée pour traiter et/ou envoyer des informations[12]. Enfin, et il faut le souligner, les puces actives sont *plus grandes* et *plus chères* que les puces passives[13]. On pense que pour pouvoir exploiter toutes les possibilités du marquage d'articles, et donc permettre à la RFID de se développer davantage, il faudra que les puces deviennent moins coûteux qu'aujourd'hui. Certains experts estiment que des puces au bon rapport qualité-prix feront leur entrée sur le marché d'ici deux ou trois ans, et qu'ils auront d'importantes répercussions sur l'efficacité et l'économie du commerce de détail.

1.2.1.2. Capacité de mémoire des puces

Un autre critère de distinction entre les différents types de puces est sa capacité de mémoire. La mémoire dont dispose en moyenne une puce d'identification passive bon marché est comprise entre 64 bits et 1 Ko. Les puces plus coûteuses, généralement actives, peuvent contenir plus de 128 Ko de données[14]. Les puces les plus simples utilisées pour le marquage d'articles dans le commerce de détail contiennent généralement 96 bits (12 octets) de données qui servent uniquement à inscrire l'identifiant unique du produit[15]. Les puces RFID des passeports stockent normalement les données biométriques du titulaire (photo du visage et éventuellement image de l'iris et/ou empreinte digitale) ainsi que les informations relatives au passeport dans une mémoire de 32 Ko.

1.2.1.3. Accès à la mémoire des puces

Les puces en lecture seule contiennent des informations qui y sont gravées une fois pour toutes et qui peuvent être ensuite consultées par les lecteurs, mais qui ne peuvent être ni écrasées, ni effacées. En revanche, les données stockées sur des puces en lecture-écriture peuvent être lues, modifiées et effacées par les lecteurs. Certains prétendent que les lecteurs sont mal nommés, car ils peuvent en l'occurrence lire, mais aussi écrire dans la puce.

Les puces passives en lecture seule qui sont dotées de peu de mémoire conviennent tout à fait pour le marquage de produits, de caisses ou de palettes. Lorsque la puce ne peut stocker que l'identifiant unique, toutes les autres informations relatives au produit peuvent être enregistrées dans des bases de données. Cette solution ne requiert donc pas une capacité d'écriture sur la puce, mais plutôt une connexion à la base de données lorsque des informations autres que le numéro d'article sont nécessaires à un certain stade de la chaîne logistique. Les différentes puces utilisées dans les différents contextes peuvent disposer d'une capacité de mémoire et de lecture-écriture beaucoup plus importante. Cela peut par exemple être utile lorsque la connexion à une base de données n'est pas possible ou pas souhaitable, lorsque la puce est réutilisée à d'autres fins, ou pour des applications ne se limitant pas à une simple identification (FTC, 2005, p. 7). À titre d'exemple, le bracelet délivré aux patients hospitalisés devra, pour contenir l'historique

12. Dans certaines configurations, la durée de vie d'une puce active et de sa pile peut aller jusqu'à dix ans.

13. De cinq à plusieurs centaines d'euros, contre moins de EUR 0.50 pour les puces passives (IDTechEx, 2005).

14. Une mémoire de 128 Ko peut paraître très petite par rapport aux mémoires de plusieurs giga-octets que possèdent aujourd'hui les clés USB ou lecteurs MP3 de base. Toutefois, la première version du PC IBM lancé en 1981 présentait une mémoire de seulement 16 Ko, extensible jusqu'à 256.

15. Voir l'annexe IV pour une description de la structure du code électronique de produit mis au point par EPCglobal (disponible en anglais uniquement).

actualisé de la courbe des températures, disposer d'une fonction de lecture-écriture. Enfin, il existe des puces hybrides, qui possèdent un espace mémoire réservé aux informations en lecture seule, et un autre pour les opérations de lecture et d'écriture.

1.2.1.4 Classification des puces RFID par Auto-ID Labs et EPCglobal

Auto-ID Labs et EPCglobal ont mis au point une classification des puces RFID. Cette classification, qui s'est affinée au fil du temps (Tableau 1), est souvent citée en référence dans les documents consacrés à la RFID.

Tableau 1. Classification des puces RFID par Auto-ID Labs

Catégorie	Description
0	Identifiant uniquement ; programmé lors de la fabrication ; lecture seule sur le terrain
1	Identifiant uniquement ; écriture unique, lectures multiples (WORM)
2	Catégorie 1, plus mémoire supplémentaire et/ou chiffrement
3	Catégorie 2, plus alimentation complémentaire par pile et capteurs
4	Puces actives (alimentés par pile)
5	Catégorie 4, plus capacité de lecture

Source : EPCglobal.

Tableau 2. Différences entre les technologies des puces passives et actives

	Puces passives	**Puces actives**
Pile	Non	Oui
Source d'alimentation	Énergie provenant du lecteur	Interne
Disponibilité de la source d'alimentation	Uniquement dans le champ d'un lecteur activé	Permanente
Force du signal requise du lecteur vers la puce	Élevée (le signal doit alimenter la puce)	Faible (sert uniquement à acheminer les informations)
Force du signal de la puce vers le lecteur	Faible	Élevée
Portée des communications	Faible à très faible (3 mètres, voire moins)	Longue (100 mètres ou plus)
Durée de vie de la puce	Très longue	Conditionnée par la durée de vie de la pile (dépend de la stratégie adoptée en matière d'économie d'énergie)
Taille moyenne de la puce	Petite	Grande
Collecte de données de plusieurs puces	- Des centaines de puces dans un rayon de trois mètres autour d'un seul lecteur - 20 puces se déplaçant à une vitesse inférieure ou égale à 8 km/h	- Des milliers de puces sur un périmètre de plus de 28 000 m^2 autour d'un seul lecteur - 20 puces se déplaçant à une vitesse de plus de 160 km/h
Fonctionnalité du capteur	Capacité à lire et à transférer les valeurs des puces uniquement lorsque la puce est alimentée par le lecteur ; aucune information sur la date/l'heure	Capacité à assurer un contrôle permanent et à enregistrer les données du capteur ; indication de la date/l'heure pour les événements survenant au niveau du capteur
Stockage des données	Petite capacité de mémorisation des données en lecture/écriture (octets)	Grande capacité de mémorisation des données en lecture/écriture (kilo-octets), avec des fonctionnalités avancées de recherche des données
Applications courantes	Processus de gestion rigides, mouvement des ressources limité, sécurité et détection élémentaires. Sécurité du fret peu élaborée (simple détection ponctuelle des effractions), fortes répercussions sur le processus de gestion. Marquage individuel des articles, valises, boîtes, cartons, palettes. Étiquettes imprimées.	Processus de gestion dynamiques, mouvement des ressources non limité, sécurité/détection, stockage/enregistrement des données. Transport intermodal : bateau, train, camion. Surveillance de zone, lecture de plusieurs puces à grande vitesse aux portes d'accès, sécurité du fret très élaborée (détection continue des effractions, indication de la date/l'heure), manifeste électronique.
Coût	Faible (moins de EUR 0.5)	Élevé (entre cinq et plusieurs centaines d'euros)

Source : Adapté de QED Systems (2002).

1.2.1.5 Futures puces

La recherche se poursuit dans le domaine des puces RFID. Certains analystes prédisent par exemple un énorme succès pour les étiquettes RFID sans puce qui, dépourvues de ce dispositif en silicium, pourront être imprimées directement sur les produits et les emballages pour un coût minime (IDTechEx, 2006b).

1.2.2. Lecteurs

Les lecteurs, souvent appelés « interrogateurs », sont le pendant des puces RFID et peuvent, comme ces derniers, présenter des caractéristiques techniques extrêmement variées. Dans un scénario type, le lecteur envoie un signal « à la puce et attend sa réponse. La puce détecte le signal et envoie une réponse qui contient un numéro de série ainsi qu'éventuellement d'autres informations. Dans les systèmes RFID de base, le signal du lecteur fonctionne comme un interrupteur marche-arrêt. Dans les systèmes plus sophistiqués, le signal radio du lecteur peut contenir des commandes destinées à la puce, des instructions pour effectuer des opérations de lecture/d'écriture dans la mémoire de la puce, voire des mots de passe »[16]. Le lecteur peut émettre le signal en permanence – ce qui permet d'être toujours à l'affût des puces présentes dans son environment – ou sous l'effet d'un événement extérieur (comme l'activation par un opérateur) afin d'économiser de l'énergie et de limiter les interférences.

La taille du lecteur, qui dépend de nombreux paramètres, va de celle d'une pièce de monnaie à celle d'un ordinateur de poche (Figure 3). Un lecteur peut être doté de fonctionnalités GPS et de dispositifs de connexion à des systèmes et des réseaux d'information. Son coût est compris entre EUR 100 et 1 000 pour un lecteur de puces passives, et entre EUR 1 000 et 3 000 au moins pour un lecteur communiquant avec des puces actives sur de longues distances (*RFID Journal*, sans date).

Figure 3. Lecteurs RFID
Lecteur de type pistolet (à gauche), lecteur de type ordinateur (au centre)
et lecteur miniature (12 x 12 x 2 mm) (à droite)

Sources : Intermec (gauche), Alien Technology (centre) et Innovision (droite).

1.3. Communication électromagnétique

La transmission des informations entre les puces et les lecteurs repose sur les lois de l'électromagnétisme. Les lois de la physique qui s'appliquent à la RFID sont les mêmes que pour n'importe quel système radio : pour fonctionner, le lecteur et le récepteur se trouvant sur la puce doivent être capables de détecter le signal qui est envoyé de l'un à l'autre au-dessus des bruits de fond.

Les concepteurs, développeurs, distributeurs et opérateurs de systèmes RFID doivent tenir compte de toutes sortes de paramètres pour que ces dispositifs puissent fonctionner. La bande de fréquences et les lois physiques de la transmission de l'énergie et des informations ont une influence capitale sur le fonctionnement des systèmes RFID. Les autres facteurs importants sont notamment le niveau de puissance, l'antenne, les interférences, la réflexion, l'absorption et le mode de communication (duplex ou semi-duplex). Tous ces éléments déterminent le rayon de fonctionnement d'un système.

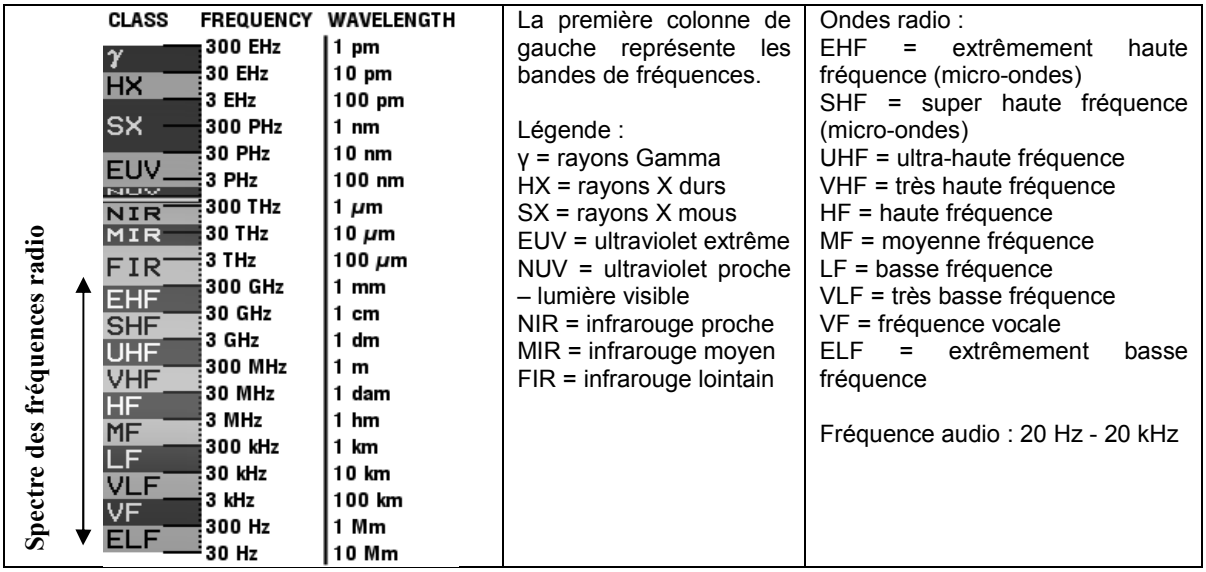
16. Garfinkel (2005), p. 20.

1.3.1. Bande de fréquences

Chaque système RFID fonctionne sur une bande de fréquences bien précise qui détermine les principales possibilités et limites du système ; ces bandes sont présentées de façon synthétique sur la Figure 4. À titre d'exemple, plus la fréquence est élevée, plus l'onde est courte et plus il est difficile pour le signal radio de circuler ou de franchir les obstacles pour atteindre un récepteur. Certains de ces inconvénients sont étroitement liés à d'autres caractéristiques techniques qui sont décrites ci-après.

Le terme « radiofréquence » qui est employé pour la RFID fait référence à l'émission d'énergie à l'intérieur du spectre des fréquences radio[17].

Figure 4. Spectre électromagnétique, fréquences, longueurs d'ondes et énergies



Note : Les fréquences EHF et SHF sont parfois considérées comme ne faisant pas partie du spectre des fréquences radio et comme constituant leur propre spectre de micro-ondes. Le spectre des fréquences radio se situe entre 9 kHz et 300 GHz.

Source : Wikipédia, « Spectre électromagnétique ».

Dès les prémices des communications radio, les pouvoirs publics ont réglementé et contrôlé l'utilisation du spectre des fréquences radio en ce qui concerne les bandes de fréquences et la puissance[18]. L'un des objectifs de cette réglementation est de partager les ressources de ce spectre, qui sont limitées. Un autre est de réduire au maximum les interférences qui peuvent être causées par un système radio sur un autre. Il est par exemple important que les systèmes RFID ne causent pas d'interférences avec la radio et la télévision, les services radio mobiles (police, services de sécurité et d'urgence), les téléphones portables,

17. Le spectre électromagnétique correspond à la gamme de toutes les ondes possibles (voir Figure 4). Le spectre des radiofréquences est la portion du spectre électromagnétique dans laquelle les ondes électromagnétiques peuvent être générées par un courant alternatif transmis à une antenne. Les ondes radio ou électromagnétiques correspondent aux champs électriques et magnétiques oscillants qui sont générés par une antenne alimentée par un courant électrique. La distance entre deux ondes consécutives est appelée « longueur d'onde ». Le nombre d'oscillations complètes d'une longueur d'onde (cycle) en une seconde est représenté par la fréquence, qui se mesure en hertz (Hz), kilohertz (kHz), mégahertz (MHz) et gigahertz (GHz). Ainsi, 132 kHz = 132 000 cycles par seconde.

18. Les premiers débats internationaux sur la réglementation des communications radio ont eu lieu en 1903 à Berlin. La première conférence sur le sujet s'est tenue à Berlin en 1906.

ainsi que les communications maritimes et aéronautiques. Comme nous le verrons plus avant (point 1.3.3), la réglementation limite aussi le niveau de puissance pour des raisons de santé et de sécurité.

Tableau 3. Fréquences et régions

Basse fréquence (LF) 30 - 300 kHz	125 - 134 kHz au Canada, en Europe, au Japon et aux États-Unis
Haute fréquence (HF) 3 - 30 MHz	13.56 MHz au Canada, en Europe, au Japon et aux États-Unis
Ultra-haute fréquence (UHF) 300 MHz - 3 GHz	433.05 - 434.79 MHz dans la plupart des pays d'Europe, aux États-Unis, et en projet au Japon 865 - 868 MHz en Europe 866 - 869 et 923 - 925 MHz en Corée du Sud 902 - 928 MHz aux États-Unis 918 - 926 MHz en Australie 952 - 954 MHz au Japon pour les puces passives, depuis 2005
Micro-ondes 2 - 30 GHz	2400 - 2500 et 5.725 - 5.875 GHz au Canada, en Europe, au Japon et aux États-Unis

Source : Ministère américain du Commerce (2005b).

Les systèmes RFID fonctionnent sur les bandes de basse fréquence (LF), haute fréquence (HF), ultra-haute fréquence (UHF) et micro-ondes. Contrairement à certains systèmes de communication radio qui utilisent des fréquences nécessitant une licence (comme par exemple la téléphonie mobile ou la télévision), les systèmes RFID fonctionnent sur des fréquences particulières sans licence qui ne sont pas totalement harmonisées à l'échelle mondiale, notamment dans la gamme des UHF et des micro-ondes. Le fait que l'on utilise pour la RFID des fréquences différentes selon les régions peut être un défi de taille pour les partisans d'un déploiement planétaire des applications RFID, même si des solutions techniques peuvent résoudre un certain nombre de ces différences (Voir Tableau 3).

1.3.2. Induction électromagnétique et ondes radio

Lorsque l'on soumet un conducteur à un courant électrique, il émet de l'énergie sous forme d'ondes radio. Il produit en outre autour de lui un champ magnétique qui peut être utilisé pour générer de l'électricité par induction. L'induction est la création d'un courant électrique dans un matériau conducteur (généralement une bobine) soumis à un champ magnétique variable. Pour transmettre l'énergie et les informations à un périphérique distant, les systèmes RFID fonctionnant en basses et hautes fréquences utilisent l'induction électromagnétique (ou « couplage inductif »), et ceux opérant dans les bandes UHF et micro-ondes utilisent les ondes radio (ou communications radio)[19].

19. L'induction permet le fonctionnement des générateurs électriques, des moteurs à induction et des transformateurs. Le phénomène d'*induction* se produit dans la zone située entre l'antenne d'un lecteur et moins d'une longueur d'onde de l'onde radio émise par cette antenne. Dans le contexte de la RFID, cette région est souvent appelée le « champ proche » (*near field*). En revanche, dans un système de *communication radio*, le transfert d'énergie s'effectue par propagation des ondes radio, comme dans le cas de la télévision, du téléphone portable, du radar et autres communications radio. La région dans laquelle se produit cette propagation est souvent appelée le « champ lointain » (*far field*, par opposition au « champ proche », région où a lieu le phénomène d'induction magnétique). C'est ainsi que la RFID par induction est parfois désignée comme une « technologie du champ proche », et la RFID par ondes radio comme une « technologie du champ lointain ». Pourtant, contrairement à ce que laisse entendre cette terminologie, le principal facteur distinctif n'est pas le rayon de fonctionnement, mais le phénomène physique qui a lieu. Cela ne signifie pas non plus que les communications établies par induction électromagnétique sont possibles dans l'ensemble du « champ proche ». De nombreux autres facteurs limitent la portée de communication des systèmes à induction électromagnétique à une portion beaucoup plus réduite du « champ proche » théorique. Pour en savoir plus sur les différences entre la RFID par induction électromagnétique et la RFID par ondes radio, se reporter à Langheinrich, 2007.

L'induction et les ondes radio sont deux phénomènes physiques radicalement différents, mais liés, qui ont été découverts par plusieurs scientifiques au XIX^{ème} siècle. Pour les spécialistes de la RFID, ils correspondent à deux domaines techniques très distincts, avec des différences au niveau des capacités, des limites (les distances de fonctionnement, par exemple) et des problèmes qu'ils présentent (interférences, absorption, aspects sanitaires, etc.). Un système dont la communication repose sur l'induction électromagnétique ne peut se transformer en un système radio simplement en changeant la bande de fréquences utilisée et la taille de l'antenne. Il n'existe pas de méthode simple pour passer d'un système reposant sur l'induction magnétique à un système reposant sur la propagation des ondes radio, si ce n'est la reconception totale du système. De la même manière, il n'y a aucun lien technologique entre une lampe à huile et une lampe électrique, bien qu'elles remplissent toutes les deux la même fonction : fournir de la lumière. La technologie qu'elles utilisent est différente, leurs inconvénients ne sont pas les mêmes, et la lumière qu'elles produisent non plus.

1.3.3. Niveau de puissance

Le signal émis par les lecteurs et les puces qui utilisent les ondes radio possède un certain niveau de puissance, mesuré en watts. Plus la puissance du signal transmis en direction du récepteur est élevée, plus il y a de chances que ce signal soit détecté par le récepteur parmi les « bruits de fond ». Un niveau de puissance élevé peut cependant représenter un danger sanitaire de plus en plus grand pour l'être humain : le radar, par exemple, fonctionne généralement à un niveau d'énergie très élevé et peut être dangereux pour une personne se trouvant directement en face de l'antenne. Un niveau de puissance élevé accroît en outre les risques d'interférences avec d'autres équipements sensibles aux ondes radio. Les réglementations adoptées par les pouvoirs publics dans tous les pays imposent des restrictions quant aux niveaux de puissance, afin de protéger la santé des populations et de prévenir les interférences. Les systèmes fonctionnant par induction magnétique obéissent aux mêmes règles, même si, dans la pratique, les distances de fonctionnement rapprochées compensent la faible puissance de la bobine des lecteurs.

1.3.4. Antenne

Le niveau de puissance du lecteur et de la puce peut être considérablement amélioré par la nature de l'antenne et en particulier en fonction de sa conception et son orientation. Les antennes à faible gain[20] émettent des rayonnements répartis de façon égale dans toutes les directions (elles sont omnidirectionnelles). Les antennes à grand gain émettent un rayonnement dans une direction particulière (elles sont unidirectionnelles) ; leur portée est plus grande et leur signal de meilleure qualité, mais elles doivent être disposées avec soin pour pointer dans une direction bien précise. Lorsque l'émetteur ou le récepteur est en mouvement, il n'est pas forcément pratique d'utiliser des antennes directionnelles aux deux extrémités de la liaison de communication. La conception et l'orientation de l'antenne ont également une incidence sur la sensibilité de la puce et du lecteur[21].

20. Le gain mesure la performance d'une antenne dans une direction donnée. Sa valeur est exprimée en décibel (db) par rapport à une antenne de référence théorique, appelée « antenne isotrope ».

21. La sensibilité du récepteur dépend du gain et de l'orientation de l'antenne, comme le montrent les antennes-râteaux et paraboles utilisées pour recevoir la télévision. L'orientation des puces (et surtout leur antenne relativement petite) est parfois plus difficile à régler que celle d'une antenne de télévision. Il arrive fréquemment que le format de la puce et du lecteur ait été conçu de telle façon que l'utilisateur doive orienter l'un ou l'autre correctement (par exemple, les puces insérées dans des cartes à puce et les lecteurs pistolets), afin de remédier aux difficultés de lecture des systèmes de base.

La taille de l'antenne des puces et des lecteurs est une autre différence majeure entre les systèmes RFID par induction et par ondes radio[22]. En règle générale, les puces des systèmes à induction électromagnétique ont besoin d'une antenne plus petite[23] que les systèmes à ondes radio. Dans certains cas, les puces RFID des systèmes reposant sur les ondes radio sont vendus sans antenne, et la taille indiquée par le fabricant ne correspond pas toujours à celle finalement obtenue lorsque la puce est opérationnelle et fixée à un objet[24].

1.3.5. Interférences, atténuation et réflexion

Comme nous l'avons vu plus haut, les communications des systèmes RFID peuvent interférer avec d'autres, notamment lorsque la puissance de transmission est élevée. Les systèmes fonctionnant par couplage inductif sont moins sujets aux interférences en raison d'une atténuation accrue du signal (voir le point 1.3.7 ci-après).

Les signaux de faible fréquence pénètrent plus facilement les liquides car l'atténuation est moindre pour les grandes longueurs d'onde. Les systèmes à basse et haute fréquences sont donc plus appropriés pour le marquage d'objets dans des environnements contenant de l'eau (tels que les humains et les animaux). Le métal stoppe les signaux radio et les réfléchit, créant des interférences. Des progrès sont en cours concernant la gestion des interférences causées par les environnements métalliques. Les systèmes fonctionnant par induction et à basse fréquence peuvent communiquer dans des environnements métalliques, mais sous certaines conditions[25].

Il existe toute une gamme de techniques de correction d'erreur par codage pour atténuer les effets du bruit. Plus les techniques de réduction, d'atténuation et de suppression des bruits mises en œuvre dans la conception du circuit de transmission des données sont complexes, et plus le coût est élevé.

1.3.6. Communication en duplex ou semi-duplex

Le degré de sophistication de la communication dépend du mode utilisé : duplex ou semi-duplex. En mode semi-duplex, l'émetteur envoie un message mais il ne sait pas si le message a été reçu tant que le récepteur ne lui a pas répondu. En mode duplex, les deux extrémités du canal de communication envoient et reçoivent les données simultanément, ce qui permet de gérer le circuit de communication en temps réel et d'utiliser des protocoles plus complexes. Or, ces derniers requièrent plus de fonctionnalités de traitement des données sur la puce, ce qui implique une plus grande consommation d'énergie et un coût plus élevé.

