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

04-Apr-2006

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

DSTI/ICCP(2005)19/FINAL
Non classifié

IDENTIFICATION PAR RADIOFREQUENCE (RFID) : FACTEURS INCITATIFS, ENJEUX ET CONSIDERATIONS

Français - Or. Anglais

JT03206925

AVANT-PROPOS

Le présent document est le fruit d'études visant à fournir une assise et à faciliter les débats au Forum de prospective sur la RFID du comité PIIC de l'OCDE qui s'est tenu à Paris le 5 octobre 2005. Il a été remanié de manière à tenir compte des observations que les États membres ont communiquées au Secrétariat après la réunion.

Le Forum avait pour objectif de favoriser un échange de vues et d'informations entre les gouvernements, les spécialistes des milieux économiques et universitaires, et la société civile ; de recenser les applications actuelles et futures de la technologie RFID et de leurs éventuels avantages économiques et sociaux ; et de mener un débat prospectif sur les questions cruciales que soulève la RFID, notamment en termes d'infrastructure et de normes, ainsi que de sécurité et de confidentialité.

Les actes du Forum sur la RFID, qui a attiré quelque 150 participants, ont été publiés séparément.

Le présent rapport a été présenté au Comité de la politique de l'information, de l'informatique et des communications (PIIC) en septembre 2005. Le Comité PIIC a convenu, lors de sa réunion de septembre 2005, de mettre ce document en diffusion générale par une procédure écrite. Ce rapport a été rédigé par Karine Perset, de la Direction de la Science, de la Technologie et de l'Industrie. Ce rapport est publié sous la responsabilité du Secrétaire général de l'Organisation.

TABLE DES MATIÈRES

Encadrés

RÉSUMÉ ANALYTIQUE

Description de la technologie, de son potentiel économique et des applications

L'identification par radiofréquence (RFID) est une technique d'identification automatique par capteur ; elle comporte trois éléments principaux : des marqueurs RFID (des transpondeurs, généralement des puces miniaturisées) ; des lecteurs RFID (émetteurs-récepteurs) ; et un dispositif de collecte, de distribution et de gestion des données capable d'identifier ou de balayer les informations avec une rapidité et une précision croissantes.

Le déploiement de la technologie RFID s'intensifie dans différents domaines : contrôle des procédés de fabrication, traçage d'objets, réalisation d'opérations financières, perception des péages et paiement aux stations-service, sécurisation de l'accès aux bâtiments et autres applications. L'établissement de normes, les progrès techniques et les prescriptions imposées aux usagers finaux ont encouragé la mise au point d'applications destinées au commerce de détail et à la grande consommation. L'année 2004 a vu l'apparition de nouveaux produits sur le marché et l'introduction prudente de nouvelles offres de services, y compris l'information des consommateurs ; l'année 2005 présente essentiellement les mêmes caractéristiques. La RFID devrait connaître une expansion planétaire, les entreprises et les pouvoirs publics ayant recours à ses applications pour stimuler le commerce mondial et dynamiser l'innovation et la compétitivité. Par comparaison au système de code à barres, la RFID promet à terme des bénéfices, une fiabilité et une rentabilité grandissantes dans des domaines tels que la gestion de la chaîne d'approvisionnement, les transports, la défense, les soins de santé, la sécurité et le contrôle de l'accès, pour n'en citer que quelques-uns. Son utilisation se généralise dans les applications de logistique commerciale, via le marquage au niveau agrégé (marquage de caisses et de palettes par exemple), et devrait produire à terme des gains de productivité au sein de la chaîne d'approvisionnement et de l'économie dans son ensemble.

Bien qu'il soit difficile de prévoir ses utilisations ultérieures, la technologie RFID est prometteuse en ce qu'elle est la première itération de réseaux de capteurs intelligents. On fait de plus en plus appel à la technologie hertzienne pour (inter)connecter des dispositifs performants, plus petits et moins coûteux tels que les puces, les capteurs et les actionneurs en bordure des réseaux IP afin de produire des applications intelligentes et novatrices.

A l'instar de l'Internet ou de la téléphonie mobile, la RFID est une technologie de réseau – plus elle se propage, plus les profits augmentent. Avec le temps, les coûts élevés associés aux premières phases d'adoption de la RFID diminueront et sa diffusion augmentera, ce qui amènera une hausse des profits et stimulera encore son utilisation. A mesure que les coûts diminueront et que la technologie gagnera du terrain, la demande devrait, à en juger par les évaluations actuelles des facteurs favorables, continuer de progresser, passant de dizaines de milliards de marqueurs en 2006 à des centaines de milliards en 2009, voire des billions par la suite. Lorsque le prix des matériels et logiciels de RFID chutera[1], beaucoup d'organismes devraient trouver à cette technologie des applications utiles à leurs opérations structurelles et logistiques. Les analystes[2] ont défini ce qu'ils estiment être trois phases distinctes du déploiement de la RFID dans l'économie : expériences et essais pilotes initiaux (2003-2005), suivis d'une phase de mise en place de l'infrastructure de la chaîne d'approvisionnement (2005-2009) avant d'aboutir à la généralisation du marquage au niveau des articles (2009-2013).