1.3.7. Rayon de fonctionnement

Deux types de lois limitent le rayon de fonctionnement des systèmes RFID : les lois de la physique et celles des pouvoirs publics (réglementations sur la puissance et la fréquence). Les lois de la physique peuvent être exprimées par : *i)* la théorie, exprimée par des équations mathématiques ; *ii)* les expériences

22. La propagation des ondes radio nécessite des antennes dont la taille est généralement égale à la moitié de la longueur d'onde de la fréquence utilisée : 150 cm à 100 MHz, 15 cm à 1 GHz, 5 cm à 2.5 GHz, et 2.5 cm à 5.8 GHz.

23. Dans les systèmes de communication utilisant le couplage inductif, « l'antenne » est en fait une bobine qui génère un champ magnétique, comme dans les transformateurs électriques.

24. La puce Hitachi μChip représentée à la Figure 2 (image de droite) ne comporte pas d'antenne (Hitachi, 2003).

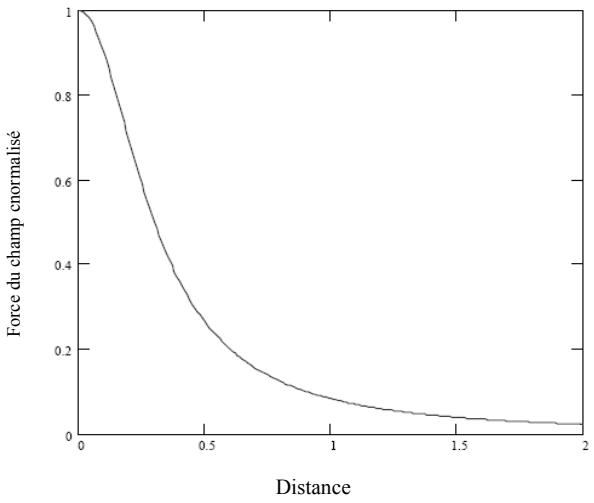
25. Pour des informations sur l'utilisation de puces UHF dans des environnements liquides et métalliques, se reporter à Desmons (2006).

réalisées en laboratoire ; et *iii)* les expériences menées dans un environnement naturel, semblable à la vie réelle. Selon le cadre de référence qui est utilisé parmi ces trois, l'évaluation des distances de fonctionnement des systèmes RFID peut être très différente.

Les distances de fonctionnement obtenues dans le cadre d'un laboratoire sont en général plus grandes que celles enregistrées dans des conditions réelles. Cependant, elles impliquent parfois des contraintes qui seraient difficiles à réunir dans la vie réelle. Ainsi, une bobine d'une taille et d'un poids irréalistes serait nécessaire pour générer un champ magnétique d'une ampleur suffisante pour d'activer une puce haute fréquence situé à seulement quelques mètres. Outre les difficultés techniques, les considérations financières jouent également un grand rôle dans l'offre de matériel fonctionnant sur des distances élevées. La recherche progresse et les coûts évoluent, de sorte que l'on peut espérer que les distances de fonctionnement s'amélioreront au fil du temps, dans les limites fixées par les lois de la physique.

Le principal élément à prendre en compte en ce qui concerne la distance de fonctionnement des systèmes RFID est le type de technologie utilisé : les communications reposant sur l'induction électromagnétique se caractérisent par une distance possible de lecture plus courte que les communications radio[26]. La distance de fonctionnement des systèmes RFID dépend également d'autres facteurs tels que la puissance de transmission, la sensibilité du récepteur, le gain et l'orientation de l'antenne, et les interférences. Les interférences dues à des « bruits » – naturels et causés par l'homme – jouent un rôle important dans les communications radio : à mesure que la distance augmente, le niveau du bruit naturel reste stable et la force du signal diminue. A partir d'une certaine distance, le niveau global de bruit empêche la détection. La portée des communications peut également être réduite par des bruits causés par l'homme à proximité du récepteur.

Figure 5. Évolution type de la force du champ magnétique selon la distance (exemple), avec une antenne de transmission de 0.8 m de diamètre



Source : AIM Frequency Forum (2000).

Selon la terminologie employée dans les normes ISO, les systèmes à couplage inductif sont parfois répartis en deux catégories : les systèmes de proximité et ceux de voisinage. Les cartes de proximité[27] sont

26. Dans les communications radio, la force du signal est divisée par quatre à chaque doublement de la distance parcourue. Dans les communications par induction magnétique, elle est divisée par huit. Voir Langheinrich (2007).

27. ISO 14443.

prévues pour une utilisation dans un rayon de 10 cm (pour une utilisation avec un distributeur automatique, par exemple), et les cartes de voisinage[28] dans un rayon de 1 m (par exemple, pour ouvrir la porte d'un parking sans baisser la vitre de la voiture ; les normes établies par l'OACI pour les passeports biométriques exigent l'utilisation de la norme ISO relative aux cartes de proximité).

Figure 6.

Distances de fonctionnement

Bande de fréquences	Type de système	Portée des communications						
		3 cm	10 cm	30 cm	1 m	3 m	10 m	> 10 m
LF	Passif							
HF	ISO 14443							
	ISO 15693							
UHF	Passif							
	Actif							
Micro-ondes	Passif							
	Actif							

Performances réelles et performances théoriques dans un environnement de laboratoire.

Source : *Atmel Applications Journal,* 2004.

Les puces actives fonctionnant sur les bandes UHF et micro-ondes ont une distance de fonctionnement nettement supérieure aux puces passives, car la pile fournit plus de puissance que le signal radio.

Dans les systèmes radio passifs, le signal allant du lecteur à la puce est généralement plus puissant que celui allant de la puce au lecteur ; il peut aussi être détecté ou reçu sur de plus grandes distances (voir le point 2.1. Sécurité de l'information).

1.3.8. Tableau récapitulatif

Le tableau ci-dessous récapitule et compare les capacités de la RFID selon les bandes de fréquences. Il donne également des exemples des différents domaines dans lesquels on peut trouver soit des systèmes à induction électromagnétique, soit des systèmes radio, le facteur déterminant étant les caractéristiques de chaque technologie.

28. ISO 15693.

Tableau 4. Caractéristiques des technologies RFID

Paramètre	Basse fréquence (LF)	Haute fréquence (HF)	Ultra-haute fréquence (UHF)	Micro-ondes
Bande de fréquences (cf. tableau 3)	30 - 300 kHz	3 - 30 MHz	300 MHz - 3GHz	2 - 30 GHz
Transmission de l'énergie et des données	Induction électromagnétique	Induction électromagnétique	Ondes radio	Ondes radio
Portée de lecture (approximative) des puces passives	En général : 20 cm Maximale : 1.2 m	En général : 20 cm Maximale : 1.2 m	433 MHz : 100 m maxi. 865 - 956 MHz : 0.5 à 5 m	En général : 3 m Maximale : 10 m
Humidité	Aucune incidence	Aucune incidence	Effet négatif	Effet négatif
Métal	Effet négatif	Effet négatif	Aucune incidence	Aucune incidence
Orientation de la puce dans la bonne direction pour la lecture	Pas nécessaire	Pas nécessaire	Parfois nécessaire	Nécessaire
Formes types de la puce	Tube en verre, puce intégrée dans un boîtier en plastique, carte à puce, étiquette à puce	Étiquette à puce, puce à usage industriel	Étiquette à puce, puce à usage industriel	Puce grand format
Domaines d'applications les plus courants	Contrôle d'accès et de parcours, freins, étiquetage dans les laveries, traçabilité des bouteilles de gaz, identification des animaux, anti-vol de voitures	Étiquetage dans les laveries, gestion des ressources, billetterie (ski, sorties, transports publics), suivi et traçabilité, accès multiple, gestion de bibliothèque, passeports, cartes de paiement	Suivi de palettes et de conteneurs	Péage routier, suivi de conteneurs, contrôle de production

Note : l'influence des métaux et des liquides varie selon le produit. La portée de lecture des puces actives dépend dans une très large mesure de la technologie utilisée.

Sources : Adapté de BSI (2005), p. 23 ; Dressen (2004) ; RFID du Groupe METRO, sur le site Internet du groupe ; Ward (2006).

1.4. Composants logiciels et éléments du réseau

Les puces et les lecteurs RFID sont souvent les composants d'un système beaucoup plus vaste qui est, à son tour, l'un des éléments de l'infrastructure des technologies de l'information d'une entreprise, souvent elle-même reliée à d'autres systèmes et réseaux d'information, y compris via Internet. Si l'on prend comme critère le degré de connexion à d'autres systèmes, les systèmes RFID peuvent être répartis en trois catégories :

- Les systèmes autonomes, qui ne sont reliés à aucun autre système et réseau d'information, y compris au sein de la même organisation.

- Les systèmes en boucle fermée, qui permettent d'assurer le suivi d'objets qui ne quittent jamais la société ou l'organisation.

- Les systèmes en boucle ouverte, qui font intervenir plusieurs partenaires, comme par exemple une chaîne de commerce de détail et ses fournisseurs.

Comme indiqué dans le document de l'OCDE intitulé « Identification par radiofréquence (RFID) : facteurs incitatifs, enjeux et considérations »[29], les infrastructures d'information associées à la RFID, en particulier celle fonctionnant en UHF, seront de plus en plus accessibles via les réseaux IP, les intranets privés et Internet.

La notion de « système RFID » ou de « réseau RFID » ne veut pas dire que tous les composants de ces systèmes et de ces réseaux fassent appel à la technologie RFID. Si les puces et les lecteurs sont évidemment les éléments de base de la RFID, certains des autres éléments constitutifs sont en fait des technologies, systèmes, applications ou protocoles préexistants qui ne relèvent pas de la RFID mais l'assistent ou la complètent. Alors que le débat sur la politique à adopter à l'égard de la RFID n'en est qu'à ses débuts, il est important de définir clairement quels sont les composants qui relèvent de la RFID ou lui sont spécifiques, et lesquels ne le sont pas.

L'efficacité des systèmes RFID dans l'infrastructure informatique globale d'une organisation dépend de la capacité du réseau de l'entreprise à acheminer efficacement les informations RFID. Les logiciels *middleware* relient les éléments RFID de base aux applications d'arrière-plan de l'entreprise. Ils permettent d'acheminer les informations depuis l'objet étiqueté jusqu'au cœur de l'infrastructure d'information de l'entreprise. La mise en œuvre en bonne et due forme de ces composants nécessite parfois des investissements et des efforts considérables.

Les critères de normalisation et d'interopérabilité jouent également un rôle essentiel dans le déploiement des systèmes RFID. C'est un aspect important à prendre en compte dans le contexte de mondialisation de l'économie, où la chaîne logistique fait intervenir tout un ensemble de partenaires qui peuvent être répartis dans le monde entier. Comme nous l'avons vu plus haut, des efforts considérables ont été déployés pour rationaliser les technologies RFID et Internet existantes en vue de créer les normes et les composants d'une architecture mondiale capable de transmettre les informations relatives aux objets en temps réel, à mesure que ceux-ci progressent sur la chaîne de production, d'approvisionnement et au-delà.

À titre d'exemple, le cadre architectural mis au point par EPCglobal comprend toute une série de normes sur le matériel, les logiciels et l'interface de données qui sont liées les unes aux autres et ont pour but d'accroître l'efficacité de la chaîne logistique grâce à l'utilisation de codes électroniques de produit (EPC). Le cadre d'EPCglobal permet de mettre en commun les informations relatives aux objets marqués entre les partenaires commerciaux faisant partie de la chaîne logistique mondiale, et d'assurer le suivi individuel des produits en temps réel. Il se compose de cinq types d'éléments : *i)* le code électronique de produit (EPC ou *Electronic Product Code*), qui identifie le produit marqué[30] ; *ii)* des puces et des lecteurs ; *iii)* des composants *middleware* qui communiquent les informations lues aux services d'information sur les EPC ; *iv)* les services d'information sur les EPC[31], qui permettent aux partenaires commerciaux d'échanger des données relatives aux EPC sur le réseau d'EPCglobal ; enfin, *v)* des services de recherche, dont l'ONS (Object Naming Service), qui peuvent être sollicités en utilisant l'EPC contenu dans une puce RFID et

29. OCDE (2006a), p. 18.

30. Voir l'annexe IV.

31. EPCglobal a récemment ratifié sa norme publique concernant les services d'information sur les EPC. Voir : www.epcglobalinc.org/standards/EPCglobal_EPCIS_Ratified_Standard_12April_2007_V1.0.pdf

permettent de connaître l'adresse spécifique de l'application associée au code du produit[32]. Le cadre architectural d'EPCglobal comporte également un dispositif de sécurité permettant l'authentification du système, la protection des données et le contrôle d'accès.

D'autres systèmes de numérotation ont été proposés pour identifier les objets, comme par exemple l'adressage IPv6, qui peut gérer pas moins de 430 quintillions d'identifiants[33].

32. L'ONS est un mécanisme permettent d'obtenir des informations sur un produit et des services connexes. L'architecture et le fonctionnement de l'ONS sont très similaires au système de nom de domaine (DNS) Internet. Lorsqu'il est interrogé sur un EPC, l'ONS racine transmet la demande aux serveurs du membre du réseau d'EPCglobal associé à ce code. Le demandeur peut ensuite – et indépendamment de l'ONS racine – obtenir les informations demandées de l'un des serveurs précités. Les données gérées par l'ONS racine se limitent à : *i*) un numéro émis par EPCglobal (« EPC Manager ID »), qui identifie le membre du réseau d'EPCglobal, et *ii*) l'identifiant du serveur de ce membre du réseau d'EPCglobal. EPCGlobal a sélectionné VeriSign pour gérer en son nom le serveur racine autorisé du réseau EPC. Voir EPCglobal (2005b), Section 7.3.

33. Soit 3.4 x 1 0^{38} adresses. Pour en savoir plus sur l'utilisation de l'IPv6 comme système de numérotation pour la RFID, voir *RFID Journal* (2003) ; Vadhia (2004) ; Le Pallec (2005).

2. SÉCURITÉ DE L'INFORMATION ET VIE PRIVÉE

La technologie RFID est parvenue à un stade de développement où la sécurité de l'information et la protection de la vie privée ont été reconnues comme des obstacles à la généralisation de son utilisation.

Selon de nombreux experts de la RFID, le déploiement à grande échelle de cette technologie prendra du temps, mais les applications qui sont en cours de mise en œuvre et les normes qui sont en train d'être conçues et adoptées pourraient bien influer sur l'infrastructure qui sera utilisée dans les prochaines décennies[34]. Pour Ari Juels[35], expert dans les questions de sécurité, « la RFID conçue en 2005 – avec toutes ses fonctionnalités et ses lacunes – risque de prédominer en 2020 ». De la même manière, les participants au Forum de prospective sur la RFID organisé par le Comité PIIC de l'OCDE ont reconnu que les questions de protection de la vie privée et de sécurité devraient être intégrées à l'infrastructure de la RFID avant le déploiement à grande échelle de cette technologie, plutôt que d'avoir à les traiter par la suite, comme cela s'est produit pour Internet. Il a été souligné que dans le cas d'Internet, la sécurité avait dû être ajoutée après coup au lieu d'être incorporée dès le départ, et qu'il ne fallait pas que l'histoire se répète avec la RFID. On peut faire le même constat en ce qui concerne la protection de la vie privée.

La communauté des experts semble être d'accord sur le fait que les questions de sécurité et de protection de la vie privée que pose la RFID devraient être traitées en priorité et de toute urgence par l'ensemble des parties prenantes afin d'empêcher le rejet à grande échelle de cette technologie par les consommateurs et les particuliers, et de favoriser un déploiement réussi des systèmes RFID à venir. « La collecte et l'utilisation, au moyen des technologies RFID, d'informations nominatives constituent un défi majeur en matière de politiques publiques pour le déploiement et l'utilisation des technologies RFID. »[36] Comme l'a indiqué la Commission européenne dans sa communication sur la RFID en Europe, « un cadre juridique et politique clair et fiable est nécessaire pour que cette nouvelle technologie puisse être acceptée par les utilisateurs ». Certaines organisations de défense des consommateurs considèrent que dans des domaines comme le commerce de détail, la RFID pourrait provoquer des réactions hostiles de la part de la population, et établissent un parallèle avec ce qui s'est produit pour les produits alimentaires génétiquement modifiés[37]. L'enjeu ici est la capacité de ces politiques à venir à bout des résistances du public à l'égard de la RFID, et à garantir pour l'avenir la sécurité et la protection de la vie privée.

2.1. Sécurité de l'information

Les chercheurs universitaires et les spécialistes de la sécurité, souvent cités dans la presse, ont appelé l'attention sur les lacunes en matière de sécurité – à la fois théoriques et concrètes – qui ont été constatées sur certains systèmes RFID pourtant largement répandus. L'annexe III fournit une sélection d'exemples de piratages, qui laissent à penser que les systèmes RFID peuvent être vulnérables à certaines attaques tout comme d'autres systèmes d'information et que la technologie RFID en est encore à ses balbutiements.

34. FTC (2005), pp. 11 et 15 ; EPCglobal (2004a).

35. Juels (2005b).

36. Ministère du Commerce des États-Unis (2005b).

37. Lace (2004).

Des attaques ont été perpétrées avec succès sur des produits ou applications RFID déployés à grande échelle[38] et/ou ont pu causer des préjudices à des sociétés et des particuliers (comme par exemple des clés de chambres d'hôtels ou des puces implantables). Cependant, elles concernaient pour la plupart des systèmes RFID bon marché qui comportaient un dispositif de sécurité restreint, voire aucun. En revanche, rares sont les exemples d'attaques réussies contre les systèmes RFID plus coûteux dotés de fonctionnalités de sécurité élaborées. Il serait donc risqué de dresser un bilan général de la sécurité des technologies RFID en s'appuyant uniquement sur les cas de produits RFID bon marché. Pour tirer des conclusions, une analyse plus pointue et plus approfondie est nécessaire.

La présente section donne un aperçu général des problèmes que pose la RFID en matière de sécurité, et des éventuelles solutions. Elle n'est pas censée être détaillée ni exhaustive. Les menaces y sont exposées dans les grandes lignes, avec quelques exemples spécifiques décrits à l'annexe III ; les risques que présentent généralement les systèmes RFID, et certaines des déficiences générales que pourraient avoir ces systèmes et qui pourraient être exploitées, sont présentés du point de vue des gestionnaires de l'entreprise.

2.1.1. Typologie des risques

Les risques résultent des menaces représentées par l'exploitation de vulnérabilités ou de faiblesses qui, lorsqu'elles sont exploitées, ont des conséquences négatives. Il existe de nombreuses manières de décrire les risques associés aux systèmes RFID. Ainsi, le document « Guidelines for Securing RFID Systems » (2007) du *National Institute of Standards and Technology* (NIST) des États-Unis s'intéresse aux risques que présentent ces systèmes pour le processus de gestion, les informations confidentielles de l'entreprise, la vie privée et les ressources externes (Tableau 5).

Tableau 5. Typologie des risques selon le *National Institute for Standards and Technology* des États-Unis

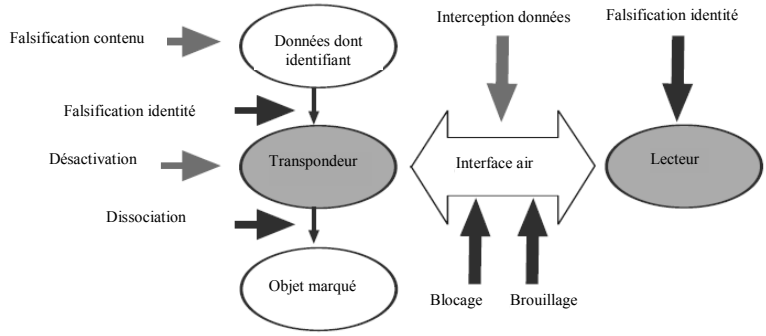
Risques pour le processus de gestion	Des attaques visant directement les composants du système RFID pourraient bouleverser le processus de gestion que le système est censé permettre.
Risques pour les informations confidentielles de l'entreprise	Un adversaire ou un concurrent pourrait accéder de façon abusive aux informations générées par le système RFID et les utiliser pour nuire à l'entreprise qui a mis en œuvre ledit système.
Risques pour la vie privée	Les droits ou les attentes relatifs au respect de la vie privée des personnes risquent d'être mis à mal si un système RFID utilise des informations considérées comme nominatives à des fins autres que celles prévues ou perçues à l'origine. La détention par les personnes de puces fonctionnelles représente également un risque pour la vie privée car ces puces peuvent être utilisées pour suivre les détenteurs des objets marqués.
Risques pour les ressources externes	La technologie RFID peut représenter une menace pour les systèmes, les ressources et les personnes qui n'utilisent pas la RFID mais sont installés en réseau ou au même endroit.

Source : NIST (2007).

Le Bureau fédéral allemand pour la sécurité de l'information (BSI) classe les principaux types d'attaques selon qu'elles interviennent dans les relations données/puce, puce/objet marqué et puce/lecteur (voir Figure 7).

38. Par exemple, le « Digital Signature Transponder » de Texas Instruments.

Figure 7. Principaux types d'attaques intervenant dans les relations données/puce, puce/objet marqué et puce/lecteur



Note : « transpondeur » est un équivalent plus technique des termes marqueur, puce ou étiquette RFID.

Source : BSI (2005).

Le BSI répertorie également les types d'attaques selon leur finalité : espionnage, tromperie, déni de service et protection de la vie privée[39] (Tableau 6).

Tableau 6. Types d'attaques selon leur finalité

	Espionnage	Tromperie	déni de service	Protection de la vie privée
Falsification du contenu		■		
Falsification de l'identité de la puce		■		
Désactivation		■	■	■
Dissociation		■		■
Interception des données	■			
Blocage		■	■	■
Brouillage		■	■	■
Falsification de l'identité du lecteur	■			

Source : BSI (2005).

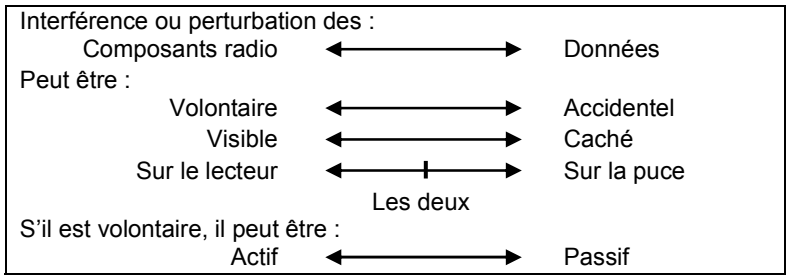
39. Selon le BSI, une attaque visant à protéger la vie privée pourrait être perpétrée par une personne qui considère que sa vie privée est menacée par le système RFID. On peut penser qu'une telle attaque viserait le système lui-même, et non les informations qu'il serait susceptible de contenir. Le « RSA Blocker Tag » (Juels, 2003) est un exemple de moyen pouvant être utilisé pour ce type d'attaque.

Les problèmes de sécurité que pose la RFID peuvent aussi être classés selon les critères classiques qui définissent la sécurité de l'information : perte de disponibilité, d'intégrité et de confidentialité[40]. Les exemples suivants permettent de mieux comprendre la nature des risques généralement associés à chacun de ces critères, et illustrent les éventuelles conséquences des attaques. Ils concernent notamment les réseaux de transport (cartes d'accès au métro), les chaînes logistiques (suivi des conteneurs, des palettes et des marchandises), le commerce de détail (gestion des stocks, règlement, services de garantie, marquage des médicaments), les documents d'identité (passeports, par exemple) et l'ouverture/le démarrage des véhicules. Ces applications n'ont pas été choisies parce qu'elles sont plus risquées que d'autres mais parce qu'elles sont courantes et faciles à comprendre.

Un grand nombre des menaces et des lacunes des systèmes RFID sont communes à l'ensemble des systèmes d'information. La principale caractéristique qui distingue les systèmes RFID des autres dispositifs est qu'une transmission d'informations a lieu entre les puces et les lecteurs. Il ne faut toutefois pas négliger les risques qui sont associés à d'autres composants – plus traditionnels – du système. Il est important de noter que les risques pour la sécurité deviennent dans de nombreux cas des menaces pour la vie privée lorsque les informations concernent des personnes identifiées ou identifiables.

2.1.1.1. Risques associés aux puces et aux lecteurs

Un certain nombre d'événements peuvent avoir un effet perturbateur sur les systèmes RFID. On peut alors parler d'interférence ou de perturbation, que ce soit du matériel, des composants radio ou des données du système. Cette interférence ou cette perturbation des composants physiques des lecteurs et des puces peut étre volontaire ou accidentelle, visible ou caché. Le bouleversement accidentel ou volontaire des composants radio peut concerner le lecteur, la puce ou les deux. Les attaques volontaires peuvent être actives ou passives. L'interférence ou la perturbation des données peut toucher le lecteur, la puce ou les deux.



Comme cela a été mentionné plus haut, les systèmes RFID comportent, comme n'importe quel système d'information, des composants matériels et logiciels. Leur spécificité réside cependant dans leur matériel – les puces et les lecteurs – et dans les méthodes de transfert d'énergie qu'ils utilisent pour communiquer.

- Disponibilité

La disponibilité est la garantie, pour les utilisateurs autorisés, de pouvoir accéder rapidement et en toute fiabilité à des services de données. Elle offre la certitude que les informations ou les ressources seront

40. Disponibilité, intégrité et confidentialité sont des distinctions théoriques utiles, mais dans la réalité, cette séparation est souvent artificielle : une défaillance au niveau de l'un de ces critères peut avoir des répercussions sur un autre, d'où l'interdépendance et le chevauchement de ces concepts. Ces critères sont souvent associés aux notions de responsabilité et traçabilité (audit). Celles-ci garantissent la désignation d'un responsable pour un mécanisme de sécurité donné et fournissent des moyens pour vérifier et mesurer son efficacité.

disponibles en cas de besoin. Prenons l'exemple des attaques par déni de service, dont l'objectif est de réduire la disponibilité d'un système. Les conséquences de ces attaques sur des systèmes RFID courants pourraient être notamment : des retards dans le traitement des documents d'identité (dans le cas, par exemple, de passeports RFID désactivés) qui pourraient perturber les processus de contrôle douanier dans les aéroports, l'impossibilité pour certaines personnes de prendre les transports en commun (dans le cas d'une carte d'accès au métro) ou de pénétrer sur leur lieu de travail (dans le cas de cartes de contrôle d'accès), l'impossibilité pour le détenteur d'un véhicule de monter à bord (dans le cas de clés de voiture RFID), ou le blocage du traitement automatique des informations relatives à des médicaments, pouvant entraîner des erreurs graves pour les patients (dans le cas du marquage des médicaments).

Les attaques visant à réduire la disponibilité des composants physiques d'un système RFID peuvent être visibles ou cachées. Les attaques visibles contre les puces consistent notamment à couper le circuit électrique qui se trouve sur la puce, à détacher la puce de l'objet marqué, à décharger la pile d'une puce active, ou à masquer l'antenne (lui faire écran) à l'aide d'une peinture ou d'un matériau conducteur. Ces stratégies peuvent avoir pour but d'échapper aux systèmes RFID anti-vol installés dans les magasins. Elles peuvent aussi être employées pour protéger la vie privée : des sociétés ont mis au point des portefeuilles (pour les cartes de crédit RFID) et des étuis pour passeports qui bloquent l'identification RFID et sont présentés comme des moyens de protection de la vie privée[41].

Les attaques cachées peuvent consister à surcharger les composants récepteurs afin de les empêcher de fonctionner ou de les détruire, par exemple en soumettant une puce passive à un champ d'énergie très puissant situé à proximité. Des passionnés de l'informatique ont démontré que le champ de forte puissance généré par la lumière flash d'un appareil photos jetable bon marché qui avait été trafiqué pouvait produire ce résultat[42].

Les atteintes aux systèmes RFID peuvent également se traduire par la surcharge du signal utile du côté du récepteur (blocage), par le fait d'empêcher le dispositif de réception de décoder le signal (masquage), ou par la perturbation de la transmission des données (brouillage). Pour citer un exemple, la création d'un bruit intempestif sur l'un ou l'ensemble des circuits de réception du système RFID peut empêcher les puces de détecter le signal utile qui provient du lecteur. Il est en outre possible de modifier le signal de façon à empêcher le lecteur ou les puces de se synchroniser avec d'autres transmetteurs, ce qui a pour effet de bouleverser le processus de décodage du signal utile[43]. Les sources de brouillage peuvent être des interférences accidentelles d'origine humaine provenant de machines et autres appareils électriques. Un pirate peut également créer volontairement des bruits. Dans ce cas, le signal utile est en concurrence avec un signal brouilleur, et c'est l'opposition entre la puissance et la géométrie relatives (obstacles, distances et orientation) du premier et du second qui détermine l'amplitude de la perturbation. La complexité de cette situation est telle qu'une attaque délibérée peut être difficile à détecter. Elle peut donc être perpétrée en

41. Voir par exemple le site Internet de DIFRwear.

42. RFID-Zapper, voir https://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN).

43. Le décodage est une étape capitale du traitement du signal. La détection est le simple fait de recevoir un signal situé au-dessus du seuil de bruit. Le processus de décodage extrait les données du signal détecté. Pour commencer à fonctionner, le décodeur doit d'abord se synchroniser avec le signal entrant. Cela suppose généralement la reconnaissance d'une chaîne de bits qui marque le démarrage de l'opération de décodage. En l'absence de quoi, il est impossible de savoir où est le début ou la fin d'un mot (octet). Un instrument de brouillage intelligent peut envoyer un signal très court pour perturber ce processus, et utiliser un bit de blocage sans perturber la totalité du signal. Le décodeur engagera alors un cycle complet et essaiera de recommencer. L'instrument de brouillage intelligent connaît ce cycle et répétera son action afin d'empêcher le récepteur de décoder le signal (même s'il peut le détecter). Il convient de ne pas confondre le décodage avec le déchiffrement/décryptage cryptographique.

cachette sans que le système RFID ne s'en aperçoive. Ces attaques sont une menace à la fois pour les puces actives et passives.

- Intégrité

L'intégrité est l'assurance implicite que les données n'ont pas été altérées au cours de la transmission, entre le point d'émission et le point de réception. Sur les systèmes RFID classiques, les conséquences d'une perte d'intégrité peuvent être par exemple des retards et des erreurs d'aiguillage dans la chaîne logistique, ou la confusion des opérations commerciales à cause d'informations endommagées ou erronées. Il arrive que la perte d'intégrité entraîne la perte de disponibilité. Par exemple, des cartes de transport détériorées ne permettront pas à leurs détenteurs d'accéder au réseau. De même, en cas d'altération des informations contenues sur la clé de contact d'une voiture, l'accès au véhicule sera certainement impossible.

Un signal brouilleur peut également être créé artificiellement pour injecter un faux signal et ainsi compromettre l'intégrité du système. L'identité d'un lecteur peut être falsifiée dans le but d'accéder à une puce, de la modifier ou de la détruire. Pour citer un exemple, une commande de désactivation (« kill ») pourrait être envoyée avant que la puce ne soit lue par le lecteur légitime, ce qui pourrait entraîner des actes d'escroquerie dans un contexte commercial ou la confusion des informations relatives à la chaîne logistique. Le clonage et l'émulation des puces pourraient être utilisés pour falsifier l'identité des marchandises et, par exemple, la remplacer par des identifiants d'articles moins coûteux. Les voleurs d'automobiles pourraient cloner les clés des véhicules. Le clonage de pièces d'identité pourrait en outre permettre d'usurper l'identité d'autres personnes afin de pouvoir pénétrer dans des zones à accès limité sur le lieu de travail. Le clonage pourrait donner lieu à une usurpation d'identité si la pièce d'identité clonée peut être utilisée comme preuve de l'identité de son détenteur.

Les attaques fondées sur la tromperie peuvent faire appel aux techniques de clonage et d'émulation. En 2005, des chercheurs ont démontré qu'il était possible de cloner le dispositif « Digital Signature Transponder », qui protège plus de 6 millions de systèmes de paiement ExxonMobil SpeedPass et plus de 150 millions de clés de contact pour automobiles. Ils ont cloné la puce en utilisant un matériel relativement bon marché, ont acheté de l'essence dans une station ExxonMobil à plusieurs reprises, et ont neutralisé le système anti-vol d'une voiture Ford. Un spécialiste des questions de sécurité a réussi à cloner la carte à puce sans contact Mifare de Philips Electronics, qui est le système de clé d'accès le plus répandu. Quant à la puce RFID « Verichip », qui est implantable sur les personnes, elle a été clonée en moins de dix minutes par un ingénieur canadien de 23 ans, pour les besoins d'un article dans le magazine *Wired*. La puce, qui avait été implantée sur le bras du journaliste, ne comportait pas de dispositif intégré de sécurité[44].

Une puce en lecture-écriture peut faire l'objet d'une modification abusive de ses données ou d'une falsification de son contenu dans le but de la rendre indisponible ou de changer l'identité ou les détails se rapportant à la marchandise ou à la personne concernée. Selon l'article de *Wired* précité, 5 millions de puces RFID ont été vendues à des bibliothèques sans être verrouillées afin de « permettre aux administrateurs des bibliothèques de modifier les données ». Malheureusement, n'importe quelle personne dotée du matériel et du logiciel appropriés peut aussi écrire dessus.

- Confidentialité

La confidentialité est l'assurance que les informations ne sont accessibles que par ceux qui y sont autorisés. Lorsque les données concernent une personne, la perte de confidentialité entraîne des atteintes à la protection de ces données. Sur les systèmes RFID classiques, les conséquences d'une perte de

44. Voir l'annexe III.

confidentialité peuvent être par exemple l'espionnage d'un concurrent dans le cadre de la chaîne logistique ou du commerce de détail, ou le vol d'un véhicule après avoir accédé aux informations de la clé électronique et cloné la puce. Selon un journal japonais, les informations qui sont stockées sur une carte des transports publics japonais (carte « Suica ») concernant les dernières gares de départ et d'arrivée empruntées par les usagers peuvent être lues par des lecteurs RFID de base, comme celui intégré au PDA Sony Clié. Un journaliste a affirmé que le fait de pouvoir lire ces informations à distance risquait de faciliter les pratiques de harcèlement de type *stalking*. La vulnérabilité des informations figurant sur les passeports (notamment les données biométriques) a été pointée du doigt comme étant un facteur possible d'escroquerie ou d'infraction avec usurpation d'identité (voir l'annexe III). Le fait d'accéder à distance et sans autorisation à des données est parfois appelé « écrémage » (*skimming*).

Tout système s'appuyant sur la technologie radio peut faire l'objet d'une interception du signal entre l'émetteur et le récepteur, ce qui peut poser des problèmes de confidentialité (ainsi que d'intégrité dans le cas où les données peuvent être réinjectées). Les systèmes RFID fonctionnant par induction magnétique génèrent eux aussi des ondes radio qu'un pirate équipé du matériel radio adéquat peut théoriquement intercepter. Mais dans la pratique, cela est très peu probable car les niveaux d'énergie seraient relativement faibles et recouverts par du bruit, ce qui obligerait le pirate à opérer à proximité des puces et du lecteur (certainement au vu de tous).

L'interception des données de RFID peut être soit active, soit passive. Le pirate (ou « l'intercepteur ») peut envoyer activement un signal à la puce en vue d'obtenir une réponse, ou simplement écouter passivement la réponse déclenchée par un lecteur activant la puce. Certaines puces ne peuvent répondre qu'avec des données (un numéro d'identification, par exemple). Les puces plus « intelligentes » peuvent quant à elles envoyer une réponse élaborée, comme si elles avaient été interrogées dans le but d'exploiter un point faible.

L'interception des données au moment de la transmission peut mettre au jour une communication entre des dispositifs RFID, et entraîner la divulgation d'informations très utiles pour le pirate (par exemple, le nombre de marchandises arrivant à l'entrepôt ou la présence d'un individu dans une zone donnée). Elle permet de suivre la puce et l'objet marqué ou étiqueté. Elle peut aussi renseigner sur le contenu des communications, et donc faciliter l'accès non autorisé à des informations professionnelles, personnelles et sur les concurrents qui peuvent être très intéressantes ; elle peut aussi donner lieu à des attaques telles que la modification abusive des données ou une « attaque de l'homme du milieu » (où l'intercepteur modifie les données échangées entre la puce et le lecteur). D'autres conséquences sur la vie privée de la perte de confidentialité sont détaillées plus avant dans la section consacrée à la protection de la vie privée.

- Considérations sur le type de technologie utilisé

Les risques varient selon le type de technologie utilisé pour exécuter une fonction particulière. Comme cela a été souligné précédemment, la RFID est un concept général qui englobe toute une variété de technologies présentant des caractéristiques différentes. Les risques mentionnés ci-dessus sont théoriquement valables pour tous les systèmes RFID. Toutefois, si l'on considère un éventail de risques, certains ont plus de chances d'apparaître sur certaines configurations techniques que sur d'autres. Des paramètres comme l'utilisation de puces actives ou passives, la communication par ondes radio ou par induction électromagnétique, ou encore l'existence d'une mémoire en lecture seule ou en lecture-écriture, ont une influence sur le degré de probabilité de certains risques. Si le tableau ci-après présente certains de ces éléments de manière très générale, il est important de noter que seul un examen détaillé de toutes les caractéristiques d'un système peut conduire à des conclusions pertinentes sur les risques potentiels des différents systèmes. Globalement, le tableau montre que les choix technologiques qui ne tiennent pas compte de la sécurité ont une incidence sur le degré de risque encouru.

Tableau 7. Comparaison des risques sur une échelle de risques

Risque	Échelle des risques Moins de risques ⟷ Plus de risques	Explication
Interception des données	Induction ⟷ Ondes radio	Le pirate doit se trouver dans les limites du rayon de fonctionnement[45].
Brouillage	Induction ⟷ Ondes radio	Idem
Suivi non déclaré	Induction ⟷ Ondes radio	Idem
Interférences radio	Induction ⟷ Ondes radio	L'induction électromagnétique n'est pas perturbée par les interférences radio.
Clonage de la puce	Authentification sur la puce ⟷ Données uniquement sur la puce	L'authentification empêche les accès non autorisés.
Altération de l'intégrité des données de la puce	Mémoire en lecture seule ⟷ Mémoire en lecture-écriture	La mémoire en lecture seule ne peut pas être modifiée (mais la puce peut être détruite).
Interruption de service par blocage de la puce	Puces actives ⟷ Puces passives	Les puces actives comprennent parfois des protocoles de communication intelligents pour empêcher les attaques.

La distance de fonctionnement – qui est explicitée dans la première section – peut être examinée sous l'angle du type d'attaque susceptible de survenir, comme le montre l'Encadré 1 ci-dessous.

45. Comme nous l'avons vu dans la première section du présent document, la loi de propagation des ondes radio est différente de celle applicable pour les champs électromagnétiques. La distance de fonctionnement des puces activées par ondes radio (bandes UHF et micro-ondes) peut être beaucoup plus importante (plusieurs mètres) que celle des systèmes à induction électromagnétique (quelques centimètres).

Encadré 1. La distance de fonctionnement du point de vue de la sécurité

Selon le document « Guidelines for Securing Radio Frequency Identification Systems » (2007) du NIST, on peut distinguer six distances de fonctionnement :

- **Distance de fonctionnement nominale** : distance, souvent établie par la norme, à laquelle les transactions autorisées sont possibles. Il s'agit de la distance de fonctionnement « officielle ».
- **Distance d'interception sur la voie de retour** : distance à laquelle un récepteur malveillant peut interpréter en toute fiabilité la réponse envoyée par une puce à un lecteur légitime.
- **Distance d'interception sur la voie aller** : distance à laquelle un récepteur malveillant peut écouter en toute fiabilité les transmissions d'un lecteur autorisé. Qu'il s'agisse de la voie aller ou de la voie de retour, la distance d'interception peut être beaucoup plus grande que la distance de fonctionnement officielle. La technique de masquage des codes, qui a été incluse dans la norme « Class 1 Generation 2 » d'EPCglobal, empêche un récepteur malveillant de décrypter les données échangées s'il n'est pas capable d'intercepter les réponses de la puce (la communication est cryptée à l'aide d'une clé envoyée par la puce au lecteur). Cela oblige le pirate à opérer à l'intérieur de la distance d'interception sur la voie de retour s'il veut décrypter la communication.
- **Distance de piratage ou de balayage malveillant :** distance à laquelle un lecteur malveillant opérant au-delà des limites de puissance autorisées peut communiquer en toute fiabilité avec une puce.
- **Distance d'exécution d'une commande malveillante** : distance à laquelle un lecteur malveillant peut exécuter la commande d'une puce qui ne requiert pas que le lecteur ait bien reçu l'information de la puce.
- **Distance d'analyse du trafic sur la voie aller** : distance à laquelle un récepteur malveillant peut détecter la présence du signal d'un lecteur sans avoir à interpréter son contenu. L'analyse du trafic peut permettre l'arrivée d'une livraison et éventuellement la comptabilisation du nombre d'articles. Une telle attaque peut être effectuée à des distances bien supérieures à l'interception de données.

Source : Adapté de NIST (2007), pp. 2-13.

2.1.1.2. Risques associés à d'autres composants

D'autres composants des systèmes RFID présentent également des risques en matière de sécurité. La sécurité des bases de données a notamment été identifiée comme une question importante et parfois sous-estimée, car ces bases de données contenant des informations associées à des puces peuvent être partagées par plusieurs entreprises, et parfois gérées par des tierces parties[46].

Par ailleurs, les systèmes RFID qui utilisent Internet pour transmettre les informations sont exposés au même type d'attaques que n'importe quel autre système d'information. Des chercheurs universitaires[47] ont par exemple signalé les éventuels problèmes de confidentialité/protection de la vie privée, de disponibilité et d'intégrité que risque de poser l'ONS (Object Naming Service) conçu par EPCglobal pour son architecture réseau (voir plus haut). EPCglobal considère que les risques en matière de sécurité doivent certes être étudiés, mais qu'ils sont limités et pas plus importants que ceux que présentent aujourd'hui les communications via Internet ou d'autres systèmes d'information.

Les recherches universitaires ont également démontré que les attaques classiques par injection de codes SQL (Structured Query Language) et de texte peuvent gravement endommager un système RFID au moyen d'une seule puce infectée[48]. Les données contenues dans les puces RFID pourraient inclure des instructions ou des codes inattendus dont le but est, par exemple, d'endommager la base de données située en arrière-plan du système RFID, de mettre en péril tout le dispositif, et/ou de s'auto-reproduire au sein du système. Dans de tels scénarios, les attaques ne sont pas fondamentalement liées à la technologie RFID mais à la qualité de la conception et du codage des logiciels *middleware* qui interagissent avec les

46. FTC des États-Unis (2005), p. 16.

47. Fabian (2005).

48. Rieback *et al.* (sans date).

dispositifs RFID. Les chercheurs ont souligné que les applications RFID étaient susceptibles d'être exploitées par des logiciels malveillants (*malware*): elles sont complexes et utilisent une grande quantité de code source, elles font appel à des protocoles, des utilitaires et des bases de données d'arrière-plan standard, elles traitent et stockent des données de grande valeur et, comme personne ne s'attend encore à ce qu'il existe des moyens de pirater la RFID, elles véhiculent une fausse notion de sécurité[49].

2.1.1.3. « S'attendre à l'inattendu »

La technologie des puces est encore relativement jeune. Par conséquent, des techniques d'attaque inédites et imprévues pourraient apparaître. Comme l'indiquent les auteurs du livre « RFID. Applications, Security and Privacy », il faut « s'attendre à l'inattendu. Si une chose est sûre concernant ce nouvel univers de la RFID, c'est qu'il y a à la fois de grands changements en perspective, et de grosses surprises en réserve[50] ». À titre d'exemple, en février 2006, le professeur et célèbre cryptographe Adi Shamir « a utilisé une antenne directionnelle et un oscilloscope numérique pour examiner l'énergie utilisée par les puces RFID pendant leur lecture. Les types d'utilisation de l'énergie ont pu être analysés pour déterminer à quel moment la puce recevait des bits de mots de passe corrects et incorrects ». M. Shamir a indiqué qu'un « téléphone portable possède tous les ingrédients nécessaires pour mener une attaque et compromettre toutes les puces RFID situées à proximité »[51].

La démonstration de la faisabilité d'une telle attaque dans des conditions de laboratoire doit être mise en balance avec les coûts de mise en œuvre de ce scénario dans des conditions réelles et avec les avantages ou les inconvénients de ce type d'attaque. Cet exemple montre toutefois qu'il serait souhaitable de tenir compte de l'évolution de la technologie lorsque l'on définit une stratégie en matière de sécurité, d'évaluer les risques au moment de la conception du système, et de les réévaluer régulièrement comme dans n'importe quel processus de gestion de la sécurité.

2.1.2. Mesures de sécurité[52]

La sécurité est mise en œuvre au moyen d'un ensemble de mesures – de gestion, opérationnelles et techniques – qui ont pour but de limiter les risques. Les systèmes RFID varient considérablement selon la technologie utilisée, les contextes d'application et les scénarios. Pour être efficaces, les stratégies relatives à la sécurité doivent reposer sur une série de mesures qui assurent l'équilibre entre le coût, les performances et la commodité d'un système donné dans un cadre réglementaire particulier. L'évaluation des risques est une condition indispensable pour déterminer le niveau de la menace et le degré de vulnérabilité à un moment précis, et pour voir quelles sont les mesures appropriées pour les atténuer. La RFID n'est à cet égard pas différente des autres systèmes d'information.

Les *mesures de gestion* sont les orientations politiques, les procédures et les normes relatives au concept d'ensemble du système. Elles définissent en détail le mode de gestion d'une entreprise et les modalités d'exécution des activités quotidiennes. Les mesures de gestion comprennent notamment : les

49. Pour en savoir plus sur les logiciels malveillants, voir « Analytical Report on Malicious Software », OCDE (2007a).

50. Garfinkel (2006), p. xliv.

51. Oren (sans date), Merrit (2006). Les spécialistes de la sécurité ont remarqué que ces attaques « latérales » n'étaient pas d'un genre nouveau et que la RFID pourrait bénéficier des techniques d'atténuation qui ont été utilisées pour protéger les cartes à puce avec contact, par exemple en masquant les pics dans la consommation d'énergie. Voir O'Connor (2006).

52. Le présent document n'a pas pour objet de fournir un inventaire exhaustif des mesures qui sont en vigueur pour contrôler les risques. Pour un inventaire plus complet, se reporter à NIST (2007) et BSI (2005).

politiques de sécurité informatique, dont certaines dispositions concernent le contrôle d'accès aux informations de la RFID, la protection du périmètre d'utilisation et la gestion des mots de passe ; la politique d'utilisation de la RFID, qui définit les usages autorisés et non autorisés des technologies RFID ; les accords avec d'autres sociétés lorsque les données associées aux systèmes RFID sont mises en commun entre plusieurs entités ; les stratégies visant à limiter la quantité d'informations stockées sur les puces (lorsqu'il s'agit de données personnelles, par exemple).

Les *mesures opérationnelles* correspondent aux actions effectuées par les utilisateurs du système. Il s'agit notamment du contrôle d'accès physique (caméras de surveillance, portes, murs, etc.), du choix de l'emplacement adéquat pour les puces et les lecteurs (par exemple pour limiter les interférences), de la formation du personnel et de l'utilisation d'identifiants dont le format empêche la divulgation des informations.

Les *mesures techniques* sont les dispositions prises au niveau technologique pour contrôler et retreindre l'accès aux informations et au système. Cela comprend :

- Les mesures visant à protéger les données de la puce : dispositif désactivant toutes les fonctionnalités de la puce lorsqu'elle reçoit une instruction d'interruption ; cryptographie[53] ; mécanismes de contrôle d'accès, comme par exemple la protection à l'aide d'un mot de passe pour empêcher tout individu d'utiliser la commande d'interruption (« kill ») contre une puce « Class 1 Generation 2 » d'EPC ; mécanismes d'authentification en vertu desquels la puce authentifie le lecteur et/ou inversement ; dispositifs anti-fraude pour empêcher que la puce ne soit arrachée de l'objet auquel elle est attachée.
- Les mesures visant à protéger l'interface radio : utilisation d'une fréquence qui évite certaines interférences (dans les liquides, par exemple) ; réglage du niveau de puissance afin de limiter la propagation des ondes radio et les risques d'interception ; blindage de la puce lorsqu'elle n'est pas sensée être en service, afin d'empêcher tout accès non autorisé, ou blindage de l'environnement pour éviter toute interception ; enfin, désactivation temporaire des puces actives[54].