Des facteurs de poids sont susceptibles d'inciter les industries et les pouvoirs publics à développer et à mettre en œuvre des solutions RFID sur l'ensemble des chaînes de valeur. Les bénéfices commerciaux

éventuels et le rendement projeté des investissements sont substantiels du fait que l'industrie et les divers organismes internationaux de normalisation et de spécification (dont l'Organisation internationale de normalisation – ISO) ont élaboré des normes interopérables, que les gros détaillants et les organismes publics ont prescrit le marquage RFID à leurs fournisseurs et qu'un nombre croissant de dispositions juridiques encouragent l'adoption de la RFID dans certains secteurs et domaines d'application. Par conséquent, les coûts de mise en application diminuent rapidement. Plusieurs problèmes persistent toutefois, qui concernent par exemple l'interopérabilité, les coûts actuels de mise en œuvre, et la confidentialité et la sécurité des données pour certaines applications RFID.

De par son caractère transsectoriel et habilitant, la RFID participe du rôle notable que les technologies de l'information et de la communication (TIC) jouent à l'appui de l'innovation, de la croissance économique et du commerce mondial. Dans la perspective d'un avenir où les infrastructures de l'information associées à la RFID seront plus largement diffusées sur les réseaux IP et contribueront davantage à l'économie mondiale, l'OCDE est bien placée pour discuter avec les parties intéressées des meilleurs moyens de créer un climat propice à la croissance et de promouvoir les pratiques optimales pour l'application et l'utilisation de cette technologie.

Questions cruciales pour les responsables publics

La RFID intéresse plusieurs des questions réglementaires et/ou de politique générale mises en évidence ici, à savoir le commerce international, les droits de propriété intellectuelle, les normes, le spectre des fréquences, la sécurité et la confidentialité. Ces problèmes ne se limitent pas aux domaines techniques ou d'action publique, mais pourraient avoir de vastes répercussions au plan social, économique, et au niveau de la sécurité nationale. Il convient donc d'examiner les avantages et les dangers éventuels de la RFID dans le contexte plus large de son incidence sur les économies et la société.

C'est maintenant que les responsables publics, l'industrie et les consommateurs doivent cerner les problèmes prospectifs d'action publique associés à la technologie et aux applications d'identification par radiofréquence, en débattre et examiner les lois existantes et proposées dans ce domaine. Il est indispensable d'appréhender cette technologie, son potentiel et ses conséquences politiques. Pour réaliser le plein potentiel de la RFID, il convient de résoudre les problèmes interdépendants que sont sa diffusion, les normes, les coûts, la confidentialité et la sécurité.

Des travaux de normalisation sont en cours, tant au sein des organismes de normalisation que des consortiums industriels, notamment l'ISO[3] et EPCGlobal[4], ce qui offre l'occasion d'examiner s'il serait avantageux de favoriser l'élaboration concertée de normes mondiales interopérables afin de diminuer les coûts et d'uniformiser les approches à mesure que cette technologie fait irruption sur les marchés. Des difficultés persistent par ailleurs en ce qui concerne l'harmonisation de l'allocation du spectre pour les opérations de RFID, qui varient selon les régions, et l'adoption de protocoles de communication interopérables à l'échelle mondiale.

Du fait que la technologie RFID va migrer vers le marquage au niveau des articles dans les prochaines années et que les pouvoirs publics y feront appel dans divers dispositifs d'identification personnelle, il est capital d'aborder les questions de confidentialité et de sécurité associées à certains de ses systèmes et applications. Ces questions joueront un rôle de poids dans la diffusion de la RFID :

- Des politiques et des innovations techniques guidées par l'industrie et les besoins individuels renforceront le potentiel des TIC et favoriseront l'émergence de technologies nouvelles telles que la RFID. Des interventions publiques bien conçues, comme des directives portant sur l'utilisation appropriée de la RFID, pourraient encourager la mise au point de solutions technologiques qui

tiendraient compte dès les premières phases des questions de protection des données personnelles et de sécurité et intégreraient des solutions intelligentes à cet effet.

- Comme dans le cas de l'Internet, l'information des consommateurs, l'autonomisation des usagers, la transparence et le choix seront vraisemblablement les meilleurs moyens d'assurer la viabilité de la technologie et de produire des bénéfices économiques.
- Il serait éventuellement judicieux d'associer des mécanismes d'autoréglementation, des directives et des solutions techniques à des programmes d'éducation et de sensibilisation.
- Il se peut que certaines applications envisageables de la RFID posent des problèmes particuliers de confidentialité et de sécurité, parce que les usagers ne peuvent voir ni sentir les fréquences radioélectriques et que la plupart des marqueurs RFID n'enregistrent pas à quel moment ou par qui ils ont été lus.
- De nombreuses applications font appel à la RFID : les retombées en matière de protection de la vie privée et des données varient considérablement en fonction du système et de l'application concernés.
- Pour construire en toute sécurité une vaste infrastructure de RFID, il convient d'établir un équilibre entre réglementation et innovation, ce qui permettra de préserver l'innovation dans le secteur privé et d'offrir des avantages aux usagers et, dans le même temps, de recenser les inquiétudes légitimes qui déterminent l'acceptation d'une technologie et d'y répondre.