De nombreuses mesures techniques sont disponibles à des degrés divers de sophistication et de robustesse. Or, la sophistication entraîne souvent une plus grande complexité. Pour citer un exemple, une cryptographie robuste implique fréquemment des processus et des techniques de gestion des clés qui ne sont pas vraiment compatibles avec des solutions simples clé en main. Par ailleurs, les puces dotées d'une plus grande puissance de traitement – un aspect indispensable pour la sécurité – risquent de nécessiter plus d'énergie, ce qui est source de nouveaux inconvénients : distance de lecture plus petite, format plus grand, besoin de piles, durée de vie plus courte, etc. À long terme, il est possible que certains de ces inconvénients puissent être atténués. Le coût des dispositifs RFID pourrait en outre être proportionnel à leur degré de sophistication, ainsi qu'à la robustesse de leur fonction de sécurité. Ce sont en fin de compte les forces du marché qui pousseront ce coût à la baisse.

53. La cryptographie s'accompagne d'un certain nombre de techniques de gestion des clés, comme par exemple la diversification des clés pour limiter les dégâts provoqués par une attaque.

54. Une autre mesure technique est le masquage des codes, qui s'appuie sur le fait que le niveau de puissance du signal émis par une puce passive est inférieur à celui d'un lecteur : un mot de passe est alors envoyé par la puce, et le lecteur l'utilise pour crypter la communication. Un pirate éventuel situé au-delà de la distance de fonctionnement de la puce mais dans celui du lecteur pourrait peut-être intercepter les données cryptées, mais pas s'emparer de la clé de chiffrement. Cette technique est incluse dans la norme « Class 1 Generation 2 » d'EPC.

D'importants travaux de recherche sont en cours pour mettre au point des mesures techniques de sécurité novatrices[55] dans des domaines comme l'authentification, la cryptographie, le blocage et les dispositifs incorporant des politiques de fonctionnement (« l'informatique de confiance »)[56]. Les techniques de minimisation des données sont également à l'étude : l'identifiant unique (par exemple, le code EPC, voir l'annexe IV) pourrait ainsi être effacé, soit automatiquement, soit par l'opérateur, ce qui signifie que seules les données correspondant à la catégorie du produit resteraient accessibles, à l'instar des codes-barres que l'on connaît aujourd'hui. La puce ne servirait donc plus à identifier de façon unique un objet particulier, mais désignerait seulement une catégorie d'objet. Une autre technique consiste à ajouter à la puce une fonction de mesure de la distance et à adapter le degré de détail de l'information transmise en fonction de la distance à laquelle le lecteur a été détecté. Prenons le cas d'une puce attachée à une bouteille d'eau : si le lecteur est situé loin d'elle, il est possible qu'elle lui réponde, mais il ne lui communiquera que la marque du produit ; il ne lui transmettra en plus son numéro d'identification que si le lecteur est très près de la puce. Aucun de ces travaux ne propose une solution miracle, mais ils sont utiles et confirment qu'il existe pour l'avenir de très nombreuses possibilités d'intégrer la sécurité au cœur même de la technologie.

Il n'existe pas de mesure de sécurité universelle qui offre une parade efficace à un type de risques particulier et dans toutes les situations. Le fait qu'une mesure de sécurité soit appropriée dépend de plusieurs facteurs : les mesures de sécurité ne sont pas toutes possibles pour tous les types de systèmes RFID. Ainsi, le cryptage des données permet certes de protéger les données sensibles des puces, mais comme l'indiquent les lignes directrices du NIST[57], il n'est pas disponible sur les systèmes répondant aux normes EPC et ISO 18000. Ensuite, toutes les mesures de sécurité présentent des avantages et des inconvénients : la protection à l'aide d'un mot de passe permet de limiter l'accès aux informations des puces, mais la longueur du mot de passe est souvent très réduite[58] ; le cryptage des données sur les puces requiert de l'énergie pour les fonctions cryptographiques, et il risque d'entraîner des délais inacceptables sur les systèmes qui ont besoin que les opérations de lecture/d'écriture entre le lecteur et la puce s'effectuent rapidement.

On constate qu'il n'existe quasiment pas de normes publiques concernant la classification et l'évaluation des fonctions de sécurité des cartes et des puces RFID. D'où la difficulté qu'ont peut-être les opérateurs, voire les fabricants, de systèmes RFID à évaluer la sécurité de ces dispositifs.

Les mesures techniques ne peuvent éliminer tous les risques. Des mesures opérationnelles et de gestion sont également nécessaires. À titre d'exemple, les outils de sécurité (tels que le cryptage) ne sont utiles que s'ils s'inscrivent dans un ensemble plus complet de dispositions contribuant à la mise en œuvre d'une politique globale en matière de sécurité.

---

55. Par exemple, la Commission européenne (2007a, p. 10) « encouragera la recherche sur la sécurité des systèmes RFID, notamment sur les protocoles de sécurité légers et les mécanismes perfectionnés de distribution de clé, afin de prévenir les attaques visant directement la puce, le lecteur et la communication puce-lecteur ».

56. Pour une présentation détaillée, voir Juels (2005a). Voir aussi le site Internet de Gildas Avoine sur le thème « RFID, Security and Privacy », qui répertorie des centaines d'articles sur les travaux consacrés aux questions de sécurité et de protection de la vie privée relatives à la RFID. Voir encore le rapport « Security Analysis Report » (2007) de BRIDGE, qui s'intéresse aux exigences de sécurité pour les systèmes en boucle ouverte.

57. NIST (2007), pp. 5-17.

58. Les puces répondant à la norme « Class 1 Generation 1 » d'EPC proposent un mot de passe de 8 bits, ce qui limite les possibilités à 256 mots de passe ; les puces « Class 1 Generation 2 » offrent quant à elles des mots de passe de 32 bits, ce qui équivaut à 4 294 967 296 possibilités.

Le Tableau 8 ci-dessous présente succinctement les mesures de sécurité des systèmes RFID mises au point par le *National Institute for Standards and Technology* des États-Unis.

Tableau 8. Aperçu des mesures de sécurité des systèmes RFID

Mesures de sécurité	Risques pour le processus de gestion	Risques pour les informations confidentielles de l'entreprise	Risques pour la vie privée	Attaques du réseau informatique
Mesures de gestion				
Politique concernant l'utilisation de la RFID	■	■	■	■
Politiques en matière de sécurité informatique	■	■		
Accords avec des entités extérieures	■	■	■	
Minimisation des données stockées sur les puces	■	■	■	
Mesures opérationnelles				
Contrôle d'accès physique	■	■		■
Positionnement approprié des puces et des lecteurs	■	■		■
Destruction sécurisée des puces	■	■	■	
Formation de l'opérateur et de l'administrateur	■	■		■
Séparation des tâches	■	■		
Formats d'identifiants non parlants		■	■	
Mesures techniques				
Contrôle d'accès au puces	■	■	■	
Fonction d'interruption			■	
Cryptage des données	■	■	■	
Système d'identification alternatif	■			
Authentification	■	■	■	
Dispositif anti-fraude	■	■		
Sélection des fréquences radio	■			■
Ajustement de la puissance de transmission		■		■
Blindage électromagnétique		■	■	■
Masquage des codes				
Désactivation temporaire des puces actives		■	■	

Note : dans les lignes directrices du NIST, les attaques du réseau informatique figurent dans la catégorie « Risques pour les ressources externes », qui inclut également les dangers dus au rayonnement électromagnétique.

Source : NIST (2007).

2.1.3 Approche holistique

Les mesures de sécurité peuvent être appliquées à n'importe quel stade du déploiement d'un système RFID. En particulier, de nombreuses mesures techniques seront probablement plus efficaces si elles sont introduites au stade le plus précoce de l'élaboration du système. Les dispositions qui étaient en place avant le déploiement de la puce peuvent globalement être considérées comme des mesures de prévention et d'anticipation, tandis que celles prises au niveau de l'environnement et du reste du système (y compris les lecteurs) peuvent être décrites dans l'ensemble comme des mécanismes de réaction et de limitation des

risques. Si l'on veut avoir une prise sur le caractère fondamentalement ouvert de la RFID, il est nécessaire d'adopter une vision holistique du système, du point de vue tant du temps que de l'espace, lorsqu'on évalue et gère les risques : *i*) évaluer les risques en matière de sécurité à tous les stades de mise en œuvre du système, y compris la planification, le déploiement, la mise en service, le traitement des données et la destruction (fin de vie)[59] ; *ii*) considérer le système RFID au sens large, en tenant compte à la fois des composants spécifiques à cette technologie et des autres, en évitant de se concentrer uniquement sur la relation puce-lecteur, et en abordant le système comme un élément faisant partie d'une vaste infrastructure composée de systèmes d'information et de réseaux. Une approche trop restreinte, axée uniquement sur le lien opérationnel entre la puce et le lecteur ne permettrait pas de saisir toutes les mesures qui pourraient être mises en place avant et après ce point pour prévenir et limiter les dommages. Ce type d'approche aurait également pour inconvénient de ne pas détecter les risques potentiels pour le réseau, les composants *middleware* et les composants situés en arrière-plan qui sont essentiels à l'efficacité d'un système RFID. Elle pourrait aussi conduire à une sous-évaluation du coût et à une surestimation de l'efficacité des mesures de sécurité susceptibles d'être mises en place.

Les technologies utilisées dans les systèmes RFID et les parties prenantes sont complexes et variées. Il est par conséquent impossible d'adopter un modèle de sécurité fermé et rigide. Les nombreuses interconnexions et interdépendances, ajoutées aux liens complexes qui existent entre les différents composants technologiques, entités et processus de gestion font qu'il n'est pas aisé d'établir un périmètre de sécurité physique et logique pour un système RFID. De plus, un grand nombre des variables intervenant dans le domaine de la sécurité échappent au contrôle de certaines des parties prenantes. On pourrait donc dire que la sécurité passe par l'adoption d'une approche holistique intégrant chacun des composants pour obtenir une vision globale de la sécurité, en acceptant qu'il puisse y avoir des lacunes au niveau de certains d'entre eux mais qu'elles seront compensées à d'autres niveaux.

Dans certains cas, des mesures de contrôle sont déjà en vigueur – sous la forme d'orientations politiques et de réglementations – et l'introduction de la RFID n'aura aucune incidence sur les modèles de sécurité existants. Dans d'autres, le déploiement de cette technologie risque de nécessiter de nouvelles évaluations des risques qui pourraient mener à la conclusion que les dispositions existantes, notamment la politique et la réglementation en matière de sécurité, doivent être renforcées.

2.1.4 Ajustement du niveau de sécurité en fonction des enjeux

Les mesures mises en place dans le cadre de la gestion de la sécurité de l'information doivent assurer un équilibre entre les risques, les coûts et l'efficacité. Le rapport coûts/bénéfices des mesures de sécurité ne peut être exprimé en termes absolus. La raison à cela est qu'il dépend du contexte d'application, et en particulier de la valeur des ressources ou des processus de gestion qui doivent être protégés. Une puce RFID peut être assimilée à un jeton contenant des informations. L'importance de sa sécurité est déterminée par la ressource à laquelle il est attaché (par exemple, la clé d'une voiture), et par la finalité de son utilisation (vérifier l'identité, autoriser l'accès à des zones protégées, payer des achats, etc.). Lorsque les puces RFID sont utilisées comme portefeuille électronique, carte de métro ou badge pour ouvrir des portes, elles peuvent susciter l'intérêt de malfaiteurs qui chercheront à les voler, les copier ou les modifier. Lorsque la RFID sert à contrôler l'accès à d'autres systèmes et réseaux, une attaque réussie pourrait mettre en péril non seulement le système RFID lui-même, mais aussi tous les systèmes et réseaux qu'il était sensé protéger.

59. Bien que la « fin de vie » ou la destruction d'un système soit souvent associée à l'élimination des informations, par exemple lorsque l'on n'en a plus besoin, elle peut aussi donner lieu à des activités telles que l'archivage des données ou leur transfert vers un autre système.

Le risque augmente lorsque les bénéfices d'une attaque sont supérieurs à ses coûts. Avant de commettre une infraction, les malfaiteurs eux-mêmes procèdent à une évaluation des risques sur les systèmes existants, afin de déterminer s'ils peuvent exploiter leurs lacunes et de quelle façon. Ils analysent également le rapport coûts/bénéfices pour voir quelle est la stratégie d'attaque la mieux adaptée pour atteindre l'objectif visé. Les malfaiteurs décideront par exemple qu'il est plus facile de cloner le badge RFID d'un hôtel que de soudoyer les domestiques ou d'entrer par effraction dans l'établissement. Des mesures de sécurité bien conçues peuvent renchérir les coûts d'une éventuelle attaque, de sorte qu'ils deviennent supérieurs aux bénéfices. En revanche, des mesures de sécurité insuffisantes par rapport à la valeur de la ressource à protéger risquent d'attiser les convoitises d'un éventuel pirate. La mise en place d'une série de mesures efficaces ne dissuadera sans doute pas un malfaiteur de commettre son méfait, mais cela pourra l'obliger à employer une autre technique, à cibler d'autres systèmes ou victimes moins protégés, ou à prendre plus de risques.

Lorsque les informations stockées sur une puce concernent des personnes identifiées ou identifiables, leur protection doit être abordée sous deux angles : celui de la sécurité et celui de la vie privée. Il arrive que les données stockées aient un caractère sensible : les informations identifiant un médicament que prend ou a sur lui un individu peuvent révéler l'état de santé de la personne ; la perte ou la détérioration du dossier médical enregistré sur le bracelet RFID d'un patient peut entraîner des situations dangereuses pour la vie de la personne ; l'accès non autorisé aux données biométriques figurant sur un passeport ou un document d'identité peut donner lieu à une usurpation d'identité. Certaines informations personnelles sensibles, telles que les données biométriques, requièrent des protections plus élaborées que d'autres, comme par exemple l'utilisation de mécanismes efficaces de cryptage et d'authentification électronique. Bien que l'évaluation des risques en matière de sécurité puisse être jugée similaire à l'estimation des incidences pour la vie privée sur le plan de la méthodologie, son ampleur n'est pas la même. Une entreprise procède en effet à une évaluation des risques pour protéger ses ressources et ses processus de gestion. Lorsqu'elle évalue les répercussions sur la vie privée, elle doit prendre en compte tous les cas d'atteinte à la vie privée que risquent de rencontrer les personnes concernées par le traitement des données, y compris lorsque cette atteinte n'a pas d'incidence directe sur l'entreprise. L'utilisation de la RFID pour vérifier l'identité des personnes est un bon exemple de cas où une étude approfondie de la sécurité et des implications sur la vie privée est nécessaire avant de prendre la décision d'adopter ladite technologie (Department of Homeland Security, 2006).

Il est possible que, dans un scénario donné, on parvienne à la conclusion que, compte tenu du niveau de risque et du coût des mesures de sécurité qui sont nécessaires pour y faire face, ainsi que des avantages procurés par l'utilisation de la RFID, il ne soit pas utile de déployer un tel système, ou qu'il faille revoir partiellement ou complètement le projet. Dans certains cas, une technologie RFID bon marché pourra sembler insuffisamment protégée contre une certaine catégorie de risques, mais suffisamment par rapport à d'autres. La décision pourrait être prise d'investir dans un type de RFID plus sûre, d'associer une RFID peu onéreuse au départ avec des mesures de sécurité ne faisant pas appel à cette technologie (par exemple, des caméras vidéo, une surveillance humaine, etc.), ou encore d'utiliser d'autres types de technologies.

2.2. Protection de la vie privée

La protection de la vie privée est la préoccupation numéro un telle qu'exprimée au travers d'études auprès des consommateurs[60] ainsi que dans les commentaires reçus par les organismes de protection des consommateurs tels que la *Federal Trade Commission* aux États-Unis[61]. Plusieurs campagnes de sensibilisation retentissantes menées par des groupes anti-« spychips »[62] (ou puces espionnes) ont conduit des sociétés à stopper leur expérimentation de la RFID et ont fait comprendre aux entreprises qu'il fallait répondre aux attentes du public en matière de protection de la vie privée pour que cette technologie puisse être adoptée à grande échelle. Comme le constate un observateur[63], la RFID est née dans un environnement technique, elle est conçue, utilisée et comprise principalement par des techniciens. Créée à l'origine pour la chaîne logistique, elle s'étend aujourd'hui au grand public mais elle peut être invisible, demeure obscure et est souvent incomprise. Les problèmes d'image qui lui sont associés ne peuvent pas simplement être ignorés sous prétexte que ce sont des craintes irrationnelles. Ces questions doivent être examinées de manière responsable par l'ensemble des parties prenantes afin de ne pas menacer les bienfaits potentiels de cette technologie, à la fois pour l'industrie et pour les individus.

En réalité, les études montrent aussi que les consommateurs ont encore une connaissance assez limitée de la RFID. Si certains considèrent que les problèmes d'atteinte à la vie privée menacent de jeter une ombre sur les points positifs de la RFID[64], d'autres se demandent si les avantages apparents de cette technologie dans certains domaines dépassent réellement les risques éventuels, notamment lorsque l'on sait que certains de ces risques ne seront pas immédiatement perceptibles. De manière plus générale, le *National Research Council* américain (2004, p. 28) a reconnu que « compte tenu des grandes différences existant entre les individus sur la question de la vie privée, ainsi que des nombreuses normes sociales, l'instauration d'une confiance publique à l'égard de la technologie RFID sera une tâche ardue et de longue haleine […] ».

Plusieurs auteurs et organisations du secteur public et du secteur privé ont déjà réalisé des études consacrées aux incidences de la RFID sur la vie privée ; ils ont rédigé des rapports, voire formulé des conseils ou des principes, pour aider les parties prenantes à appliquer les cadres existants en matière de protection de la vie privée. Une liste de références est fournie à l'annexe V. Ces documents sont une base très utile sur laquelle s'appuient en partie les observations qui suivent. Les sections suivantes passent en revue les problèmes de protection de la vie privée que risque de poser la RFID, ainsi que les garanties possibles. Les *Lignes directrices de l'OCDE sur la protection de la vie privée* ont servi de fil conducteur dans la présentation des problèmes de protection de la vie privée.

2.2.1 Présentation des problèmes de protection de la vie privée

Les configurations matérielles et logicielles de la RFID sont très variées et peuvent être déployées dans des contextes très différents. Cette technologie n'entraîne pas systématiquement, ni forcément, des

60. Selon Cap Gemini (2005a), les questions relatives à la vie privée sont, en ce qui concerne la RFID, celles qui préoccupent le plus les consommateurs européens. Aux États-Unis, cette préoccupation est encore plus prononcée, sans doute en raison de la plus grande visibilité des activités anti-RFID qui sont menées dans ce pays par les associations de défense des consommateurs.

61. FTC (2005), p. 12.

62. Voir le livre « Spychips » de Katherine Albrecht et Liz McIntyre (2006), ainsi que le site Internet www.spychips.com.

63. Pradelles (directeur en charge du respect de la vie privée des clients chez Hewlett Packard), 2006.

64. Cap Gemini (2005b).

problèmes de protection de la vie privée, et lorsque c'est le cas, la nature, l'importance et l'ampleur de ces problèmes varient à la fois en fonction de la technologie utilisée et du contexte[65].

Dans la plupart des cas, l'éventuelle ingérence de la RFID dans la vie privée a tendance à être proportionnelle à plusieurs paramètres interdépendants, dont les suivants : *i)* la capacité pour une puce d'être lue à distance sans la participation de la personne ; *ii)* la possibilité d'obtenir des informations personnelles ou sensibles sur des individus par déduction et profilage ; *iii)* le degré d'interopérabilité (qui peut lire les puces ? Qui peut accéder à toutes les informations relatives au produit ?) ; *iv)* les capacités de suivi de la RFID.

2.2.1.1 Invisibilité de la collecte des données

Une caractéristique importante de la RFID est que la collecte des données peut avoir lieu sans que la personne concernée ne s'en rende compte : la communication électromagnétique est invisible, elle n'est pas perceptible par les sens, elle pénètre les obstacles tels que les sacs ou les vêtements, les puces et les lecteurs RFID peuvent être de taille très réduite, et rien n'indique parfois qu'ils sont en marche. Cela entraîne à la fois des problèmes de sécurité (des attaques par brouillage, interception et lecture peuvent par exemple être commises à distance) et de protection de la vie privée[66]. L'invisibilité génère de l'incertitude et peut conduire les personnes à penser que « quelque chose se passe peut-être dans leur dos », créant une résistance générale à l'égard de cette technologie. Toutefois, ce qui, dans certains cas, peut conduire à un sentiment de peur peut aussi, dans d'autres, être un facteur d'incitation à utiliser cette technologie : la possibilité d'établir automatiquement la communication entre le lecteur et les puces, en traversant des obstacles et sans ligne de vue directe, est également le gros avantage de la RFID dans le contexte des chaînes logistiques, du contrôle d'accès et autres. Cela peut aussi apporter plus de commodité et de choix aux consommateurs lorsqu'ils font leurs courses.

2.2.1.2 Profilage

L'accès aux informations contenues sur les puces attachées aux objets que possèdent ou portent les individus pourraient révéler des aspects de leur vie, comme par exemple leur intérêt pour des thèmes particuliers (dans le cas de livres marqués avec des puces RFID), ou le fait qu'ils ont de l'argent sur eux (lorsque la RFID est insérée sur des billets de banque) ou portent des objets de valeur. La structure de données EPC n'est pas un numéro unique attribué par hasard ; elle comprend, outre le numéro de série de l'objet, des éléments qui identifient le fabricant du produit (« EPC manager number ») et le code produit (« object class »), à l'instar du système des codes-barres. Consultées par un tiers, ces données pourraient révéler des détails sur l'objet lui-même, et donc des informations sensibles, comme par exemple : « Cette personne a du Prozac sur elle. Elle est certainement dépressive ou en contact avec une personne dépressive »[67], etc. Or, avant d'en arriver à une telle inférence, la tierce partie devra lire le contenu de la puce et remplacer le code du produit par son nom. Peut-être connaîtra-t-elle le lien entre le code et le produit pour l'avoir préalablement recherché. Sinon, elle pourrait soumettre le code du fabricant (« EPC manager number ») à un Object Naming Service (ONS) afin d'obtenir l'adresse réseau de l'entreprise. Ensuite, pour se procurer le nom du produit, elle pourrait envoyer à cette adresse une requête comportant le

65. Selon Ann Cavoukian, commissaire à l'information et à la protection de la vie privée de l'Ontario (2006a), les principes appliqués à la RFID doivent « concerner les systèmes d'information RFID, pas les technologies ».

66. La collecte et la transmission de données personnelles à l'insu de l'individu concerné ne sont pas un sujet nouveau dans le domaine de la vie privée. Le problème a notamment été abordé dans le cadre de l'utilisation des technologies biométriques. Voir OCDE (2005).

67 Stapleton-Gray (sans date).

code du produit[68]. Enfin, elle pourrait peut-être procéder à l'inférence précitée. Il convient de noter ici qu'un tel scénario repose sur des hypothèses car le marquage des produits est une pratique encore peu développée.

La révélation du type de savon ou de dentifrice acheté au supermarché peut ne pas être considérée comme une véritable atteinte à la vie privée. Mais dans certains cas, les profils et les déductions auxquels on peut parvenir à partir d'un ensemble de puces RFID qu'un individu porte sur lui pourraient devenir très précis et révéler des informations beaucoup plus indiscrètes, notamment son identité. Des informations sensibles telles que la nationalité de la personne ou ses données biométriques pourraient aussi être divulguées par des passeports biométriques non protégés.

Effectuer des inférences à partir des données disponibles dans le but d'améliorer les profils existants n'est pas une pratique nouvelle. Les sociétés de crédit, les banques et les compagnies d'assurance utilisent depuis longtemps des techniques de profilage pour attribuer à leurs clients un niveau de risque. Des sites Internet très connus comme Amazon formulent des suggestions de livres et de DVD à des clients qui renouvellent leurs visites, en s'appuyant sur leurs habitudes d'achat et de navigation. Cela permet souvent aux consommateurs de disposer de plus d'avantages et d'options, et aux entreprises de proposer des services de meilleure qualité, et parfois mieux adaptés, à la demande du client. La RFID ne modifie pas fondamentalement les techniques de profilage, mais : *i)* l'invisibilité de cette technologie permettrait d'effectuer ce profilage à l'insu des personnes[69] et *ii)* si elle était plus répandue, elle pourrait rendre les techniques de profilage plus précises et plus efficaces en fournissant davantage de données.

2.2.1.4 Suivi

Le suivi (*tracking*) d'objets, de marchandises, de colis, de palettes et d'animaux est la principale fonctionnalité de la RFID. Le suivi des personnes est possible si celles-ci transportent ou ont sur elles des objets intégrant des puces RFID. Cette technologie est utilisée par exemple dans les parcs d'attractions pour permettre aux parents de retrouver leurs enfants. On la trouve également dans les stations de ski – où elle permet à des amis de se localiser mutuellement – dans les hôpitaux pour savoir où se trouvent les patients, et dans les prisons pour suivre les déplacements des détenus dans l'établissement.