INTRODUCTION A LA RFID

L'identification par radiofréquence (RFID) est un sous-ensemble évolué d'identification et acquisition automatiques de données (AIDC) du domaine des TIC qui fait appel aux communications par radiofréquence pour autoriser la lecture avec ou sans contact d'informations concernant l'identification d'entités (produits, personnes ou animaux), de lieux, de données temporelles ou de transactions[5].

Bien que la technologie RFID soit apparue dans les années 40 pour l'identification des armes et qu'elle soit déjà amplement utilisée dans plusieurs domaines (péage automatisé, cartes de proximité ou marqueurs antivol), ce n'est que récemment que l'amélioration de la structure des coûts et la diminution de la taille des puces l'ont rendue accessible et applicable à un large éventail d'applications de localisation dans l'ensemble de l'économie, notamment dans les secteurs de l'industrie, du transport, de la sécurité, et des biens et services de consommation.

L'identification par radiofréquence fait intervenir des transpondeurs et des lecteurs. Les transpondeurs, – sous la forme de marqueurs RFID ou de cartes sans contact– sont des circuits électroniques reliés à des antennes qui communiquent des données aux lecteurs par l'intermédiaire d'ondes radio électromagnétiques au moyen d'interfaces d'air, de protocoles de données et de nombreux autres protocoles. Il existe des marqueurs RFID actifs, qui sont munis d'une pile, et passifs. Ces derniers n'ont pas d'alimentation interne ; l'énergie nécessaire à leur fonctionnement provient du champ électromagnétique du lecteur. Les marqueurs passifs ont une portée inférieure à celle des marqueurs actifs, et ont aussi une fonction passive : avec eux, ce sont les lecteurs qui activent, guident et structurent la communication, alors que les marqueurs actifs sont capables d'émettre spontanément.

Il existe de nombreux types de systèmes RFID, qui se distinguent par leur mode précis de fonctionnement et leur performance d'exploitation. De manière générale, les marqueurs RFID bon marché utilisés pour l'identification d'objets de base se composent d'un minuscule circuit électronique relié à de petites antennes capables de transmettre un numéro de série spécifique à un lecteur. Généralement rattachés à des objets matériels, ils permettent de localiser ces derniers. Les lecteurs situés dans un rayon restreint communiquent avec les marqueurs, et en reçoivent des informations qu'ils renvoient pour traitement à un système de TI composé de bases de données, d'intergiciels et de logiciels d'application.

L'expression « marqueur RFID » désignera ici un dispositif généralement attaché à des objets matériels ou à un être vivant. Quand l'un de ces objets s'approche d'un lecteur RFID désigné (de par son propre mouvement ou celui du lecteur), il est possible de lire les données contenues dans le marqueur qui lui est associé. Celles-ci servent à identifier l'objet en question ou à fournir des renseignements à son sujet. Les applications font souvent appel à plusieurs lecteurs RFID, de sorte que les objets marqués peuvent être identifiés à différents endroits, par exemple tout au long d'un flux de production ou d'un flux logistique[6]. Selon les besoins de l'application, les lecteurs transmettent des données, qui concernent par exemple l'identification et la localisation, et peuvent en recevoir d'autres, telles que le prix du produit, sa couleur, la date d'achat et sa date de péremption. Pour cela, la puce se compose d'une mémoire bon marché et d'un circuit radioélectrique miniaturisé.

La technologie RFID revêt d'autres formes : cartes sans contact, utilisées aux fins de contrôle d'accès par exemple ; identification personnelle (passeports et cartes d'identité électroniques), clés numériques (véhicules ou motels), ou cartes de paiement. Il s'agit pour l'essentiel de formes évoluées de la technologie

qui comportent des dispositifs de sécurité supplémentaires (un microprocesseur avec fonctions de traitement et de cryptographie intégrées)[7].

Les marqueurs RFID, autrement dit des puces bon marché dotées d'une fonction de communication sans fil qui attachent des informations à des objets quotidiens et permettent leur identification à distance, peuvent être combinés à des capteurs équipés de fonctions de localisation s'appuyant sur la technologie GPS (système mondial de radiorepérage) ou à la téléphonie mobile, et (inter)connectés à des réseaux IP. De nombreux spécialistes estiment que cette interconnexion constitue l'assise technique d'un environnement dans lequel les objets quotidiens pourront communiquer. Par extension, on voit dans la RFID une composante de « l'Internet des choses » et des réseaux de capteurs répartis.

FACTEURS FAVORABLES ET OBSTACLES A L'ADOPTION DE LA RFID

Les applications de RFID et de cartes intelligentes sans contact sont d'ores et déjà courantes dans plusieurs domaines : procédés de fabrication, gestion du péage autoroutier, badges d'accès aux bâtiments, transports en commun, emprunts bibliothécaires, et lutte contre le vol à l'étalage[8]. Néanmoins, compte tenu de leur coût élevé, des problèmes de fonctionnement et de l'absence de normes reconnues, leur incidence sur la gestion de la chaîne d'approvisionnement a pour l'instant été plus modérée.