Le suivi est rendu possible par la collecte ou le traitement des données relatives au lieu et à la date, et peut avoir lieu *a posteriori* une fois que les informations ont été saisies dans la base de données, ou en temps réel.

Le suivi *a posteriori* peut être consécutif au regroupement de diverses informations (lieu, heure et autres) qui ont été préalablement enregistrées dans une ou plusieurs bases de données, et qui sont en quelque sorte des « empreintes numériques ». Pour citer des exemples, les tickets RFID de cinéma ou de manifestations sportives peuvent enregistrer l'heure à laquelle est arrivé le titulaire du ticket, ainsi que le lieu. Les badges utilisés pour contrôler l'accès sur un lieu de travail permettent d'autoriser l'entrée dans certains locaux à certaines personnes seulement, et assurent souvent le suivi des salariés en ce qui concerne leur temps de présence et le nombre d'heures de travail. Les cartes RFID d'accès au métro telles que le passe Navigo à Paris, la carte Oyster à Londres ou la carte Suica à Tokyo offrent à leurs détenteurs la possibilité d'emprunter le réseau de transport et d'effectuer le trajet qu'ils ont payé. Tous ces systèmes

68. Il est probable que le système du fabricant demandera une authentification s'il est déployé dans une configuration interentreprises.

69. Un exemple hypothétique de déduction élémentaire effectuée à l'insu de la personne est souvent cité : il s'agit du cas de malfaiteurs qui accèdent aux informations figurant sur les objets portés par une personne, et qui les utilisent pour décider d'agresser cette personne (par exemple, la personne en question porte un vêtement de créateur ; elle a donc des chances d'avoir sur elle des objets de valeur).

RFID ont besoin, pour leur fonction de contrôle d'accès, de traiter les informations relatives au lieu, mais si ces dernières sont archivées sous le nom de la personne, elles risquent d'être utilisées à d'autres fins, de type traçage ou pistage.

Selon les cadres de protection de la vie privée, les données personnelles ne sauraient être divulguées, mises à disposition ou utilisées de quelque manière que ce soit à des fins autres que celles spécifiées à l'origine, si ce n'est avec l'accord de l'intéressé ou lorsque la loi le permet. Les traces numériques ne sont pas un concept nouveau dans le domaine des applications en ligne, et elles sont utilisées depuis longtemps dans le cadre des enquêtes criminelles. L'un des objectifs de la protection de la vie privée est d'empêcher la généralisation de leur utilisation. L'étude de leurs implications sur la vie privée peut aider à détecter les fonctionnalités du système qui pourraient entraîner une violation des principes de protection de la vie privée tels que la « limitation d'utilisation », et à déterminer quelles alternatives techniques ou fonctionnelles peuvent empêcher une utilisation détournée, comme par exemple les technologies respectueuses de la vie privée et les stratégies de minimisation des données et d'anonymisation.

Le suivi en temps réel consiste généralement à suivre les déplacements d'une personne bien précise, mais la RFID pourrait aussi être mise à profit pour suivre une personne non identifiée, par exemple en sélectionnant un individu au sein d'un groupe et en examinant son comportement, sans connaître son nom ou son identité. Cependant, des scénarios de ce type nécessiteraient tout d'abord que la personne soit équipée d'une puce fonctionnelle (ni désactivée, ni bloquée) pouvant être lu ultérieurement, et que le responsable du suivi déploie des lecteurs aux endroits appropriés, en tenant compte de la distance de fonctionnement de la technologie RFID utilisée et d'autres contraintes techniques. Le fait que la puce puisse être lue par l'entité qui l'avait remise à la personne, par plusieurs parties ou par tout individu doté du matériel adéquat, dépendrait de la nature des mesures de sécurité incorporées à la puce et du degré d'interopérabilité de cette dernière. La possibilité que ce suivi en temps réel ait lieu à l'insu de la personne concernée ou à des fins criminelles a été évoquée par les opposants à la RFID, mais peu de cas ont en fait été signalés pour le moment.

Les problèmes suscités par le fonctionnement d'une infrastructure ouverte qui pourrait être utilisée pour suivre des objets et des personnes ne rentrent pas dans le cadre de la présente étude, car ce type d'infrastructure n'est pas prévue à court terme. Par ailleurs, la généralisation hypothétique d'environnements équipés de capteurs ubiquitaires, où tous les objets comporteraient des puces pouvant être lues par n'importe qui et capables d'interagir avec l'environnement (faisant du bureau, de la maison ou des rues des espaces « intelligents »), pourrait également susciter des inquiétudes en ce qui concerne le suivi en temps réel et *a posteriori*. Cependant, comme il s'agit de suppositions sur le long terme, elles ne seront pas étudiées dans le présent document. Ces deux sujets pourraient être abordés dans le cadre plus général de l'infrastructures de surveillance.

2.2.1.3 Interopérabilité

Le contexte dans lequel ont lieu la collecte des informations RFID et leur association à des personnes a son importance. Dans un système à boucle fermée, où la puce est essentiellement lue et modifiée par l'entité qui l'a déployé initialement, il n'est pas facile de déterminer si l'utilisation de la RFID donnerait des résultats vraiment différents de ce qui se passe avec les systèmes ne faisant pas appel à cette technologie, comme les cartes avec contact ou les codes-barres. Ces codes permettent d'ores et déjà de recueillir des informations sur ce qu'achètent les consommateurs, en les associant à des noms ou d'autres données personnelles (cartes de crédit, chèques ou cartes de fidélité, par exemple). Ces informations enrichissent les profils et sont souvent utilisées pour améliorer les campagnes de marketing. Les cadres de protection de la vie privée existants peuvent déjà être appliqués et, bien que conférant plus de commodité au stade de la collecte des données, la RFID ne permettrait pas d'ajouter plus d'informations dans la base de données de l'entreprise. Certaines parties prenantes estiment toutefois que cette technologie permettrait

d'obtenir davantage d'informations, comme par exemple des indications en temps réel sur le lieu, ou l'historique du produit.

La situation serait sans doute différente avec un système à boucle ouverte, où les données RFID éventuellement associées à des personnes identifiées ou identifiables pourraient être consultées ou lues par de nombreux acteurs en raison de l'interopérabilité, et où une grande quantité de données personnelles pourraient être regroupées. Bien que les caractéristiques d'interopérabilité et de normalisation ne soient exploitées pour l'instant que par quelques applications de RFID, elles pourront présenter des intérêts pour ceux qui souhaitent déployer la RFID à grande échelle. Certaines parties prenantes considèrent que l'interopérabilité pourrait favoriser une plus grande dissémination des données personnelles (qui est un motif de limitation de la collecte, de l'objectif visé et de l'utilisation). Par exemple, si les puces portées par les personnes étaient, du fait de leur interopérabilité, lisibles par n'importe quel individu doté du matériel adéquat, cela pourrait encourager certains à recueillir des données personnelles qu'ils n'auraient pas collectées sinon. La collecte de données personnelles pourrait progressivement devenir la norme, au lieu d'être l'exception.

L'interopérabilité pourrait en outre faciliter l'adoption de spécifications en matière de protection des données. Ainsi, la proposition émise par des chercheurs universitaires d'intégrer dans la norme ISO du protocole lecteur-puce des politiques explicites sur le respect de la vie privée, inspirées des principes de l'OCDE (Floerkemeir, 2004), montre tout d'abord que des dispositifs RFID respectueux de la vie privée peuvent être envisagés, et laisse ensuite entendre que les instances et les processus de normalisation pourraient faciliter leur généralisation. Dans un autre exemple, au niveau des politiques, la Commission européenne (2007a) a demandé aux organismes de normalisation européens de s'assurer que les normes européennes et internationales répondaient aux exigences européennes, notamment en ce qui concerne la vie privée et la sécurité, afin de mettre en évidence les lacunes et de créer le cadre qui convient pour l'élaboration des prochaines normes sur la RFID.

Si l'interopérabilité peut être une source d'avantages pour les entreprises et supprimer les obstacles techniques à la dissémination des données personnelles, nombreux sont les cas où les entreprises considéreront que les informations issues de la RFID sont trop stratégiques pour être partagées. « Wal-Mart ne veut pas que ses concurrents lisent les puces qui sont déployées dans les magasins de son enseigne. Wal-Mart ne veut probablement pas que ses fournisseurs aient connaissance d'informations sur les autres fournisseurs de l'enseigne. Il veut garder la mainmise sur ces informations pour des raisons de compétitivité »[70].

Enfin, un autre problème est souvent cité lorsqu'il est question de la RFID et de son utilisation à grande échelle : la création d'un pilier supplémentaire qui soutiendrait l'infrastructure de surveillance des personnes qui est train d'apparaître, c'est-à-dire une infrastructure RFID globale et parfaitement interopérable, qui pourrait permettre aux puces d'être lues par n'importe quel individu équipé d'un matériel dûment connecté. Bien que cela ne risque pas de se produire à court terme – raison pour laquelle nous n'abordons pas le sujet dans le présent document – il est important de garder à l'esprit que toute étude s'intéressant au concept d'infrastructure de surveillance des personnes devra tenter d'évaluer les possibilités de convergence entre plusieurs technologies et processus susceptibles de faciliter la tâche de surveillance, comme par exemple la RFID et les réseaux à base de capteurs, la biométrie ou la gestion des identités numériques.

70. FTC des États-Unis (2005), p. 15.

2.2.2 Garanties possibles

Les *Lignes directrices de l'OCDE sur la protection de la vie privée*, adoptées en 1980, sont le fruit d'un consensus international sur la politique générale à adopter concernant la collecte et la gestion des données personnelles. Leur mise en œuvre dans le contexte de la RFID risque toutefois de susciter un certain nombre de questions. Elle peut cependant être facilitée par différents principes et outils relevant des pouvoirs publics.

2.2.2.1 Principes de protection de la vie privée

La première question de fond que l'on peut se poser lorsque l'on envisage d'utiliser les *Lignes directrices de l'OCDE sur la protection de la vie privée* pour garantir le respect de la vie privée dans le contexte de la RFID est : « Quand la RFID relève-t-elle du champ d'application des *Lignes directrices de l'OCDE* ? ». Les deux sections qui suivent tentent de répondre à cette question en analysant à quel moment les données RFID peuvent être considérées comme personnelles, et quand l'opérateur de cette technologie est le maître du fichier. La section suivante s'intéresse aux problèmes soulevés par l'invisibilité de la RFID, et notamment aux questions ayant trait à l'information et au consentement de la personne concernée. Bien évidemment, et conformément au principe des garanties de sécurité figurant dans les *Lignes directrices sur la vie privée*, les mesures de protection qui ont été examinées dans la section du présent rapport consacrée à la sécurité sont primordiales pour que les systèmes RFID garantissent le respect de la vie privée.

2.2.2.1.1 Quand la RFID relève-t-elle du champ d'application des *Lignes directrices de l'OCDE sur la protection de la vie privée* ?

Selon les *Lignes directrices de l'OCDE sur la protection de la vie privée*, « par "données de caractère personnel", on entend toute information relative à une personne physique identifiée ou identifiable ». Étant donné que ces lignes directrices ne concernent que les données personnelles, lorsque les technologies RFID sont utilisées dans des contextes où les données ne concernent pas une personne physique identifiée ou identifiable, les principes de protection de la vie privée ne sont pas applicables. Cependant, comme on le verra ci-après, il peut y avoir des risqués pour la vie privée si les données RFID sont associées à un individu meme quand la possibilité d'identification de cet individu est assez basse. Dans tous les cas, comme on peut le lire dans l'exposé des motifs de ces *Lignes directrices* : « Il peut être difficile de tracer la ligne de démarcation précise entre les données de caractère personnel au sens de l'information relative à des personnes identifiées ou identifiables et les données anonymes, et c'est à la réglementation de chaque pays Membre qu'il appartiendra de le faire. »[71]

Dans certains cas, les données RFID sont sans conteste à caractère personnel (par exemple, dans de nombreuses applications de contrôle d'accès). Dans d'autres, elles peuvent prendre un caractère personnel lorsqu'il est possible de les associer à une personne identifiable. Ainsi, lorsque la RFID est utilisée dans la chaîne logistique, le numéro unique enregistré sur la puce qui est, par exemple, fixée sur une boîte de médicaments pour des besoins d'identification et de suivi, n'entre pas dans la catégorie des données personnelles. En revanche, les mêmes informations peuvent acquérir un caractère personnel si elles sont collectées ou traitées de telle façon qu'un tiers puisse les associer à un autre ensemble d'informations se rapportant à une personne (par exemple, par une infirmière pour savoir quel patient a reçu tel médicament, ou par une pharmacie pour fournir des services d'assistance à ses clients).

71. Exposé des motifs des *Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*, paragraphe 41.

Par conséquent, si certaines données sont personnelles par nature (le nom, par exemple), d'autres peuvent le devenir une fois qu'elles sont associées à une personne identifiée ou identifiable, ce qui dépend du contexte. L'une des conséquences est que les entités qui mettent en œuvre des systèmes RFID ne sont pas systématiquement soumises aux cadres de protection des données. Une analyse attentive de la nature et de l'utilisation des données RFID à chaque étape de leur cyle de vie est indispensable pour déterminer si elles doivent être considérées comme personnelles et pour éviter de les traiter comme telles lorsque ce n'est pas nécessaire.

Une zone d'ombre continue à susciter la polémique, à savoir la possibilité d'utiliser des données RFID uniques pour distinguer une personne d'une autre au sein d'un groupe. Ce type d'usage est en fait très similaire aux cookies Internet, à la différence qu'un cookie ne peut être lu que par le serveur qui l'a envoyé à l'ordinateur client, alors que la RFID pourrait, si son interopérabilité était mise en œuvre, permettre au magasin A de lire les puces qui sont fixés aux articles vendus par le magasin B. Le client pourrait tirer des avantages de cette identification, mais pourrait aussi considérer dans certains cas que la collecte de données est une atteinte à sa vie privée, *a fortiori* si le magasin établissait un lien entre les données RFID et le client.

Le Groupe de travail européen Article 29 estime que la collecte, sur une ou plusieurs puces RFID, d'un ensemble de données uniques qui pourraient être associées à une personne en particulier place ces données à caractère personnel dans le champ d'application de la loi européenne sur la protection des données. Ce point de vue a été remis en question par des représentants de l'industrie qui considère que les cadres de protection des données ne devraient s'appliquer que lorsque les données traitées par les systèmes RFID soit contiennent des informations nominatives telles que le nom, un numéro de compte ou d'enregistrement soit sont combinées avec d'autres données personnelles (par exemple les données personnelles enregistrées dans une base de données ou dans une carte à puce)[72].

Les partisans de la protection de la vie privée soutiennent que le fait de pouvoir établir un lien entre un ensemble de caractéristiques et une personne bien précise peut constituer dans certains cas une atteinte à la vie privée de cette personne, qu'elle puisse être nommée ou non. Pour l'individu, les inférences pourraient fournir au responsable du système RFID un niveau de probabilité d'identification suffisament élevé pour générer des problèmes de protection de la vie privée même lorsque la personne ne peut pas être formellement identifiée. Les techniques permettant de désigner des individus au milieu d'une foule présentent des risques de discrimination, de fixation dynamique des prix ou d'activités criminelles. Toutefois, certaines entreprises soulignent que le fait, dans ces cas-là, de considérer les informations RFID comme des données de caractère personnel conduirait à l'impossibilité de respecter certaines obligations, comme par exemple le droit des individus à accéder aux informations qui les concernent[73].

À ce stade, et alors que le débat se poursuit[74], on peut considérer que le fait de pouvoir traiter chaque personne de façon spécifique risque de susciter des problèmes d'atteinte à la vie privée dans certains contextes, le degré de risque étant proportionnel à plusieurs facteurs : *i)* la spécificité des données

72 . International Chamber of Commerce et al., 2005, section 4.2; EPCglobal, 2005a, section 3.1; EPCglobal, 2007.

73. Si une personne A demande à consulter les données qui la concernent, comment le maître du fichier saura-t-il dans quel enregistrement de la base de données elles se trouvent ? La personne A devra fournir le(s) puces(s) qui ont été associée(s) à son nom par le maître du fichier, afin que celui-ci puisse retrouver les données dans le système et lui permettre d'y accéder. Or, rien ne prouvera que les puces appartiennent bien à cette personne, et donc que le profil présenté ne sera pas en fait divulgué à un individu se faisant passer pour la personne A.

74. Un document clé à cet égard est l'« Avis 4/2007 sur le concept de données à caractère personnel » du Groupe de travail Article 29 (juin 2007).

contenues sur la puce (les codes EPC, par exemple, sont véritablement uniques ; les codes propriétaire ne le sont peut-être pas autant ; les codes uniques cryptés restent des codes uniques) ou le nombre de puces qu'une personne transporte avec elle (plus ce nombre est élevé, et plus les chances de spécificité augmentent) ; *ii)* la probabilité que les puces soient ou non partagées par plusieurs personnes ; *iii)* la capacité de lire la puce à une distance suffisamment grande sans que la personne concernée n'intervienne et n'en ait conscience.

Une autre question primordiale est de savoir si l'opérateur de la RFID est le maître du fichier.

L'efficacité des cadres de protection des données et de la vie privée dépend dans une large mesure de la capacité à désigner une entité chargée de veiller au respect des règles sur la protection des données et dont la responsabilité sera engagée en cas de non-respect. La notion de maître du fichier a été définie dans ce but, et notamment pour éviter de faire reposer la responsabilité sur les sociétés et les individus agissant pour le compte d'autres entités. Cette notion revêt donc, comme c'est indiqué dans l'exposé des motifs des *Lignes directrices de l'OCDE sur la protection de la vie privée*, « une importance capitale ».

Selon les *Lignes directrices de l'OCDE sur la protection de la vie privée*, le maître du fichier désigne toute personne qui « est habilitée à décider du choix et de l'utilisation des données de caractère personnel »[75]. Comme nous l'avons vu plus haut, l'association des données RFID avec une personne identifiée ou identifiable dépend du contexte : le numéro d'identification d'une boîte de médicaments, par exemple, n'est pas une information à caractère personnel, mais il le devient s'il est destiné à être associé à d'autres informations relatives à une personne identifiée ou identifiable.

L'interprétation à la lettre de la définition de « maître du fichier » risque de poser des problèmes dans le contexte de la RFID, car décider du choix des données RFID n'est pas la même chose que de décider du choix des données personnelles. La plupart du temps, le fabricant d'une marchandise sera habilité à décider du choix des données RFID, mais il ne saura pas si elles seront un jour associées à des personnes. Inversement, un magasin qui déploie la RFID peut décider d'utiliser les données figurant sur les puces pour établir un profil de ses clients. Par conséquent, la notion de maître du fichier gagnerait, dans le domaine de la RFID, à être interprétée en gardant à l'esprit que le choix des données personnelles sera le plus souvent lié au choix d'associer les données RFID avec des personnes. Dans une certaine mesure, c'est la façon dont les données RFID sont utilisées qui leur donne ou non un caractère personnel.

En conséquence, lorsqu'une entité lit une puce RFID et associe ses données à la personne qui achète, transporte ou porte la puce, elle peut être considérée comme le maître du fichier, et assumer à ce titre toutes les responsabilités découlant des *Lignes directrices sur la protection de la vie privée*. En revanche, lorsqu'une entité fournit à une personne une puce opérationnelle (non désactivée) mais qu'elle ne collecte ni n'enregistre aucune donnée RFID en rapport avec cette personne, on pourrait conclure que cette entité n'est soumise à aucune obligation en vertu des cadres de protection de la vie privée existants. Elle ne sera pas considérée comme le maître du fichier, même si le fait de fournir des puces opérationnelles à un individu pourrait permettre à un tiers de suivre la personne concernée en temps réel, éventuellement à son insu ou de manière illicite.

Ce cas de figure suscite une interrogation, qui est de savoir si cette entité n'aurait pas cependant pour responsabilité d'enlever ou de désactiver la puce avant de confier l'objet à la personne, ou *i)* d'informer la

75. « Par « maître du fichier », on entend toute personne physique ou morale qui, conformément au droit interne, est habilitée à décider du choix et de l'utilisation des données de caractère personnel, que ces données soient ou non collectées, enregistrées, traitées ou diffusées par ladite personne ou par un agent agissant en son nom », *Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*, paragraphe 1.

personne que l'objet comprend une puce en état de marche qui peut être lue à distance par un tiers, et *ii)* de l'informer sur le contenu de la puce et sur la manière de se prémunir contre la lecture à distance ou autres intrusions. Cela ne veut pas dire qu'une telle entité doive être considérée comme maître du fichier et être en tant que tel soumise aux obligations définies par les *Lignes directrices*, comme par exemple la participation individuelle ou la spécification des finalités.

L'une des approches adoptées pour résoudre cette question est celle de la commissaire à l'information et à la protection de la vie privée de l'Ontario, qui affirme que « les entités qui ont généralement le contact le plus direct et les relations les plus étroites avec la personne doivent être celles qui ont la responsabilité d'assurer la protection de la vie privée et la sécurité des données, quel que soit le moment où apparaît ou disparaît la puce RFID dans le cycle de vie du produit ». Des mesures telles que la désignation par les détaillants d'un « administrateur des informations » – à qui les particuliers peuvent demander des renseignements, des conseils, de l'aide et des solutions – ont également été proposées. Le document « Privacy Best Practices for Deployment of RFID Technology » mis au point par le *Center for Democracy and Technology* (CDT) américain indique que « la tâche d'information incombe à la société qui entretient une relation directe avec le consommateur ». Fait intéressant, ce document fait observer que la société ayant les relations les plus étroites avec la personne ne sait pas forcément que les produits qui lui sont fournis contiennent des puces RFID. Il recommande donc que « l'entité commerciale qui intègre des systèmes RFID dans ses produits en avise ses acheteurs directs et, dans la mesure du possible, encourage ces derniers à faire de même auprès de leurs propres acheteurs et ainsi de suite, afin de permettre à la société qui entretient une relation directe avec le consommateur de l'informer en bonne et due forme de l'utilisation de la technologie RFID »[76].

S'agissant des obligations d'information qui incombent aux entités fournissant des puces aux particuliers, il peut être intéressant de regarder de plus près d'autres cadres réglementaires. Ainsi, les *Lignes directrices de l'OCDE régissant la protection des consommateurs dans le contexte du commerce électronique*, qui datent de 1999, donnent des indications sur la politique d'information préconisée à l'égard du consommateur, en appelant les entreprises à fournir « des informations exactes et facilement accessibles qui décrivent les biens ou services offerts, et qui soient suffisantes pour permettre aux consommateurs de décider en connaissance de cause de s'engager ou non dans la transaction ». Ces lignes directrices ne s'appliquent qu'aux transactions électroniques. Cela étant, elles s'appuient sur des législations et des politiques régissant les pratiques commerciales loyales, que ce soit en ligne ou hors ligne. Il peut donc s'avérer utile d'appliquer ce principe d'information générale à toutes les parties intervenant dans la fourniture de puces RFID aux particuliers[77]. Un autre parallèle pourrait être établi avec l'exemple de la sécurité du produit et de la mise en garde du consommateur sur les risques existants.

2.2.2.1.3. Information et consentement

L'invisibilité de la technologie qui a été abordée plus haut est une caractéristique fondamentale de la RFID, mais aussi un multiplicateur de risque pour les atteintes potentielles à la vie privée que sont par exemple le profilage et le suivi. Ainsi, un profilage effectué à l'aide de la RFID pourrait poser moins de

76. Voir CDT (2006). Le document cité a été élaboré par des représentants de distributeurs de logiciels et de matériel, de sociétés utilisatrices de la technologie RFID, d'organismes professionnels et d'associations de défense des consommateurs.

77. Bien que les entreprises qui ne collectent pas d'informations personnelles auprès des particuliers ne soient pas soumises à l'obligation d'information, nombreux sont ceux qui estiment que le fait de préciser qu'elles ne collectent pas de données personnelles instaure un climat de confiance qui peut être bénéfique pour les particuliers, pour l'entreprise et pour l'image générale que donne la technologie de l'information concernée, ce qui contribue à faciliter son adoption.

problèmes si cette technologie était déployée en toute loyauté et transparence, et si les personnes concernées étaient préalablement informées et donnaient leur accord.