Pour tirer parti des avantages qu'offre la RFID, les intervenants du secteur privé et du secteur public doivent bien appréhender les utilisations et la rentabilité potentielles de la technologie et de ses applications, de même que leurs défauts et leurs inconvénients actuels, afin d'élaborer des politiques prospectives.

Éléments favorables à l'adoption de la technologie et avantages

Le déploiement de la RFID est devenu un souci majeur et, dans certains cas, une priorité absolue pour les entreprises œuvrant dans les domaines de la fabrication et de la production, de la logistique, du commerce de détail, des soins de santé, et pour certains organismes publics partout dans le monde. Les marqueurs RFID sont une technologie prometteuse qui permet à ses utilisateurs de recueillir et de distribuer, voire de stocker et d'analyser avec efficacité des informations sur les objets assujettis à un suivi, en particulier dans le cadre des procédures d'inventaire et de localisation, des opérations administratives, du contrôle de la sécurité et de nombreux autres domaines. Le Electronic Product Code™ (EPC), ou code de produit électronique, l'équivalent de la codification GS1 pour les codes à barres appliquées à la RFID, attribue à chaque produit un numéro de série unique et identificateur au niveau de l'article, ce qui offre en outre un moyen de lutter contre la contrefaçon, et pourrait sensiblement diminuer le nombre d'infractions aux droits de propriété intellectuelle (DPI) et assurer la traçabilité des produits pour certaines applications. C'est le consortium influent GS1 qui en est principalement à l'origine.

Les marqueurs RFID peuvent améliorer la commodité, le choix, les prix, la sûreté et la sécurité et permettre d'offrir toute une gamme de nouveaux produits. Outre ses retombées sur la gestion de la chaîne d'approvisionnement, grâce à la réduction du coût des produits et aux gains de temps aux caisses automatisées qu'il autorise, le marquage RFID après-vente au niveau des articles offre d'intéressantes possibilités en termes de services (retour des achats) et d'innovations dans le domaine des appareils électroménagers intelligents - réfrigérateurs, fours et lave-linge dotés de fonctions RFID, ou inventaires personnels de CD-ROM ou de livres – dans le cadre d'un réseau ubiquitaire.

Mettre la RFID au service des consommateurs

Certains des principaux fabricants de téléphones cellulaires se préparent à mettre sur le marché des appareils de communication qui intègrent la technologie RFID et dont ils espèrent qu'ils transformeront la façon dont les consommateurs achètent des produits, des services et utilisent leurs cartes de crédit. La technologie NFC (communication en champ proche) utilise des transmissions RFID de courte portée qui assurent des communications faciles et sécurisées entre différents appareils. Cela signifie par exemple que pour acheter des billets de concert, réserver une chambre d'hôtel et effectuer d'autres types de réservations, et régler ces opérations par carte de crédit au moyen d'informations stockées dans le téléphone portatif, il suffira de tenir celui-ci à proximité (moins de 20 centimètres) d'une affiche ou d'un panneau publicitaire [9].

A moyen terme, la RFID pourrait également servir à créer des produits intelligents qui communiquent avec des appareils ménagers intelligents. Merloni Elettrodomestici, un fabricant italien d'électroménager, a été le premier à intégrer la RFID à ses appareils[10]. La société a mis au point un lave-linge, un réfrigérateur et un four intelligents. Lorsque les vêtements sont placés dans le lave-linge, un lecteur RFID intégré lit leurs étiquettes (s'ils sont dotés de marqueurs RFID) et les lave en fonction des instructions qu'elles contiennent. Le réfrigérateur est conçu pour surveiller la date de péremption de chaque produit et afficher les informations relatives à sa valeur nutritionnelle ; il peut même fournir des recettes de plats réalisables au moyen des ingrédients qu'il contient. Le four, pour sa part, détermine automatiquement le temps de cuisson et les températures à partir des instructions inscrites sur les étiquettes.

Unilever, le fabricant anglo-néerlandais de biens de consommation, a créé le prototype de la cuisine du futur où des lecteurs RFID installés dans les placards lisent toutes les étiquettes des produits rangés sur les étagères. Un programme informatique détermine quels produits peuvent être cuisinés avec ce qui se trouve dans la cuisine [11].

Facteurs commerciaux favorables à l'utilisation des marqueurs RFID

Facteurs commerciaux favorables à l'utilisation de marqueurs RFID dans les applications en « boucle fermée »

Si la chaîne d'approvisionnement demeure aujourd'hui le moteur essentiel du développement de la RFID, les entreprises envisagent de recourir à cette technologie dans des applications plus spécialisées qui leur permettraient d'obtenir rapidement des retours supérieurs sur leurs investissements. Alors que les chaînes d'approvisionnement se caractérisent généralement par leur ampleur et leur hétérogénéité (boucle ouverte), les applications spécifiques, localisées (boucle fermée) peuvent apporter d'autres justifications aux investissements dans la RFID. Il s'agit des applications d'entreposage, de détection de vol, de localisation et de traçage d'actifs, de localisation des personnes, de suivi des inventaires en cours, de réparation et de maintenance, et de suivi de bagages. Les applications auxquelles les entreprises intègrent actuellement cette technologie fonctionnent en général en boucle fermée ; leurs résultats sont mesurables à court terme et leur déploiement peut être effectué par étapes.

Facteurs commerciaux favorables dans les chaînes d'approvisionnement en « boucle ouverte »

Les marqueurs RFID devraient (et, dans certains cas, ont déjà prouvé leur potentiel à cet égard) produire des gains de productivité dans la gestion de la chaîne d'approvisionnement et favoriser une meilleure allocation des actifs grâce à l'accélération des flux d'information et à l'amélioration de la gestion des stocks.

- **Rapidité et précision :** en termes de rapidité, la RFID est plus prometteuse que les codes-barres ; en effet, ses applications pourraient faire moins appel à l'intervention humaine dans la mesure où des applications intergicielles appropriées et des applications logicielles et matérielles à haute capacité de gestion des données seront disponibles et mises en place. Ainsi, il existe plusieurs fonctions d'entreposage où les marqueurs RFID peuvent instantanément fournir des informations détaillées sur le nombre exact d'articles, que ce soit à la station d'accueil ou dans le stock de l'entrepôt. Il convient de noter que les résultats dépendent en grande partie du type de matériel faisant l'objet du suivi et de l'environnement de mise en œuvre ; il est donc nécessaire de procéder à des expériences.

- **Transparence :** Les participants à la chaîne d'approvisionnement peuvent tirer profit de la capacité des marqueurs RFID à renfermer davantage d'informations sur un produit que la technologie à codes à barres existante : numéros de lots, numéros de série, dates de péremption et autres renseignements pertinents.

- **Ajout d'informations :** Certains marqueurs RFID sont inscriptibles et, à mesure qu'ils passent par les différentes phases du cycle de vie du produit, on peut y ajouter des informations, concernant la traçabilité alimentaire par exemple. Ils peuvent également être équipés de capteurs permettant de détecter la température, l'humidité, etc.

Les fonctions de la RFID citées ci-dessus devraient créer des gains de productivité grâce à l'automatisation des opérations de réception, d'expédition, de reconstitution des stocks, de contrôle de la qualité, de suivi des lots (rappels ou péremption) et autres opérations de la chaîne d'approvisionnement, et permettre par ailleurs une meilleure allocation des actifs grâce à des taux de remplissage supérieurs, à la diminution des stocks, à la réduction du nombre de vols, et à une meilleure gestion des produits au regard de leur date de péremption. On estime que l'utilisation de la RFID permettrait à tous les participants à la chaîne d'approvisionnement, et non aux seuls détaillants ou distributeurs, de réaliser des bénéfices. On pense également que la RFID influencera d'autres aspects des opérations commerciales, notamment les ventes et la commercialisation.

Plusieurs études ont conclu que la RFID est susceptible de réduire de 3 % à 5 % les coûts associés à la chaîne d'approvisionnement, et d'augmenter de 2 % à 7 % le montant des recettes[12]. Les détaillants, en particulier, en tireraient profit car elle permet de diminuer les ruptures de stock (dont le taux s'établit à 9 % en moyenne à l'échelle mondiale[13], et qui se traduisent par des pertes de ventes substantielles pour les détaillants) et le nombre de vols (qui leur coûtent en moyenne 1,7 % des ventes brutes[14]).

Prescriptions particulières en matière de marquage RFID imposées aux fournisseurs par les détaillants ou les pouvoirs publics

Le fait que les grands détaillants et les organismes publics, dont le Ministère américain de la défense et Wal-Mart, aient exigé de leurs principaux fournisseurs qu'ils utilisent des marqueurs RFID, conjugué aux progrès techniques et à la baisse des coûts, a favorisé l'adoption de cette technologie. Beaucoup de fabricants citent cette consigne de leurs clients comme la raison première au déploiement de la RFID en 2005[15].

- **Secteur du détail** : En juin 2004, Wal-Mart a imposé à ses cent principaux fournisseurs d'apposer à compter du début de 2005 des marqueurs sur les palettes et caisses destinées à un groupe de supermarchés situés dans le nord du Texas, et à compter du début de 2006 à ses 200 fournisseurs suivants. Les marqueurs lui permettent de tracer les produits à partir du moment où ils quittent l'entrepôt du fournisseur jusqu'à celui où ils sont rangés dans les réserves et sur les étagères de ses magasins, en passant par ses centres d'entreposage et de distribution. Pour Wal-Mart, qui a été parmi les premiers à adopter l'étiquetage à grande échelle au niveau des articles, il s'agit avant tout d'établir un lien fonctionnel entre les phases initiales de livraison et de commercialisation et les phases finales de distribution et d'achat. Les fournisseurs font appel aux systèmes de TI de Wal-Mart pour suivre automatiquement les ventes de leurs produits dans les magasins de la chaîne et coordonner le réapprovisionnement. D'autres détaillants se sont engagés dans cette voie, dont Tesco, la plus grande chaîne britannique de supermarchés, et l'allemand Metro. Par ailleurs, Wal-Mart a depuis étendu l'utilisation de la RFID à ses 300 premiers fournisseurs et à d'autres magasins.