Lorsque les données RFID se rapportent à une personne identifiée ou identifiable, plusieurs principes de protection de la vie privée permettent ensemble de régler le problème de l'invisibilité et de faire face à la plupart des risques décrits dans la précédente section en ce qui concerne le suivi et le profilage. Énoncé dans les *Lignes directrices sur la protection de la vie privée*, le « principe de la limitation en matière de collecte » stipule que les données doivent être obtenues « le cas échéant, après en avoir informé la personne concernée ou avec son consentement ». Ce principe est renforcé par l'obligation de spécifier les finalités en vue desquelles les données sont collectées, au plus tard au moment de la collecte des données (« principe de la spécification des finalités »). Les données collectées ne doivent ensuite être utilisées et divulguées que pour atteindre ces finalités ou d'autres qui seraient compatibles avec les précédentes, ou avec le consentement de la personne concernée et lorsqu'une règle de droit le permet. Le « principe de la transparence » prévoit que le traitement des données personnelles ne doit pas avoir lieu de façon dissimulée, une approche corroborée par le « principe de la participation individuelle », qui donne aux personnes les moyens d'accéder aux données les concernant et de les contester.

Si le principe d'information ou de consentement de la personne se retrouve dans la plupart des orientations sur la RFID émises par les parties prenantes, ses interprétations varient quant à la teneur des informations à fournir, la façon de les fournir, ainsi que l'opportunité du consentement de la personne.

Un consensus semble se dégager entre plusieurs associations de défense des consommateurs et de protection de la vie privée ainsi qu'avec certains acteurs industriels[78] sur le fait que l'information des personnes est une exigence fondamentale[79], et qu'elle contribue à atténuer la résistance psychologique liée à l'invisibilité de la technologie en rendant cette dernière plus visible.

Bien qu'il y ait peut-être aussi un consensus sur la nécessité d'informer les personnes du fait que des données sont collectées à l'aide de la technologie RFID, la question du contenu et de l'efficacité de ces informations fait débat. Outre les informations sur les finalités de la collecte et le droit d'accès aux données, un certain nombre d'éléments pourraient être inclus dans les communications sur la RFID, comme par exemple : *i)* l'existence des puces; *ii)* leur contenu, leur utilisation et la façon dont elles sont gérées ; *iii)* l'existence d'un environnement de RFID ; *iv)* l'activité de lecture ; *v)* la possibilité de désactiver les puces ; *vi)* les coordonnées du service d'assistance.

L'importance des notices d'information sur la protection de la vie privée est depuis longtemps reconnue par l'OCDE, en particulier dans le contexte des activités en ligne[80]. Les études laissent cependant entendre que l'efficacité des notices d'information en ligne est inversement proportionnelle à la quantité et la complexité des éléments à communiquer (OCDE, 2006b). Dans le cas de la RFID, une information exhaustive du consommateur risque de ne pas être possible lorsque l'espace disponible sur les articles n'est pas suffisant pour insérer un texte détaillé, et lorsque la collecte et le partage des données ont lieu en temps

78. Y compris la Chambre de commerce internationale et EPCglobal (« Guidelines on EPC for Consumer Products »). Dans ces lignes directrices, EPCglobal indique : « Les consommateurs seront avertis clairement de la présence de l'EPC sur les produits ou leur emballage, et seront informés de l'utilisation de la technologie EPC. Cette information se fera par l'apposition d'un logo ou d'un identifiant EPC sur les produits ou leur emballage ».

79. « L'information est un élément capital du déploiement et du fonctionnement responsables de l'EPC. »

80. Les travaux de l'OCDE sur la protection de la vie privée en ligne reconnaissent que des notices d'information sont nécessaires en la matière, et des principes directeurs de l'OCDE (2003, p. 29) encouragent les entreprises et les pouvoirs publics à créer de telles notices et à les publier sur leur site Internet.

réel[81]. Il sera sans doute plus difficile de mettre au point des notices d'information efficaces pour la RFID que pour les notifications en ligne, où l'on a pu tirer parti de l'interactivité, des liens hypertexte et du caractère intrinsèquement informationnel du support Internet. Enfin, rien ne dit que les consommateurs seront prêts et aptes à comprendre et à assimiler des informations techniques sur la RFID avant de faire des choix.

Des études plus approfondies seront peut-être requises pour régler ce problème. Les solutions possibles sont par exemple des moyens d'information modernes tels que des alertes audio ou vidéo, et l'utilisation d'un symbole universel[82]. Des travaux complémentaires restent toutefois nécessaires pour trouver un consensus sur les informations qui doivent obligatoirement être communiquées et sur les moyens de diffusion les plus efficaces.

Lorsque les données RFID sont associées à une personne identifiée ou identifiable, la possibilité pour cette personne de consentir à ce que des données RFID la concernant soient collectées et rattachées à ses données personnelles est un paramètre important, du point de vue tant de la protection des données/de la vie privée que de la dimension psychologique (ou de la confiance). La difficulté à élaborer des notices d'information efficaces dans le contexte de la RFID risque de rendre la question du consentement encore plus importante.

Comme on peut le lire dans l'exposé des motifs qui figure dans les *Lignes directrices de l'OCDE sur la protection de la vie privée*, l'information de la personne concernée doit généralement être une exigence minimale ; en revanche, l'obtention de son consentement n'est pas toujours possible pour des raisons pratiques, ou peut aller à l'encontre de l'intérêt général. Les exemples de cas où l'information ou le consentement de la personne concernée ne peut être considéré comme nécessaire – les mises à jour courantes et les activités des services chargés de l'application de la loi – laissent toutefois entendre que ces cas doivent rester minoritaires[83].

Pour le Groupe de travail Article 29, le consentement est presque toujours souhaitable, sauf si le système RFID est autorisé par la loi ou est utilisé dans l'intérêt vital des personnes, comme c'est le cas pour certaines applications médicales. Un certain nombre d'entreprises, d'organismes de protection de la vie privée et de représentants de la société civile reconnaissent également que le consentement n'est pas toujours nécessaire, mais ne sont pas d'accord quant aux critères selon lesquels il doit être supprimé[84]. Des

81. Voir CIPL (Center for Information Policy Leadership), 2007.

82. Le *Center for Information Policy Leadership* a entrepris de mettre au point un symbole pour respecter le principe de transparence de la RFID. Voir CIPL (2007).

83. Paragraphe 52 : « La nécessité de porter les données à la connaissance de la personne concernée ou d'obtenir le consentement de cette dernière est une règle essentielle, cette connaissance constituant l'exigence minimale. En revanche, il n'est pas toujours possible, pour des raisons pratiques, d'imposer l'obtention du consentement. En outre, le paragraphe 7 rappelle également (« le cas échéant ») qu'il existe certains cas où, pour des raisons pratiques ou de principe, on peut ne pas juger nécessaire de porter les données à la connaissance de la personne concernée ou d'obtenir son consentement. Les enquêtes criminelles et la mise à jour courante des listes de distribution peuvent servir d'exemples à cet égard. »

84. Selon le *Transatlantic Consumer Dialogue*, « la RFID doit être utilisée de façon transparente, afin que les consommateurs sachent lorsqu'elle est utilisée (et puissent choisir) ». La *Privacy Rights Clearing House* reconnaît que pour certaines applications, il serait suffisant d'informer les particuliers, mais que ces derniers devraient avoir la possibilité de désactiver les puces, et préconise l'interdiction du suivi si la personne n'a pas donné son accord. Pour la Chambre de commerce internationale, « le choix du consommateur est, le cas échéant et dans la mesure du possible, un élément essentiel pour obtenir sa confiance et son adhésion ». Les « Guidelines for Consumer Products » (2005d) d'EPCglobal reconnaissent également que le choix est un principe fondamental et lancent un appel pour que de nouvelles méthodes efficaces, rentables et fiables soient trouvées pour accroître la faculté de choix du consommateur.

travaux complémentaires sur la question du consentement pourraient être utiles pour réduire ces divergences.

De manière générale, l'information et le consentement peuvent être considérés comme des conditions indispensables pour que la personne concernée fasse le choix opportun. On peut cependant rétorquer que parfois, cette personne n'a pas d'autre possibilité que d'accepter la collecte de données si elle veut bénéficier du service correspondant. À titre d'exemple, il est probable que les sociétés de transport en commun qui ont commencé à mettre en place des systèmes RFID pour contrôler l'accès au réseau finiront à terme par supprimer l'infrastructure servant à délivrer et traiter les tickets en papier. Le choix de l'utilisateur se limitera alors à accepter la collecte de données personnelles, ou à ne pas utiliser le réseau de transport en question. Lorsque l'alternative à la collecte de données personnelles implique de gros sacrifices financiers pour la personne, le consentement peut perdre alors toute valeur. L'information et le consentement ne sont pas la panacée pour la protection de la vie privée.

2.2.2.2 Autres garanties

Les mesures suivantes ne font pas explicitement partie des *Lignes directrices de l'OCDE sur la protection de la vie privée*, mais elles peuvent être utiles pour aider ou faciliter leur mise en œuvre.

2.2.2.2.1. Mesures techniques

En règle générale, il peut être intéressant d'envisager la mise en place de mesures techniques pour empêcher que les informations RFID soient utilisées dans des contextes où elles pourraient être associées à des personnes. La protection de la vie privée peut être intégrée à la conception des produits et des systèmes RFID.

Ainsi, des techniques spécifiques de minimisation ou d'agrégation/d'anonymisation des données peuvent contribuer à éliminer les risques d'utilisation détournée. La collecte du numéro de série figurant dans le code EPC pourrait par exemple être bloquée techniquement lorsqu'elle n'est pas nécessaire pour l'application concernée. De manière générale, le fait de rendre impossible l'association des données RFID avec les personnes concernées peut être un moyen efficace de maintenir ces informations dans la catégorie des données « non personnelles », et donc de protéger la vie privée. La minimisation, l'anonymisation des données et leur dissociation par rapport aux personnes peuvent aussi être effectuées au niveau des applications d'arrière-plan.

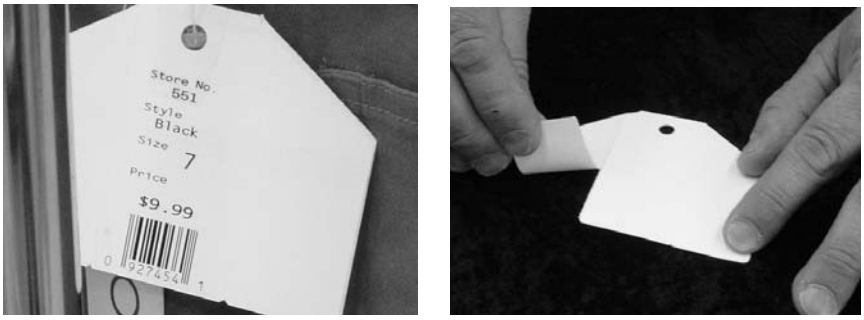
Les mesures techniques qui permettent aux opérateurs des systèmes RFID et aux particuliers d'avoir une mainmise sur la technologie peuvent aussi contribuer à prévenir ou atténuer les risques. Un certain nombre de programmes de recherche s'intéressent aux moyens techniques de protéger la vie privée[85]. Par exemple, la commande d'interruption (« kill ») qui figure sur le protocole Classe 1 Génération 2 d'EPCglobal peut être enclenchée sur le point de vente pour désactiver la puce de façon permanente[86]. L'antenne du « Clipped Tag » IBM peut être facilement enlevée par le client ou par le commerçant, ce qui transforme une puce UHF lisible à grande distance (10 m) en une puce lisible à faible distance (2 cm), utilisable pour des services de garantie, de traçabilité ou autres (voir Figure 8). Dans la plupart des cas, la

85. « Compte tenu des résultats de la consultation européenne, la Commission soutiendra aussi le développement des technologies de protection de la vie privée comme moyen de limiter les risques en la matière. » (Commission européenne, 2007a). Pour des exemples de travaux menés sur les mesures techniques de protection de la vie privée, voir Juels (2005a) et le site Internet de Gildas Avoine sur le thème « RFID, Security and Privacy ».

86. Les associations de consommateurs soutiennent la désactivation automatique des puces RFID au point de vente, sauf si le consommateur donne son accord pour la conserver. Voir ANEC/BEUC, 2007.

réduction de la distance de lecture à quelques centimètres rend nécessaire la participation préalable du client à la collecte des données, et peut constituer dans certains cas un moyen novateur d'atténuer – à défaut de supprimer - les risques d'atteinte à la vie privée. Cependant, comme il a été indiqué dans la section sur la sécurité, étant donnée la complexité et la variété de la technologie RFID et des scénarios possibles d'utilisation, on peut dire qu'il n'existe pas de solution technique universelle et parfaite pour protéger la vie privée.

Figure 8. « Clipped Tag » IBM



Note : Cette puce RFID fonctionnant sur la bande UHF peut être lue à une distance de 10 mètres jusqu'à ce que le consommateur la déchire, enlevant ainsi l'antenne. La puce continue de marcher, mais elle ne peut être lue qu'à une distance de quelques centimètres.

Source : Markowitz (2006).

Il convient de noter par ailleurs que les mesures techniques ont toujours un coût qui, dans certains cas, peut décourager les fabricants de dispositifs RFID d'intégrer une protection dans la conception des puces, et les opérateurs de RFID d'incorporer ces puces dans la conception de leurs systèmes RFID. De plus, dans un environnement concurrentiel, on ne sait pas très bien si la majoration du prix d'un produit (ou la diminution de la marge bénéficiaire par produit) due à l'utilisation de technologies respectueuses de la vie privée peut se transformer facilement en avantage commercial au profit d'un fabricant ou d'un produit particulier. Des stratégies visant à inciter les entreprises à élaborer et utiliser des technologies RFID incluant des protections suffisantes pour la vie privée pourraient être envisagées.

La minimisation de la collecte des données, l'anonymisation de celles-ci et l'utilisation de mesures techniques intégrant la protection de la vie privée dans la conception du système ne sauraient toutefois empêcher les maîtres de fichier d'informer les particuliers afin d'obtenir leur consentement ou leur participation active. Parallèlement, le fait d'informer les personnes et de solliciter leur accord ne devrait pas empêcher les maîtres de fichier d'utiliser des technologies respectueuses de la vie privée.

2.2.2.2.2. Évaluation de l'incidence sur la vie privée

Dans un contexte où les configurations techniques et les scénarios d'utilisation sont très variés, il n'existe pas de solution technique unique qui compenserait l'absence de consentement dans tous les cas de figure et assurerait un équilibre entre la protection de la vie privée, le coût, la commodité et la facilité d'emploi. Une étude approfondie pourra être nécessaire pour déterminer si – et dans quelle mesure – l'utilisation de la technologie suscite des problèmes d'atteinte à la vie privée avec un système particulier. Une telle analyse supposerait l'examen de l'application de la RFID, du type de données collectées, de la nature et des caractéristiques techniques de la RFID utilisée, et de la possibilité que les données collectées soient associées à une personne identifiée ou identifiable.

Les approches consistant à évaluer dès la conception l'incidence d'un système RFID sur la vie privée permettent de voir et de comprendre quels sont les risques d'atteinte à la vie privée et les stratégies les

mieux adaptées pour les atténuer. Ces approches peuvent être considérées comme de bonnes pratiques. Pour faire écho à ce qui a été dit plus haut concernant la gestion des risques en matière de sécurité, le choix d'une approche holistique pour la question de la protection de la vie privée – en prenant en compte chaque étape et chaque composant du système global – peut être considéré comme souhaitable. Il convient notamment d'étudier l'ensemble du cycle de vie des données RFID dans le système d'information global de l'organisation. Dans le cas où l'on déploie des systèmes utilisant des puces RFID interopérables, cette évaluation ne doit pas porter uniquement sur le système d'information initial mais aussi s'intéresser aux risques pour la vie privée que présente la puce durant tout son cycle de vie.

Comme nous l'avons vu dans la section consacrée à la sécurité, les technologies RFID ne sont pas toutes à égalité face à la probabilité de certains risques et, selon le contexte dans lequel elles sont utilisées, certaines présentent peu, voire pas de risques spécifiques. Le choix d'une technologie RFID plutôt qu'une autre peut avoir des conséquences importantes sur la vie privée. Un exemple type est la distance de fonctionnement des systèmes à ondes radio par rapport à celle de certains systèmes à induction magnétique dont le rayon est très limité, rendant parfois nécessaire une intervention humaine active pour l'opération de lecture. On peut suggérer, comme bonne pratique, que la protection de la vie privée soit l'un des critères utilisés pour déterminer les caractéristiques d'un système au moment de son élaboration.

2.2.2.2.3. Sensibilisation et compréhension

Les études menées aux États-Unis et en Europe[87] montrent que le grand public connaît très peu la RFID et ses implications, mais qu'il cherche à s'informer[88]. La FTC aux États-Unis, la commissaire à l'information et à la protection de la vie privée de l'Ontario et la commissaire européenne Viviane Reding, pour n'en citer que quelques-uns, ont appelé à ce que des efforts supplémentaires soient faits pour permettre à l'opinion de mieux comprendre quels sont les avantages et les risques de cette technologie. Mieux faire connaître et comprendre les possibilités et les lacunes de la RFID peut contribuer à éliminer les résistances psychologiques – fondées sur des faits réels ou des impressions – et à accroître l'efficacité des notices d'information sur la vie privée qui s'y rapportent. Cela pourra aider les consommateurs à faire des distinctions entre les différentes technologies RFID, à comprendre comment cette technologie est mise en œuvre lorsqu'ils interagissent avec elle, et à poser les bonnes questions sur le respect de la sécurité et de la vie privée[89]. Outre l'obligation officielle d'informer les particuliers, les pouvoirs publics pourront envisager d'encourager les opérateurs à fournir des descriptions accessibles à tous, exhaustives, transparentes et instructives sur les systèmes RFID, afin de donner des informations capitales sur la façon dont ils fonctionnent et la manière dont le respect de la vie privée a été pris en compte.

Les initiatives destinées à mieux faire connaître et comprendre cette technologie pourraient aussi consister à employer un langage simple et à éviter le jargon technique qui peut rendre les choses inintelligibles, vu que cette technologie se développe et touche le grand public. Décrire la RFID en gardant à l'esprit qu'il faut instruire le lecteur peut certainement être utile à cet égard. Comme nous l'avons évoqué plus haut, le seul acronyme « RFID » est trompeur, et des expressions comme « champ proche » et

87. Près des deux tiers des réponses formulées lors de la consultation en ligne effectuée auprès du public par la Commission européenne en 2006 ont indiqué que jusqu'à ce jour, les informations disponibles n'étaient pas suffisantes pour permettre aux particuliers de se faire une opinion éclairée sur la part de risques que présente la RFID (Commission européenne, 2007a). L'étude réalisée par Cap Gemini (2005a et 2005b) conduit au constat que même si elle est un peu plus poussée aux États-Unis, la connaissance générale de la RFID est faible, que ce soit dans ce pays ou en Europe.

88. Cap Gemini (2005a).

89. Des campagnes d'information visant les expliquant aux individus comment protéger les puces RFID pourraient également être envisagées.

« champ lointain », bien qu'ayant sans aucun doute un sens au niveau technique, risquent de déconcerter le grand public.

Une autre source de confusion peut être la généralisation, à la hausse ou à la baisse, du degré de risque associé à la RFID, qui peut vite être abusive dans certaines situations et risque d'être déstabilisante. Le débat sur les risques et les avantages de cette technologie s'appuie fréquemment sur des exemples de scénarios bien particuliers, qui donnent lieu à des généralisations inexactes. Il existe différents types de technologies RFID, avec des propriétés différentes et de nombreuses façons de les mettre en œuvre. Il y a des cas où la protection de la vie privée est une source de préoccupation justifiée, comme il y en a d'autres où l'incidence sur la vie privée est quasiment nulle. Il est donc important d'éviter de tirer des conclusions générales à partir d'exemples spécifiques, car les avantages ou les inconvénients d'une mise en œuvre ne sont pas forcément transposables à une autre. Plutôt que de centrer son attention sur la technologie elle-même et sur le fait qu'elle a de manière générale une incidence bonne ou mauvaise sur la vie privée, il vaut mieux adopter une approche plus équilibrée qui pourrait consister à examiner de quelle façon la RFID est mise en œuvre, si les risques sont pris en compte et comment ils sont gérés.

Les efforts de sensibilisation et d'éducation peuvent contribuer dans une large mesure à clarifier les choses et à faciliter le déploiement des technologies RFID, dans l'intérêt des entreprises et des particuliers. Cela étant, comme cela a été montré dans la première section du document, la RFID est une technologie complexe, et elle va sans doute le rester. Il y a par conséquent des limites aux résultats que la sensibilisation et l'éducation peuvent donner. On ne peut donc s'attendre à ce que l'homme de la rue ait compris toutes les subtilités de la sécurité des données et de la protection de la vie privée qui concernent la RFID lorsqu'il fera ses courses au supermarché, prendra le métro et utilisera son passeport ou le badge remis par son employeur. Comme pour toutes les technologies de l'information qui sont un jour utilisées par le grand public, l'éducation est l'une des réponses aux questions de la sécurité et de la protection de la vie privée, mais elle ne saurait être la seule.

CONCLUSION

Les technologies RFID sont souvent présentées par leurs partisans comme la « prochaine grande révolution informatique », et font l'objet d'une profusion de communications et de publicités, qui tournent parfois au battage marketing ou au récit à sensation. Ce phénomène peut aider à faire connaître une technologie qui présente un gros potentiel positif pour les entreprises et les particuliers. Mais il peut aussi avoir les effets inverses. La complexité des technologies RFID, leur diversité technique et leurs innombrables possibilités d'application sont des facteurs de malentendus. Comme toutes les technologies de l'information, si la RFID était mise en œuvre sans prendre en compte comme il se doit les risques qu'elle présente en matière de sécurité et de vie privée, elle pourrait porter préjudice à l'entreprise qui l'a déployée, et avoir des effets néfastes sur les personnes concernées. Si des risques étaient détectés sur des systèmes RFID – existants ou futurs – sensibles (comme les passeports et les cartes de crédit), utilisés à grande échelle (dans les transports par exemple) ou spectaculaires (tels que les implants), il se pourrait que le tapage qui est fait autour de la RFID se transforme en peur, ternissant l'image qu'a le grand public de cette technologie et menaçant son avenir prometteur. Ce scénario est déjà d'actualité. Un certain nombre de systèmes RFID ont été déployés sans considération suffisante pour la sécurité et la vie privée, ont été la cible de vives critiques de la part des organismes de défense des consommateurs et de protection de la vie privée, et ont conduit à la création de groupes d'opposants ou anti-« puces espionnes » (*spychips*). Parallèlement, un dialogue a été engagé entre l'industrie, la société civile et les organismes de défense des consommateurs et de protection de la vie privée pour développer de bonnes pratiques en matière de sécurité et de respect de la vie privée.

La transparence implique que les individus comprennent ce que la technologie peut et ne peut pas faire. Sensibiliser le public sur les capacités et les lacunes de la technologie peut être une condition nécessaire pour empêcher les particuliers et les entreprises déployant la RFID d'imaginer des risques qui n'existent pas ou d'en négliger d'autres bien réels, et pour les aider à faire les bons choix.

Les *Lignes directrices de l'OCDE sur la sécurité* fournissent un cadre neutre et adaptable qui peut être appliqué aux systèmes et réseaux RFID. Tous les principes qui y sont énoncés peuvent être pris en compte dans le contexte de la RFID.

Les *Lignes directrices de l'OCDE sur la protection de la vie privée* sont également applicables aux systèmes RFID lorsque des données personnelles entrent en jeu. Le présent document laisse toutefois entendre que le dialogue reste nécessaire pour éclaircir ou trouver un accord sur plusieurs points, comme par exemple : *i)* les notions de données personnelles et de maître du fichier ; *ii)* la nature des informations à fournir au public et les meilleurs moyens de les communiquer pour que la transparence soit efficace ; *iii)* les cas dans lesquels le consentement des personnes est ou n'est pas nécessaire. La transparence a été présentée comme primordiale, à la fois de la part des maîtres de fichier et des entités qui fournissent des puces aux particuliers sans avoir le statut de maîtres de fichier.

Bien que les principes de l'OCDE sur la protection de la vie privée fournissent un cadre indispensable pour la protection de la vie privée, y compris pour les systèmes RFID, le présent rapport appelle en outre l'attention sur d'autres pratiques et mesures qui figurent dans les *Lignes directrices sur la sécurité* de 2002, et qui pourraient aider à la mise en œuvre des principes de protection de la vie privée et accroître leur efficacité.