- **Organismes publics** : Aux États-Unis, sous l'impulsion du Ministère de la défense, les organismes publics ont rapidement mis en œuvre des solutions RFID. Les applications les plus répandues à ce stade sont le contrôle des stocks et le traçage des produits coûteux. En octobre 2004, le Ministère de la défense a indiqué qu'à compter de janvier 2005, il exigerait de ses fournisseurs qu'ils apposent des marqueurs sur les caisses et palettes expédiées vers ses entrepôts. Il affirme que la RFID lui a permis de réaliser plus de 100 millions de dollars USD d'économies[16], les informations précises quant à la disponibilité des produits lui ayant par exemple évité de passer des commandes de réapprovisionnement sur les champs de bataille. L'administration américaine de la sécurité sociale a lancé un projet pilote dont elle affirme qu'il a produit des rendements substantiels, notamment pour les applications administratives de suivi des stocks ou de mise en œuvre de porte-monnaie électroniques dans son propre réseau de stations-service. De plus, un Conseil américain de la RFID, constitué de représentants de toute la branche exécutive et d'organismes indépendants, se réunit deux fois par an. Il comporte quatre sous-commissions chargées des applications, des questions réglementaires, des normes, et des questions de confidentialité et de sécurité. En Europe, le Groupe de travail RFID de l'UE est en train de rédiger une communication de la Commission qui expose les problèmes associés à cette technologie (le Groupe réunit des représentants de plusieurs Directions générales : société de l'information, entreprises, fiscalité et douanes).

Tableau 1. Avantages potentiels de la RFID pour les partenaires de la chaîne d'approvisionnement

Fabricants	Logisticiens	Détaillants
Réduction du temps de chargement des expéditions	Sélection plus rationnelle des commandes	Amélioration de la planification, de la programmation et de la distribution en magasin grâce aux données en temps réel.
Fiabilité accrue des expéditions	Taux supérieur de remplissage des commandes	Hausse de la productivité sur le point de vente et plus grande exactitude aux caisses
Précision accrue des données communiquées par les détaillants en ce qui concerne les ventes aux consommateurs	Réduction des pertes de stocks	Rendements plus fiables
Diminution du nombre de contrefaçons et de détournements	Diminution du nombre d'erreurs administratives et autres erreurs humaines	Amélioration de la logistique inverse
Soutien renforcé à la gestion des stocks par les fournisseurs	Diminution des besoins en main d'œuvre	Gestion plus rapide et précise des stocks
Plus grande facilité à rappeler les produits pour des raisons de sécurité	Baisse de la fraude chez les fournisseurs	Optimisation du niveau des stocks en magasin
Planification plus précise de la demande	Précision accrue des inventaires	Diminution des pertes internes et externes
Raccourcissement des délais d'exécution des commandes	Réduction du temps et des coûts de gestion des stocks	Réduction des besoins en main d'œuvre
Moindre besoin de stocks de sécurité	Rationalisation du processus d'acheminement	Automatisation des opérations de réception, de règlement des fournisseurs, et d'expédition vers les magasins
Meilleure utilisation de la main d'œuvre	Sécurité renforcée de la distribution des produits médicaux	Meilleure utilisation des actifs réutilisables (les palettes par exemple)
Hausse des ventes	Automatisation des opérations de réception, de règlement des fournisseurs, et d'expédition	Baisse des redevances de stationnement et des droits de surestarie
Diminution du temps et des coûts associés au dénombrement périodique, à la réception, à la collecte et à l'expédition des produits	Amélioration de la capacité dérivant de la plus grande efficacité des opérations	Lutte renforcée contre le marché gris
Moins de remboursements aux clients pour erreurs de livraison	Diminution des pénalités pour erreur d'exécution	Moyens plus efficaces d'évaluer l'exécution et l'efficacité des programmes de mise en étalage

Source : Shutzberg, L. (2004), Radio Frequency Identification (RFID) in the Consumer Goods Supply Chain: Mandated Compliance or Remarkable Innovation? Industry White paper, Rock-Tenn, Norcross GA. p51.

Aspects législatifs favorables aux programmes de déploiement de la RFID

Les lois, notamment celles ayant trait à la traçabilité des produits, au suivi des personnes et à la sécurité nationale (obligations de recyclage, prescriptions d'étiquetage indiquant le pays d'origine, suivi pharmaceutique, traçabilité des ingrédients alimentaires, techniques visant à prévenir la contrefaçon, ou contrôles transfrontaliers) favorisent l'adoption de la RFID dans certaines industries et certains domaines d'application.

Les directives européennes portant sur la gestion des emballages et des déchets, notamment la Directive relative aux déchets d'équipements électriques et électroniques (DEEE), la Directive relative aux emballages et aux déchets d'emballage et la Directive relative aux véhicules hors d'usage, attribuent la responsabilité de la gestion des déchets aux producteurs. La RFID peut éventuellement aider à détecter les équipements et sous-composants dont le traitement est nécessaire, et identifier le fabricant responsable.