Faisant écho aux indispensables évaluations des risques sur le plan de la sécurité, des pratiques telles que l'évaluation des incidences sur la vie privée peuvent permettre de mettre en évidence les problèmes dès le début d'un projet, et de choisir les mesures de prévention et d'atténuation les mieux adaptées et les plus rentables. Cette manière de procéder pourra éviter de mettre au point des systèmes qui risquent de porter atteinte à la vie privée et qu'il serait extrêmement coûteux de transformer par la suite en systèmes respectueux de la vie privée. Comme l'on ne peut pas espérer que les problèmes de sécurité et de vie privée soulevés par la RFID soient résolus complètement au niveau de la technologie, une approche holistique – comprenant l'évaluation des risques en matière de sécurité, l'évaluation des incidences sur la vie privée, et la gestion de tous ces éléments – a été préconisée tout au long du présent document. Cette approche se justifie par la diversité des technologies RFID ainsi que de leurs éventuelles applications et utilisations, par l'évolution constante de ces technologies et des risques, et par les interdépendances entre les systèmes RFID et les autres dispositifs auxquels ils sont connectés.

La disponibilité et l'adoption de mesures techniques faciles à mettre en œuvre, efficaces et peu coûteuses pour la sécurité et la protection de la vie privée pourraient être les clés d'un déploiement réussi de la RFID. De telles mesures existent déjà. Toutefois, leur coût et leur complexité technique peuvent constituer des obstacles à leur mise en œuvre dans certains domaines. Des recherches sont certes en cours, mais des efforts dans ce sens et des initiatives visant à inciter la mise en place de ces mesures techniques pourraient être bénéfiques. Cela étant, la sécurité et la protection de la vie privée ne doivent pas dépendre uniquement de dispositions techniques, mais plutôt d'un ensemble de mesures opérationnelles, techniques et de gestion. Enfin, le fait d'intégrer la protection de la vie privée dans la technologie plutôt que de l'ajouter après coup a été présenté par plusieurs spécialistes des aspects techniques et des questions politiques comme une méthode pouvant s'avérer efficace. Les approches de « protection intégrée de la vie privée » (« *privacy by design* ») ou les technologies favorisant la protection de la vie privée, que ce soit au niveau puce/lecteur ou en arrière-plan, pourraient être encouragées.

Globalement, la RFID est un sujet de préoccupation pour un large éventail de parties prenantes, depuis les ingénieurs et les concepteurs des systèmes jusqu'à ceux qui achètent la technologie et leurs clients, en passant par les particuliers qui portent éventuellement les objets marqués. Certaines parties prenantes (les fournisseurs, par exemple) ont plus tendance à mettre l'accent sur les mesures préventives pour réduire les risques, alors que d'autres vont peut-être privilégier les mesures visant à atténuer les conséquences des lacunes (les utilisateurs, par exemple). Une communication efficace et une coopération étroite entre toutes les parties prenantes, y compris les particuliers, peuvent contribuer à améliorer les systèmes RFID en matière de sécurité et de protection de la vie privée.

Le présent rapport constitue la première étape d'une série de travaux de l'OCDE consacrés aux questions de sécurité et de protection de la vie privée dans les environnements faisant appel à des capteurs[90]. Les résultats et les conclusions de ce rapport concernent les utilisations actuelles et à court terme des technologies RFID. Or, ces technologies et leurs utilisations évoluent rapidement. Il est donc primordial de suivre cette évolution et de détecter les éventuelles nouvelles tendances qui nécessiteraient une nouvelle analyse, voire modifieraient les résultats actuels et conduiraient à d'autres conclusions. À cet égard, un certain nombre de faits nouveaux susceptibles de se produire risquent de créer des problèmes qui ne sont pas abordés dans le présent document. Ces faits nouveaux sont par exemple la généralisation du marquage des objets et des applications RFID à boucle ouverte traitant des données personnelles. La création d'un « Internet des choses » ainsi que le développement et le déploiement à grande échelle d'autres technologies à base de capteurs pourraient, en supprimant à terme les frontières entre le monde physique et le monde virtuel, modifier à longue échéance la nature des problèmes de sécurité et de protection de la vie privée, et restent à étudier.

90. Il est complété par les travaux du Groupe de travail sur l'économie de l'information (GTEI). Voir OCDE 2007b et 2007c.

ANNEX I. EXAMPLES OF RFID STANDARDS (disponible en anglais uniquement)

RFID standards include (AIM, n.d. 2006):

- A number of standards developed and adopted by national and regional standardisation organisations such as the American National Standards Institute (ANSI), the European Telecommunication Standards Institute (ETSI) and the European Committee for Standardization (CEN);

- Standards and specifications adopted by sector specific standards organizations, such as the specification for RFID biometric passports adopted by the International Civil Aviation Association (ICAO) which defines how ISO 14443 standard on contactless smartcards should be implemented for travel documents (ICAO, 2004) and the Automotive Industry Action Group (AIAG) "Application Standard for RFID Devices in the Automotive Industry" (ARF-1) or "Tire and Wheel Identification Label Standard" (B-11); and

- The MIT Auto-ID Center (now Auto-ID Labs)[91] specifications related to the Electronic Product Code (EPC), now included in the work of GS1/EPCglobal[92], as well as EPCglobal Architecture Framework which includes a collection of interrelated standards for hardware, software, and data interfaces, with core services for enhancing the supply chain. EPCglobal/GS1 Class 1 Generation 2 standard has been ratified by ISO in July 2006 as ISO 18000-6C.

91. The Auto-ID Center, created in 1999 was replaced in 2003 by the Auto-ID Labs which is a network of academic research labs.

92. EPCglobal is a joint venture between GS1 (former EAN International) and GS1 US, former Uniform Code Council, both bodies regulating barcode in Europe and in the US respectively.

The table below highlights the main international RFID standards.

Table 9. Main International RFID Standards

ISO 10536	Identification cards – Contactless integrated circuit(s) cards (cards operating at very short proximity, < 1cm)
ISO 14443	Identification cards – Proximity integrated circuit(s) cards (cards operating at 10 cm distance and include a microprocessor). For example, this is the standard chosen by ICAO for passports (ICAO, 2004)
ISO 15693	Identification cards – contactless integrated circuit(s) cards – Vicinity cards (cards operating at 1 meter and usually not containing a microprocessor).
ISO 18000	RFID for Item Management - Air Interface (description of the standard air interface operating below 135 KHz, at 13.56 MHz, 2.45 GHz, 860 MHz to 960 MHz, 433 MHz)
ISO 10374	Freight containers -- Automatic identification (includes a container identification system, data coding systems, description of data, performance criteria and security features)
ISO 11784, ISO 11785, ISO 14223	Animal tagging
ETSI TS 102.190, ISO 18092, and ECMA 340	Near Field Communications Interface and Protocol-1 (NFCIP-1)
Standards directly related to Electronic Product Codes (EPC):	
Auto-ID Center Specifications	• 900 MHz Class 0 Radio Frequency (RF) Identification Tag Specification (communications interface and protocol, RF, and tag requirements, operational algorithms for 900MHz communications) • 13.56 MHz ISM Band Class 1 Radio Frequency (RF) Identification Tag Interface Specification (communications interface and protocol, RF, and tag requirements). • 860MHz -- 930 MHz Class 1 Radio Frequency (RF) Identification Tag Radio Frequency & Logical Communication Interface Specification (defines communications interface and protocol, RF, and tag requirements). • Conformance Requirements Specification v. 1.0.4 for Class-1 Generation2 UHF RFID (compliance for physical interactions (the signaling layer of the communications), operating procedures, and commands; between interrogators and tags for 860 MHz – 960 MHz communications.)
EPCglobal Architecture Framework	A collection of interrelated standards for hardware, software, and data interfaces, with core services for enhancing the supply chain through the use of Electronic Product Codes (EPCs). Includes standards for : • Tag Data, • EPC Tag Data Translation, • Class 1 Generation 2 UHF Air Interface Protocol (“Generation 2”), approved as ISO 18000-6C in July 2006 • Reader Protocol, • Reader Management, • Application Level Events , • Object Naming Service (ONS), • Certificate Profile, • Drug Pedigree • EPC Information Service version 1.0, approved on 12 April 2007.

Sources: Pedris-Lopez, 2006; RFID Association Australia website (www.rfidaa.org/standards) ; EPCglobal web site (www.epcglobalinc.org/standards/);

ANNEX II. NFC, UWB, ZIGBEE, RUBEE, WI-FI, ULTRASONIC TECHNOLOGIES (disponible en anglais uniquement)

Near Field Communication (NFC): is a short range technology that enables two devices to communicate when they are brought into actual touching distance. Sponsored by the NFC Forum which groups more than 100 companies including Sony, NXP (Philips) and Nokia, NFC enables sharing power and data using magnetic field induction at 13.56MHz (HF band), at short range, supporting varying data rates from 106kbps, 212kbps to 424kbps. A key feature of NFC is that it allows two devices to interconnect. In reader/writer mode, an NFC tag is a passive device that stores data that can be read by an NFC-enabled device (*e.g.* smart poster, for which a technical specification was developed). In Peer-to-Peer mode, two NFC devices can exchange data. For example, Bluetooth or Wi-Fi link set up parameters can be shared using NFC and data such as virtual business cards or digital photos can be exchanged. In Card Emulation mode, the NFC device itself acts as an NFC tag, appearing to an external reader as a traditional contactless smart card. This enables contactless payments and e-ticketing, for example. NFC is backed by 14 mobile operators representing 40% of the global mobile market.[93] NFC standards are acknowledged by major standardisation bodies and based on ISO/IEC 18092.

NFC mode	Applications
Peer to peer mode	Connect electronic devices
Read/Write mode	Access digital content (*e.g.* poster)
Card emulation mode	Make contactless transactions

ZigBee[94] : developed and promoted by the association of companies called "ZigBee alliance", the ZigBee specification adds application profile, security and network layers to IEEE 802.15.4 standard for wireless low-rate personal area networks. It operates in the UHF/microwave bandwidth with battery powered tags that communicate with each other. ZigBee adds to IEEE 802.15.4 the option of AES-128 encryption security. ZigBee protocols are intended for use in embedded applications requiring low data rates and low power consumption, enabling devices to form a mesh network of up to 65 000 nodes, covering a very large area.[95] It targets general-purpose, inexpensive, self-organizing, mesh network that can be used for industrial control, embedded sensing, medical data collection, smoke and intruder warning, building automation, home automation, domotics, etc. The resulting network will use very small amounts of power so individual devices might run for a year or two using the originally installed battery.

RuBee is a commercial name for a peer to peer communication protocol designed for active or passive tags operating at Low Frequency (using magnetic induction), suitable in environments containing water and/or metal. It is being standardised by IEEE as P1902.1 "IEEE Standard for Long Wavelength

93. "Mobiles Hope to be 'smart wallet'", BBC News Web site, International version, 21 November 2006, http://news.bbc.co.uk/2/hi/technology/6168222.stm.

94. See the Zigbee Alliance web site: www.zigbee.org. The name ZigBee comes from the zigzag path of bees which serves to signal new food location to other members of the colony, an analogy of mesh network topology.

95. « So, Who Needs ZigBee?", 8 November 2005, http://rfdesign.com/next_generation_wireless/who-needs-zigbee/ See also www.zigbee.org/en/press_kits/092706/Documents/ZigBeeTutorial.pdf.

Wireless Network Protocol ". According to IEEE, the standard "will offer a "real-time, tag searchable" protocol using IPv4 addresses and subnet addresses linked to asset taxonomies that run at speeds of 300 to 9,600 Baud. RuBee Visibility Networks are managed by a low-cost Ethernet enabled router. Rubee enables tag networks and telepresence applications. Individual tags and tag data may be viewed as a stand-alone, web server from anywhere in the world. Each RuBee tag, if properly enabled, can be discovered and monitored over the World Wide Web using popular search engines (*e.g.*, Google). [96]

Wi-Fi and **Bluetooth** communication protocols are usually not considered as RFID or sensor technologies since they were originally designed for connecting devices such as PCs, laptops and printers. They are commercial names for communication protocols IEEE 802.11 and IEEE 802.15.1. Both operate in the same frequency range (near 2.4 GHz). Bluetooth is a building block for personal area networks (PAN) or short distance wireless networks which connect together devices such as PC, Personal Digital Assistants (PDA), peripherals (keyboard, mouse…), cell phones, pagers, etc. Wi-Fi was developed to be used for laptop connectivity to local area networks but is now increasingly used for more services, including Internet and voice over IP, and connectivity of computer devices such as printers, webcams, DVD players, etc. However, several vendors have developed Wi-Fi active tags that allow for the use of existing Wi-Fi coverage and access points instead of deploying a specific RFID communication infrastructure. They are being used for example for asset tracking in power plants and hospitals, by theme amusement parks such as in Legoland (Denmark) to help parents find their children or to keep track of automotive vehicles in Venice (Italy) Port's visitor parking facility (Malykhina, 2005; Collins, 2004; Aeroscout, 2005).

Ultra Wide Band[97] can enable wireless connectivity at very large bandwidth for very close electronic devices (*e.g.* computer and monitor). UWB technology transmits information spread over a very large bandwidth (25% or more of the center of the center frequency or at least 500 MHz)[98] but at very low power levels thus not interfering with other narrower band devices nearby. The receiver translates the pulses into data by listening for a familiar pulse sequence sent by the transmitter. As the data is moving on several channels at once, it can be sent at high speed, up to 1 gigabit per second. It also has the ability to penetrate walls. Frequency regulations limits UWB to low power levels in order to keep interferences at or below to the level of noise produced unintentionally by electronic devices such as TV sets. As a consequence, UWB is limited to short range applications, enabling wireless connectivity (*e.g.* wireless monitors, camcorders, printing, music players), home or office networking, automotive collision detection systems, medical imaging, etc. It is promoted by two industry associations, the WiMedia Alliance and the UWB Forum.[99] UWB is a fairly new technology that was regulated in 2002 by the US Federal Communications Commission (FCC), in 2006 in Japan and in 2007 in Europe (Yomogita, 2006; Holland, 2007). As it has been regulated only recently, the type of innovative applications it will enable in the future is still unclear.

---

96. "IEEE Begins Wireless, Long-Wavelength Standard for Healthcare, Retail and Livestock Visibility Networks", 8 June 2006, IEEE, http://standards.ieee.org/announcements/pr_p19021Rubee.html.

97. Elements of information about UWB come from the following sources: Ultrawideband planet, FAQ, www.ultrawidebandplanet.com/faq/. "An introduction to Ultra Wide Band (UWB) wireless", Rafael Kolic, 24 February 2004, Deviceforge.com, www.deviceforge.com/articles/AT8171287040.html. "Intel and UWB", www.intel.com/standards/case/case_uwb.htm.

98. "A UWB signal centered at 2 GHz would have a minimum bandwidth of 500 MHz and the minimum bandwidth of a UWB signal centered at 4 GHz would be 1 GHz. The most common technique for generating a UWB signal is to transmit pulses with durations less than 1 nanosecond". UWB resource center, Palowireless; "Ultra Wide Band Tutorial", www.palowireless.com/uwb/tutorials.asp.

99. See www.wimedia.org and www.uwbforum.org.

Ultrasonic (based on ultrasound waves) technology enables tags to transmit unique 20 kHz to 40 kHz acoustic signals to a receiver. The signal does not require a line of sight between the reader and the tag, but it does not penetrate solid walls and the receiver has to be located in the same room. It is not subject to electromagnetic interferences and does not create such interferences. Tags are battery powered. This technology has been tested and deployed in hospital environment. [100]

Hewlett Packard (HP)'s experimental "Memory Spot" chip (see Figure below) suggests that technological innovation is likely to force us to review today's concepts and definitions of RFID. About the size of a grain of rice, the "Memory Spot" chip can broadcast data at 10 megabit per second, has a built-in antenna and a storage capacity ranging from 32 kilobytes to 512 kilobytes. It uses microwaves (2.45 GHz) but needs to be positioned very close (1 mm) to the reader for the communication to take place. It has read/write capacity and enables cryptography. These chips, which could reach the market within two or three years, can store large amounts of text, sound, pictures and even video clips. For example, they could enable adding a video clip to a postcard, a medical record to a patient wristband, "adding voice instructions to a consumer medicine bottle, storing a document electronically on the printed copy […] attaching a copy of the manual to every piece of equipment so you always know where to find it". As noted by a journalist, with this type of memory capacity, processing and networking capability, memory spots "will function like mini-computers rather than like passive tags". The memory spot prototype demonstrates that the differences between a tag and a computer are decreasing. (Kanellos, 2006; Krill, 2006; HP, 2006; Taub; 2006)

Figure 9. HP Memory Spot

"Attach a chip to the prints of photographs and add music, commentary or ambient sound"

Source : HP Memory Spot

100. "Testing Ultrasound to Track, Monitor Patients", Mary Catherine O'Connor , RFID Journal, 15 March 2006, www.rfidjournal.com/article/articleprint/2199/-1/1/. See www.sonitor.com.

ANNEX III. SECURITY EXPLOITS (disponible en anglais uniquement)

This annex provides a list of security exploits found in the literature.

Lack of basic security:

- Of the ten different types of RFID systems used in hotels, a hacker found that none used encryption. He also found out that many systems which use encryption failed to change the default key set by the manufacturer, or that they used sample keys provided in user manuals sent with the cards. He created a database of such sample keys to conduct dictionary attacks and was able to open about 75 % of all the cards collected. In addition, he created a master key card to open every room in a hotel, office or other facility. He cloned Philips Electronics' Mifare, the most commonly used key-access system. To create a master key he simply needed two or three key cards for different rooms to determine the structure of the cards. (Zetter, 2006)
- The same hacker was also able to crash RFID-enabled alarm systems designed to sound when an intruder breaks a window or door to gain entry. Such systems require workers to pass an RFID card over a reader to turn the system on and off. The hacker found that by manipulating data on the RFID chip, he could crash the system, opening the way for a thief to break into the building through a window or door.
- According to a Japanese newspaper, data about the passenger's latest entry and exit stations stored in the Suica card[101] can be read by basic RFID readers, such as the one embedded in Sony Clié PDA. The journalist claimed that the possibility to read such information at a distance could facilitate stalking. [102] Similarly, a British newspaper reports that access to data corresponding to "every journey taken in the past 10 weeks" in the London Oyster card is possible by keying in its serial number on a website or taking the card to a reader machine in the underground. The journalist reports that this information can be used in divorce procedures.[103]
- The implantable RFID "Verichip" was cloned in less than 10 minutes by a 23 year old Canadian hardware developer for the purpose of an article in the magazine *Wired*. The tag, implanted in the journalist's arm for the purpose of the article, featured no security at all (Newitz, 2006).
- According to the same *Wired* article, 5 millions of RFID tags have been sold to libraries in an unlocked state to "make it easier for libraries to change the data". Unfortunately, these tags also enable anyone with the appropriate software and hardware to write on the tag as well.

---

101 10 million Suica cards were issued between 2001 and 2004. See www.jreast.co.jp/e/press/20041003/.

102. http://kodansha.cplaza.ne.jp/digital/it/2003_08_27/content.html, article in Japanese.

103. "How an Oyster Card can Ruin your Marriage", The Independent on Sunday, reproduced at www.theabi.org.uk/press/p0602.htm

Insufficient security

- Texas Instrument "Digital Signature Transponder" which secures over 6 million tags ExxonMobil SpeedPass payment transponders and over 150 million automobile ignition keys has been cloned in 2005 by RSA Laboratories using inexpensive off-the-shelf equipment. The team purchased gasoline at an ExxonMobil station multiple times with the cloned pass and spoofed a Ford car immobiliser system (Bono et al., 2006).
- Electronic passports have been under intense scrutiny since their announcement:
  - A German computer security consultant successfully cloned an ICAO compliant RFID electronic passport using an off the shelve RFID reader and software tools (Zetter, 2006).
  - The same consultant conducted a successful attack against RFID passport readers by cloning a passport chip and modifying the image it contained to exploit a known vulnerability in the software library used to decode the image. (Zetter, 2007)
  - A shielding solution planned for the US e-passport that is aimed at preventing remote reading of the passport when the document is not open was found to allow such reading when the booklet is only a half inch open, such as in a pocket or handbag (Flexilis, 2006). The prototype Dutch RFID passport, featuring the Basic Access Control[104] protection, was cracked by security specialists and they claimed that the attack was possible at a 10m range (Lettice, 2006).
- Expensive cars secured by software methods can be stolen using a simple laptop: "The expert gang suspected of stealing two of David Beckham's BMW X5 SUVs in the last six months did [used] software programs on a laptop to wirelessly break into the car's computer, open the doors, and start the engine" (Leftlane News, 2006).

104. Basic Access Control is an optional feature which unlocks the RFID chip only if the passport's machine readable zone has been read by an optical reader, and encrypts the data exchanged using information derived from the content of that zone.

ANNEX IV. THE ELECTRONIC PRODUCT CODE (EPC) NUMBER STRUCTURE (disponible en anglais uniquement)

01	0000A89	00016F	000247DC0
Header 8 bits	EPC manager 28 bits	Object class 24 bits	Serial number 36 bits

"The EPC is a generic, universal numbering scheme for physical objects, similar in scope to the barcode numbering scheme (UPC). However, […] the EPC has the capability to identify every single, individual product item. […] The manager number identifies the company involved in the production of the item (manufacturer) and the object class defined the product itself. The Serial number is unique (within the scope of the other numbers) for an individual product entity. The 96-bit code can thus provide unique identifiers for 268 millions companies (2^{28}). Each manufacturer can have 16 million (2^{24}) object classes and 68 billion serial number (2^{36}) in each class."

(*Source*: JISC Technology and Standards Watch, May 2006)

"The structured hierarchy of EPC numbers nests identification information onto distinct segments of the EPC string (*i.e.*, the EPC Manager Number segment identifies who, the Object Class segment identifies what, and the Serial Number segment identifies which). As a result, each segment conveys a different level of information about the item to which the EPC is attached."

Source: EPCglobal, EPCglobal Position Paper, Implementation of the EPCglobal Network Root ONS, Release 1, 2005

ANNEX V. EXAMPLES OF PRIVACY REFERENCES (disponible en anglais uniquement)

A large number of resources related to RFID privacy are available. This list reflects only a subset of the documents that the Secretariat has gathered to date. It only contains documents with a policy guidance dimension, issued either by governmental bodies or by organisations with a public policy focus or international orientation. It is complementary to the bibliography.