Les lois portant sur le suivi des fournitures médicales et des aliments afin de garantir la santé et la sécurité des personnes stimulent aussi l'adoption de la technologie RFID. Dans certains cas, les lois proposées ou existantes imposent aux fabricants et aux détaillants de gérer des dispositifs de traçabilité très onéreux de ces produits. Ceux-ci pourraient faire appel à différentes technologies pour se conformer aux directives, mais le choix de la RFID s'impose pour une mise en œuvre économique. Dans certains cas, elle est expressément préconisée ou prescrite. Aux États-Unis, par exemple, la Food and Drug Administration recommande aux fabricants de médicaments, aux distributeurs et aux détaillants de l'adopter pour lutter contre la contrefaçon[17]. Par ailleurs, dans l'industrie alimentaire, la traçabilité des aliments assurée par la RFID est au centre des discussions[18].

Le Transportation Recall Accountability and Documentation (TREAD) Act, loi adoptée aux États-Unis après les rappels massifs auxquels ont dû procéder Firestone et Ford, impose l'intégration de marqueurs RFID dans les pneus d'automobiles afin de pouvoir en assurer un suivi rigoureux en cas de rappel[19].

Le Ministère américain de la sécurité intérieure encourage la création d'une norme ISO pour les scellés électroniques des conteneurs. Les ports et les transporteurs du monde entier attendent la mise au point définitive de cette norme avant d'investir dans son application. Les procédures accélérées dont bénéficieront les transporteurs qui utilisent des scellés RFID dans les ports américains en encourageront la mise en œuvre[20]. Les coûts initiaux seront élevés, puisque l'application de la RFID à un grand nombre de conteneurs nécessite une infrastructure spéciale à chaque point clé de l'expédition des cargaisons, mais les coûts marginaux devraient par la suite être modérés[21]. Les applications concernant les cartes sans contact pour l'identification nominale des citoyens (documents de voyage, cartes d'identité en Belgique, et plusieurs programmes en Europe) et pour les prestations personnelles (le projet britannique de carte de prestation), progressent aussi rapidement[22].

Problèmes associés à la RFID

Malgré les nombreux avantages que présente la technologie RFID, il convient pour réaliser son potentiel de résoudre divers problèmes interdépendants ayant trait aux aspects techniques et économiques, aux normes, à la confidentialité et à la sécurité.

Enjeux techniques

Il convient de remédier aux problèmes techniques associés aux lois de la physique. Si les ondes radioélectriques peuvent traverser la plupart des articles, la conjugaison des matériaux, des fréquences d'exploitation, de la puissance et de l'environnement connexes peut s'avérer problématique.

Le brouillage est le principal obstacle. En effet, il existe plusieurs sources de parasites potentiels lorsque les marqueurs et les lecteurs tentent d'établir une communication bidirectionnelle. La première vient de ce que les signaux de données d'un lecteur peuvent entrer en collision avec ceux d'un autre lecteur (collision entre lecteurs). Par ailleurs, la prolifération des appareils sans fil (téléphones sans cordon et mobiles, assistants numériques personnels, appareils électroniques grand public, etc.) risque aussi de produire des brouillages électromagnétiques avec les systèmes RFID. Ce phénomène pourrait devenir un problème substantiel et porter atteinte à la fiabilité des systèmes RFID puisque, dans la plupart des pays,

cette technologie ne dispose pas de sa propre bande de fréquences réservée mais opère dans des bandes qu'elle partage avec d'autres usagers. Si les applications de RFID se généralisent, il faudra, dans le cadre de leur mise au point et de leur utilisation, prendre davantage en considération les interférences radiomagnétiques émanant d'autres appareils.

La création et l'utilisation d'applications de RFID doivent prendre en compte le brouillage potentiel entre la RFID et l'utilisation existante des gammes de fréquences radioélectriques. Il ne sera peut-être pas possible d'établir dans toutes les gammes de fréquences envisagées par l'industrie une norme radio mondiale unique pour les systèmes RFID. En particulier, les fréquences allouées à l'exploitation de la RFID ne sont pas partout uniformes dans la bande des ondes décimétriques (UHF : 860 MHz-960 MHz), y compris dans les différents pays européens, ce qui limite l'interopérabilité des systèmes de RFID, selon la région ou le pays où le système est utilisé.

Un autre enjeu technique auquel la RFID est confrontée est celui de la sécurité. En effet, l'intégration de dispositifs cryptographiques augmente les coûts et risque de ralentir sa performance.