A. RFID in general

DPAs and other official bodies

International
25th International Conference of Data Protection and Privacy Commissioners – Sidney – "Resolution on Radio-Frequency Identification", 20 November 2003
www.cnil.fr/fileadmin/documents/uk/Resolution_RFID-VA.pdf

Regional
Article 29 Working Party – "Working Document on Data Protection Issues Related to RFID Technology", 19 January 2005
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

European Commission's RFID consultation website
www.rfidconsultation.eu

Canada
Ontario - Information and Privacy Commissioner
"Privacy Guidelines for RFID Information Systems", June 2006
www.ipc.on.ca/images/Resources/up-rfidgdlines.pdf
"Practical Tips for Implementing RFID Privacy Guidelines", June 2006
www.ipc.on.ca/images/Resources/up-rfidtips.pdf

Germany
Resolution of the 72nd German Data Protection Conference of the Federation and the Länder held in Naumburg from 26 to 27 October 2006, "Binding rules for the use of RFID technologies"

Federal Commissioner for Data Protection and Freedom of Information
"RFID Radio Chips for Every Occasion"
www.bfdi.bund.de/cln_029/nn_672292/EN/Topics/technologicalDataProtection/Artikel/RFID_E2_80_93RadioTagsForAllOccasions.html

Italy
GarantePrivacy
"Smart (RFID) Tags: Safeguards Applying to Their Use", 9 March 2005
www.garanteprivacy.it/garante/doc.jsp?ID=1121107

France
CNIL
Address by Philippe Lemoine relating to Radio-Tags (RFIDs), 2003
www.cnil.fr/fileadmin/documents/uk/CNIL-lemoine-RFID_102003_VA.pdf

Japan
"Guidelines for Privacy Protection with Regard to RFID tags", 8 July 2004
www.rfidconsultation.eu/docs/ficheiros/JP_RFID_PrivacyGLsRev_METI.pdf

Korea
"RFID Privacy Protection Guideline" (unofficial translation)
www.worldlii.org/int/other/PrivLRes/2005/3.html

Netherlands
Minister of Economic Affairs,
"RFID in the Netherlands", 25 September 2006 (document transmitted to the Parliament)

UK
ICO – "Data Protection technical guidance", 9 August 2006
www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/radio_frequency_indentification_tech_guidance.pdf
www.rfidconsultation.eu/docs/ficheiros/RFID_Ofcom_statement.pdf

US
« The use of RFID for Human Identification» (Draft Report),
Department of Homeland Security
www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf

"RFID applications and implications for consumers", March 2005
Federal Trade Commission
www.ftc.gov/os/2005/03/050308rfidrpt.pdf

Business

Enterprise Privacy Group - A privacy code of conduct for RFID technologies – 3 May 2005
www.rfidconsultation.eu/docs/ficheiros/EPG_RFID_Privacy_Code_of_Conduct.pdf

EPCglobal – Guidelines on EPC for consumer products
www.epcglobalinc.org/public/ppsc_guide/

EPCglobal - "EPCglobal Submission to the Article 29 Working Party in Response to its Working Document 10107/05 WP 105 of January 19, 2005 on Data protection issues related to RFID Technology".
http://ec.europa.eu/justice_home/fsj/privacy/docs/rfid/epcglobal_en.pdf

EPCglobal- "EPCglobal Response to the EU RFID Online Consultation"
www.rfidconsultation.eu/docs/ficheiros/EPCglobal_Response_to_EU_RFID_Online_Consultation.pd

EuroCommerce Position paper
www.rfidconsultation.eu/docs/ficheiros/EuroCommerce_Position_on_RFID.pdf

International Chamber of Commerce - "ICC principles for responsible deployment and operation of electronic product codes"
www.iccwbo.org/home/statements_rules/statements/2005/EPC_principles.asp

UK RFID Council - UK Code of practice for the use of RFID in retail outlets
www.rfidconsultation.eu/docs/ficheiros/code_release_1_0_120406__logos.pdf

Civil Society

Center for Democracy and Technology Working Group on RFID: "Privacy Best Practices for Deployment of RFID Technology"
www.cdt.org/privacy/20060501rfid-best-practices.php

EPIC Guidelines on Commercial Use of RFID Technology
www.epic.org/privacy/rfid/rfid_gdlnes-070904.pdf

Privacy Rights Clearinghouse - "RFID position statement of Consumer, Privacy and civil Liberties Organisations"
www.privacyrights.org/ar/RFIDposition.htm

Trans Atlantic Consumer Dialogue – "Resolution on Radio Frequency Identification", April 2005.
www.tacd.org/docs/?id=274

B. RFID in specific areas

Libraries
"Privacy and Confidentiality Guidelines" (American Library Association)
www.ala.org/ala/oif/statementspols/otherpolicies/rfidinlibraries.pdf

Ontario Information and Privacy Commissioner
"Guidelines for using RFID tags in Ontario Public Libraries"
www.ipc.on.ca/images/Resources/rfid-lib.pdf

Drugs & healthcare:
RFID Feasibility Studies and Pilot Programs for Drugs / Compliance policy guide
www.fda.gov/oc/initiatives/counterfeit/rfid_cpg.html

Workplace:
UNI "RFID in the Workplace – UNI code of Good Practice"
www.union-network.org/uniindep.nsf/2702f48e48fad7dac125718e0034fd79/$FILE/RFIDdraft.pdf

"Pervasive Computing: Trends and Impacts", 2006
www.bsi.de/literat/studien/percenta/Percenta_eacc.pdf

BIBLIOGRAPHIE

Aeroscout (2005), *Port of Venice Deploys Aeroscout Visibility System for Vehicle Inventory Management*, Aeroscout, San Mateo, www.aeroscout.com/viewItem.asp?type=press&itemId=23.

AIM (n.d.), *RFID Standards*, site Internet d'AIM. www.aimglobal.org/standards/rfidstds/RFIDStandard.asp, consulté le 8 juin 2007.

AIM (2001), *Shrouds of time. The history of RFID,* AIM, Pittsburg. www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf

AIM Frequency Forum (2000), *Draft paper on the Characteristics of RFID systems*, Version 1.0. www.aimglobal.org/technologies/rfid/resources/RFIDCharacteristics.pdf

Alberganti, Michel (2007), *Sous l'oeil des puces*, Actes Sud, Paris.

Albrecht, Katherine et McIntyre, Liz (2005), *Spychips*, Plume.

ANEC/BEUC (2007), *Consumers' scenarios for a RFID policy - Joint ANEC/BEUC Comments on the Communication on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework COM(2007) 96*, Bruxelles, www.anec.org/attachments/ANEC-ICT-2007-G-059.pdf.

Article 29 Working Party (2005), *Working Document on data protection issues related to RFID technologies*.

Article 29 Working Party (2007), *Opinion 4/2007 on the concept of personal data*.

Avoine, Gildas (n.d.), *RFID Security and Privacy*, site Internet : http://lasecwww.epfl.ch/~gavoine/rfid/.

Australian Government, Department of Communications, Information Technologies and the Arts (2006), *Getting the most out of RFID. A starting Guide to Radio Frequency Identification for SMEs*, www.dcita.gov.au/__data/assets/pdf_file/41249/Getting_the_most_out_of_RFID.pdf

Bacheldor, Beth (2006), *Hospital Tries ZigBee to Track Patients*, *RFID Journal*, 21 juillet 2006, www.rfidjournal.com/article/articleview/2509/.

BMWi (German Federal Ministry of Economics and Technology) (2007), *European Policy Outlook RFID*, Berlin, www.nextgenerationmedia.de/Nextgenerationmedia/Redaktion/en/PDF/Final_20version_20European_20Policy_20Outlook_20RFID,property=pdf,bereich=nextgenerationmedia,sprache=en,rwb=true.pdf.

Bono, S., Green, M., Stubblefield, A., Juels, A., Rubin, A. et Szydlo, M. (2006), *Security Analysis of a Cryptographically-Enabled RFID Device*, dans "Proceedings of the 14th Usenix Security Symposium", p. 1-16. https://db.usenix.org/events/sec05/tech/bono.html.

BRIDGE (Building Radio Frequency Identification for the Global Environment) (2007), *Security Analysis Report*, BRIDGE, www.bridge-project.eu/data/File/BRIDGE%20WP04%20Security%20Analysis%20Report.pdf

BSI (Bundesamt für Sicherheit in der Informationstechnik) (2005), *Security aspects and Prospective Applications of RFID Systems,* BSI, Bonn, www.bsi.bund.de/fachthem/rfid/RIKCHA_englisch_Layout.pdf.

Cap Gemini (2005a), *RFID and Consumers. What European Consumers Think About Radio Frequency Identification and the Implications for Business*, Cap Gemini, Paris. www.capgemini.com/news/2005/Capgemini_European_RFID_report.pdf.

Cap Gemini (2005b), *Consumer education is key to boosting awareness and overcoming misconceptions about RFID*, Cap Gemini, Paris, www.capgemini.com/news/2005/0209RFID.shtml.

Cardullo, Mario, *Genesis of the Versatile RFID Tag*, *RFID Journal*, www.rfidjournal.com/article/articleview/392/1/2/.

Cavoukian, Ann (2004), *Tag, you're it: Privacy Implications of Radio Frequency Identification (RFID) Technology*, Information and Privacy Commissioner/Ontario, Toronto, www.ipc.on.ca/images/Resources/up-rfid.pdf.

Cavoukian, Ann (2006), Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines), Information and Privacy Commissioner/Ontario, Toronto, www.ipc.on.ca/images/Resources/up-rfidgdlines.pdf.

CDT (Center for Democracy and Technology) (2006), *CDT Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology*, www.cdt.org/privacy/20060501rfid-best-practices.php.

CIPL (Center for Information Policy Leadership) (2007), *RFID Transparency Symbol Project*, Hunton & Williams, www.hunton.com/files/tbl_s47Details/FileUpload265/1948/RFID_Two-Pager.pdf.

Collins, Jonathan (2004), "Lost and Found in Legoland", *RFID Journal*, www.rfidjournal.com/article/articleview/921/1/1/.

Commission européenne (2007a), *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions*, Commission européenne, COM(2007)96 final, Bruxelles. http://ec.europa.eu/information_society/policy/rfid/doc/rfid_en.pdf.

Commission européenne (2007b), *The RFID Revolution: Your voice on the Challenges, Opportunities and Threats. Commission Staff Working Document. Results of the Public Online Consultation on Future Radio Frequency Identification Technology Policy*, Commission européenne, SEC(2007)312, http://ec.europa.eu/information_society/policy/rfid/doc/rfidswp_en.pdf.

Commission européenne (2007c), Communication from the Commission to the European Parliament and the Council on the Follow-up of the Work Programme for Better Implementation of the Data Protection Directive, COM(2007)97 final, Commission européenne, Bruxelles. http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_en.pdf

Desmons, Dimitri (2006), *UHF Gen 2 for Item-Level Tagging*, Impinj Inc, www.impinj.com/files/Impinj_ILT_RFID_World.pdf.

DIFRwear site Internet, www.difrwear.com, consulté le 11 juillet 2007.

Dressen, David (2004), "Considerations for RFID selection", *Atmel Applications Journal*, www.atmel.com/dyn/resources/Prod_documents/secrerf_3_04.pdf.

Dutch DPA (Data Protection Authority), R. Beugelsdijk, (2006) RFID, *Promising or Irresponsible? Contribution to the Social Debate about RFID*, Dutch DPA, La Haye, www.dutchdpa.nl/documenten/en_rap_2006_rfid.shtml.

Engels, D.W. et Sarma, S.E. (2005), *Standardization requirements within the RFID class structure*, Auto-ID Labs, MIT, janvier 2005, Cambridge MA, USA. http://autoid.mit.edu/CS/files/11/download.aspx.

EPCglobal (2004a), *The EPCglobal network: Overview of Design, Benefits, & Security*, EPCglobal Inc., www.epcglobalinc.org/news/EPCglobal_Network_Overview_10072004.pdf.

EPCglobal (2004b), *EPCglobal Object Name Service (ONS) 1.0*, EPCglobal Inc., www.epcglobalinc.org/EPCglobal_ONS_1.0.pdf.

EPCglobal (2005a), *Submission to the Article 29 Working Party in Response to its Working Document 10107/05, WP 105 of January 19, 2005 on Data Protection issues related to RFID Technology*, EPCglobal Inc., http://ec.europa.eu/justice_home/fsj/privacy/docs/rfid/epcglobal_en.pdf.

EPCglobal (2005b), *The EPCglobal Architecture Framework*, EPCglobal Inc., www.epcglobalinc.org/standards/Final-epcglobal-arch-20050701.pdf.

EPCglobal (2005c), *EPC Radio-Frequency Identity Protocols Class 1 Generation 2UHF RFID. Protocol for communications at 860 Mhz -960 Mhz. Version 1.0.9*, EPCglobal Inc., www.epcglobalinc.org/standards/Class_1_Generation_2_UHF_Air_Interface_Protocol_Standard_Version_1.0.9.pdf.

EPCglobal (2005d), *Guidelines on EPC for Consumer Products*, EPCglobal Inc., www.epcglobalinc.org/public/ppsc_guide/.

EPCglobal (2007), *Position Paper on the Definition of Personal Data in the Context of RFID/EPC Technology Applications*, EPCglobal Inc..

EPIC (Electronic Privacy Information Center) (n.d.), *RFID Privacy Page*, www.epic.org/privacy/rfid/.

Fabian B., Olivier, G. et Spiekermann, S (2005), *Security Analysis of the Object Name Service (ONS) for RFID,* International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, SecPerU'05, IEEE, http://lasecwww.epfl.ch/~gavoine/download/papers/FabianGS-2005-sptpuc.pdf.

Finkenzeller, Klaus (2003), *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd Edition, Wiley & Sons.

Finkenzeller, Klaus (2006), *Standardization of RFID*, RFID Handbook, site Internet, www.rfid-handbook.de/rfid/standardization.html.

Flexilis (2006), *RFID E-Passport Vulnerability*, Flexilis, www.flexilis.com/epassport.php.

Floerkemeir, C., Schneider, R., Langheinrich, M. (2005), *Scanning with a purpose – Supporting Fair Information Principles in RFID Protocols.,* 2nd International Symposium on Ubiquitous Computing Systems, UCS 2004, 8-9 novembre 2004, Tokyo, Japon.

Garfinkel, Simson et Holtzman, H. (2005), *Understanding RFID Technology*, in Garfinkel Simson. and Rosenberg Beth, "RFID Applications, Security, and Privacy", Addison-Wesley Professional, Boston.

Gartner (2005), *Gartner Says Worldwide RFID Spending to Surpass $3 Billion in 2010*, Gartner, Stamford, www.gartner.com/press_releases/asset_141469_11.html.

HP (Hewlett-Packard) (2006), *HP Unveils Revolutionary Wireless Chip that Links the Digital and Physical Worlds*, HP, www.hp.com/hpinfo/newsroom/press/2006/060717a.html.

Hitachi (2003), *Hitachi to Sell Inexpensive μ-Chip Inlets at Fraction of the Cost of Existing Inlets, Open the Way to Use in Various Applications*, communiqué de presse de Hitachi, www.hitachi.com/New/cnews/031204.html

Holland, Colin (2007), *Europe approves UWB regulations*, EETimes Europe, http://eetimes.eu/showArticle.jhtml?articleID=197800214.

IDTechEx (2005), *Active RFID - A profitable business*, IDTechEx, www.idtechex.com/products/en/articles/00000396.asp.

IDTechEx (2006a), *RFID Market $2.71Bn in 2006 to $12.35Bn in 2010 - RFID Forecasts 2006 to 2016: The latest research from IDTechEx*, IDTechEx, www.idtechex.com/products/en/articles/00000409.asp.

IDTechEx and Das, Raghu (2006b), *Chipless RFID – The End Game*, IDTechEx, www.idtechex.com/products/en/articles/00000435.asp.

ICC (International Chamber of Commerce), EICTA (European Information, Communications and Consumer Electronics Technology Industry Association), ICRT (International Communications Round Table) et JBCE (Japan Business Council in Europe) (2005), *European Commission DG Internal Market – Art.29 Data Protection Working Party Working Document on data protection issues related to RFID technology – WP 105/ Response by ICC, EICTA, ICRT and JBCE to the public consultation,* ICC, EICTA, ICRT and JBCE, http://ec.europa.eu/justice_home/fsj/privacy/docs/rfid/eicta_en.pdf.

ICAO (International Civil Aviation Organisation) (2004), *Annex I - Use of Contactless Integrated Circuits in Machine Readable Travel Document. Version 4.0*, ICAO, Montréal. http://mrtd.icao.int/component/option,com_remository/Itemid,32/func,fileinfo/id,2/.

Juels, A., Rivest, R. and Szydlo, M. (2003), "The blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", in V. Atluri, ed. 8th ACM *Conference on Computer and Communications Security*, pp. 103-111. ACM Press.

Juels, A. (2005a), *RFID Security and Privacy: A Research Survey*, RSA Laboratories, www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf

Juels, A. (2005b), *RFID Privacy: a technical primer for the non-technical reader*, RSA Laboratories, www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/rfid_privacy/DePaul23Feb05Draft.pdf.

Kanellos, Michael (2006), *HP's Memory Spot puts video, audio into photos*, CNET News.com, http://news.zdnet.com/2100-1040_22-6094586.html.

Krill, Paul (2006), *HP hails Memory Spot chips to extent content access*, Infoworld www.infoworld.com/article/06/07/17/HNmemoryspotpalo_1.html.

Lace, Susan (2004), *Calling in the chips? Findings from the first summit exploring the future of RFID technology in retail*, National Consumer Council, London, www.ncc.org.uk/technology/calling_in_chips.pdf.

Lahiri, Sandip (2005), "RFID: A Technology Overview", *RFID Sourcebook*, IBM Press.

Langheinrich, Marc, (2007), "RFID and Privacy", dans Milan Petkovic, Willem Jonker (Eds.), *Security, Privacy, and Trust in Modern Data Management*, Springer, Berlin Heidelberg New York, www.vs.inf.ethz.ch/publ/papers/langhein2006rfidprivacy.pdf

Le Pallec, Sophie (2005), *La convergence des identifiants numériques,* CGEMP, Université Paris Dauphine, http://2005.jres.org/resume/70.pdf.

Leftnane News (2006), *Gone in 20 minutes : using laptops to steal cars*, Leftlane news, www.leftlanenews.com/2006/05/03/gone-in-20-minutes-using-laptops-to-steal-cars/.

Lettice, John (2006), *Face and Fingerprints Swiped in Dutch Biometric Passport Crack*, The Register, www.theregister.co.uk/2006/01/30/dutch_biometric_passport_crack/.

Malykhina, Elena (2005), "Active RFID Meets Wi-Fi to Ease Asset Tracking", *InformationWeek*. www.informationweek.com/story/showArticle.jhtml?articleID=57701494.

Merritt, Rick (2006), *Cellphone could crack RFID tags, says cryptographer*, EEtimes online, www.eetimes.com/showArticle.jhtml?articleID=180201688.

Moore Bert (2006), *RFID: A Plethora of Standards*, AIM, Warrendale, Pennsylvania. www.aimglobal.org/members/news/templates/aiminsights.asp?articleid=1615&zoneid=43.

Moskowitz, P., Lauris, A. et Morris, S. (2006), *Privacy-Enhancing Radio Frequency Identification Tag: Implementation of the Clipped Tag*, RFID Journal Live, www-03.ibm.com/solutions/businesssolutions/sensors/doc/content/bin/Clipped_Tag_White_Paper.pdf?g_type=hpfeat.

National Research Council, Committee on Radio Frequency Identification Technologies, (2004), *Radio Frequency Identification Technologies: a Workshop Summary*, National Research Council, Washington.

Newitz, Analee (2006), "The RFID Hacking Underground", *Wired*, www.wired.com/wired/archive/14.05/rfid.html

NIST (National Institute of Standards and Technology) (2007), *Guidelines for Securing Radio Frequency Identification (RFID) Systems*, Special publication 800-98, NIST, Gaithersburg, http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf.

O'Connor, Mary Catherine (2006), "EPC Tags Subject to Phone Attacks", *RFID Journal*, www.rfidjournal.com/article/articleview/2167/1/1/.

O'Connor, Mary Catherine (2007), "Building Automation Will Drive ZigBee Adoption", *RFID Journal*, www.rfidjournal.com/article/articleview/2943/1/1/.

OECD (1980), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris.

OECD (1999), *OECD Guidelines for Consumer Protection in the Context of Electronic Commerce*, OECD, Paris.

OECD (2002), *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, OECD, Paris.

OECD (2003), *Privacy Online. OECD Guidance on Policy and Practice*, OECD, Paris.

OECD (2005), *Biometric Based Technologies*, OECD, Paris.

OECD (2006a), *Radio Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations*, OECD, Paris.

OECD (2006b), *Making Privacy Notices Simple: an OECD Report and Recommendations*, OECD, Paris.

OECD (2006c), *Foresight Forum "Radio Frequency Identification (RFID) Applications and Public Policy Considerations": Proceedings*, OECD, Paris.

OECD (2007a), *Analytical report on Malicious Software*, DSTI/ICCP/REG(2007)5/FINAL, OECD, Paris.

OECD (2007b), *RFID: Challenges and Benefits in Technology Implementation*, DSTI/ICCP/IE(2007)6/FINAL, OECD, Paris.

OECD (2007c), *RFID: Outline of Further Work*, document de travail du secrétariat, OECD, Paris.

Oehlmann, H. (2006), ISO RFID application standards published in 2006, Odette.se, www.odette.se/files/seminariet%202006-04-11/Oehlmann.pdf.

Ohkubo M., Suzuki K., Kinoshita S., (2003), *Cryptographic Approach to "Privacy-Friendly" Tags*, rapport presenté à : RFID Privacy Workshop @ MIT 2003, www.rfidprivacy.us/2003/papers/ohkubo.pdf.

Oren, Y. et Shamir, A. (n.d.), *Power analysis of RFID*, site Internet de Yossi Oren, www.wisdom.weizmann.ac.il/~yossio/rfid/.

Parlement Européen (2007), *RFID and Identity Management in Everyday Life. Striking the balance between convenience, choice and control*, IPOL/A/STOA/2006-22, PE 383.219, www.europarl.europa.eu/stoa/publications/studies/stoa182_en.pdf.

Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, Juan. and Arturo Ribagorda (2006), *RFID Systems : A Survey on Security Threats and Proposed Solutions*, http://lasecwww.epfl.ch/~gavoine/download/papers/PerisHER-2006-pwc.pdf.

Pradelles, Daniel, *RFID & Privacy. Perception of Reality?*, presentation faite à l'atelier "European Commission Consultation on RFID" du 17 juin 2006, www.rfidconsultation.eu/docs/ficheiros/Daniel_Pradelles.pdf.

QED Systems (2002), *Part 1: Active and Passive RFID: Two Distinct, But Complementary, Technologies for Real-Time Supply Chain Visibility*, QED Systems, www.autoid.org/2002_Documents/sc31_wg4/docs_501-520/520_18000-7_WhitePaper.pdf.

Rees, Richard (2004), *ISO Supply chain RFID Standards*, presentation faite à "RFID and Telecommunication Services Workshop", ETSI, http://portal.etsi.org/docbox/ERM/open/RFIDWorkshop/RFID_20%20Richard%20Rees_BSI.pdf.

Resolution of the 72nd German Data Protection Conference of the Federation and the Länder, Naumburg du 26 au 27 octobre 2006 (2006), *Binding Rules for the Use of RFID Technologies*.

RFID Journal (n.d.), "Frequently asked question. The cost of RFID equipment", *RFID Journal*, www.rfidjournal.com/faq/20/86, consulté le 23 mai 2007

RFID Journal (2003), "Military's RFID Alternative: IPv6", *RFID Journal*, www.rfidjournal.com/article/articleprint/609/-1/1/.

Rieback, M., Crispo, B. et Tanenbaum A. (n.d.), Is your cat infected with a Computer Virus?, Vrije Universiteit, Amsterdam, www.rfidvirus.org.

Simpson, Richard et St. Arnaud, Bill (2007), *Position paper on "Social and Economic Factors Shaping the Future of the Internet"* pour l'atelier organisé par la NSF et l'OCDE.

Song, Jieun *et al* (2005), *Security Enhanced RFID Middleware system, "*Transactions on Enginering", Computing and Technology, v10, p.79-80.

Stapleton-Gray, Ross (n.d.), *RFID, Surveillance and Privacy: The Sorting Door Project*, Stapleton-Gray & Associates, Inc.

Swedberg, Claire (2006), "Chicago Fire Dept. Tests ZigBee-based RFID System"*, RFID Journal*, www.rfidjournal.com/article/articleview/2717/1/1/.

Taub, Howard et Genuth, Iddo (2006), *HP's Memory Spot Chip is Spot On*, site Internet The Future of Things, www.tfot.info/content/view/79/59/.

UIT (Union internationale des télécommunications) (2005), *The Internet of Things*, ITU, Geneva. http://mrtd.icao.int/component/option,com_remository/Itemid,32/func,fileinfo/id,2/.

US Department of Commerce (2005a), *RFID in 2005: Technology and Industry Perspectives – Workshop Summary – Wednesday 6 April 2005*, US Department of Commerce, Washington DC, www.technology.gov/Events/2005/RFID/0406_Summary.pdf.

US Department of Commerce (2005b), *Radio Frequency Identification. Opportunities and Challenges in Implementation*, Department of Commerce, Washington. www.technology.gov/reports/2005/RFID_April.pdf.

US Department of Homeland Security, Data Privacy & Integrity Advisory Committee (2006), *The Use of RFID for Human Identify Verification*, www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf.

US FTC (Federal Trade commission) (2005), *Radio Frequency Identification: Applications and Implications for Consumers. A workshop report from the staff of the Federal Trade Commission*, FTC, Washington, www.ftc.gov/os/2005/03/050308rfidrpt.pdf.

Vadhia, D. et Gupta, R. (2004), *IPv6 vs EPC,* Silicon Valley World Internet Center. www.worldinternetcenter.com/Pubs/Pubs2004/feb05/IPv6vEPC.pdf

Ward, Matt et Kranenburg, Rob van (2006), *RFID: Frequency, standards, adoption and innovation*, JISC Technology and Standards Watch, London. www.jisc.ac.uk/uploaded_documents/TSW0602.pdf.

Yomogita, Hiroki (2006), *Japan's UWB Finally Takes off with Upcoming UWB-Enabling Devices*, Nikkei Electronics, http://techon.nikkeibp.co.jp/english/NEWS_EN/20060803/119881/.

Zetter, Kim (2006), *Hackers Clone E-Passports*, Wired, www.wired.com/news/technology/1,71521-0.html.

Zetter, Kim (2007), "Scan This Guy's E-Passport and Watch Your System Crash", *Wired*, www.wired.com/politics/security/news/2007/08/epassport.