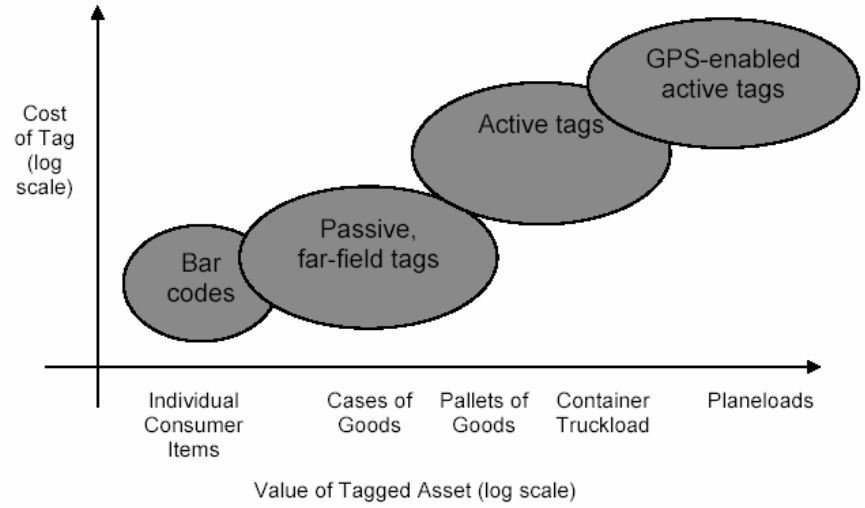
Coût de mise en œuvre

La RFID est d'ores et déjà employée dans de nombreuses applications, comme celles « d'identification d'amis ou d'ennemis » sur le champ de bataille ou de suivi des véhicules, qui sont aisément justifiables, mais son utilisation généralisée est encore dans ses toutes premières phases. Un obstacle substantiel à l'adoption de cette technologie est le coût encore élevé de sa mise en œuvre.

Si l'on veut que la RFID s'impose à grande échelle, il convient de démontrer que la rentabilité des capitaux engagés dépasse celle des la technique de suivi par codes à barres actuellement utilisée. Une multitude d'entreprises affirment avoir atteint un retour sur investissement en moins de 12 à 18 mois[23], mais beaucoup (notamment celles qui la mettent en œuvre à échelle réduite, et les PME qui sont tenues de l'adopter pour respecter les consignes) estiment que le rendement du capital investi est insuffisant, selon AMR Research[24]. La technologie offre certes la possibilité de réaliser des économies sur les coûts d'exploitation, mais le montant des investissements demeure prohibitif : selon la valeur de l'article marqué, le prix du marqueur peut être élevé, comme l'indique le graphique 2. Par exemple, le coût d'un marqueur radiofréquence EPC est fonction du volume, de sa capacité de mémoire et de son emballage, et varie entre 20 et 50 centimes USD. Les lecteurs sont également onéreux : la plupart coûtent de 1 000 à 3 000 USD, selon les dispositifs qu'ils comportent. De plus, les entreprises devront parfois acheter séparément chaque antenne, lesquelles coûtent 250 USD environ au minimum[25]. Les bases de données et les infrastructures nécessaires ajoutent par ailleurs au coût de mise en œuvre. De manière générale, on pourrait penser que les coûts associés à la technologie RFID[26] sont à peu près également répartis entre le matériel, les logiciels et l'intégration des systèmes aux systèmes de TI existants. Or, comme dans le cas des projets de carte intelligente et de carte sans contact, l'élément de coût essentiel des projets d'application de marqueurs RFID réside peut-être dans leur intégration aux processus en place, ou dans la reconfiguration des processus, plutôt que dans le matériel ou les équipements de réseau et de calcul supplémentaires.

Graphique 2. Les types de marqueurs adaptés à différentes sortes d'actifs

L'axe vertical correspondant au coût du marqueur et l'axe horizontal correspondant à la valeur de l'actif sont tous deux logarithmiques



Source : National Academies of Science, 2004

Coût du marqueur (échelle logarithmique) Valeur de l'actif étiqueté (échelle logarithmique)
Articles individuels Caisses Palettes Conteneurs transport routier Transport aérien
Codes-barres Marqueurs passifs en champ lointain Marqueurs actifs Marqueurs actifs dotés d'une fonction GPS

Une autre question directement liée est celle de savoir qui assume le coût de la RFID et qui en recueille les bénéfices. Les fournisseurs (souvent des petites et moyennes entreprises) ont protesté, soutenant qu'ils étaient obligés d'effectuer des investissements qui permettent aux détaillants de réaliser des économies. Ils verront probablement dans les solutions RFID une stratégie commerciale plutôt qu'une question de conformité quand le coût du déploiement diminuera et occasionnera des économies d'échelle plus importantes en diminuant le coût relatif des marqueurs, des lecteurs et des logiciels qui constituent le système RFID. Selon AMR Research[27], 137 fournisseurs de Wal-Mart ont investi 250 millions d'USD dans la RFID (soit de 1 à 3 millions d'USD chacun) pour satisfaire aux prescriptions minimales à la date de janvier 2005 imposée par Wal-Mart, pour acheter les marqueurs, les lecteurs et les principaux logiciels. AMR Research a par ailleurs estimé que pour dégager des bénéfices substantiels et un retour sur investissement et ne pas simplement engager les dépenses nécessaires pour satisfaire aux obligations, chaque fournisseur devrait dépenser de 13 à 23 millions d'USD pour intégrer la RFID à ses applications, remplacer les logiciels existants et assurer le stockage et le partage de volumes importants de données, selon le cas.

Modification des procédés

La RFID pourrait certes amener des progrès considérables mais, comme toutes les avancées techniques, elle exige que des modifications appropriées soient apportées aux méthodes opérationnelles. Beaucoup d'entreprises ont déclaré que la RFID n'est ni une solution, ni un objectif, mais un outil qui permettra de remplacer les procédés actuels par des méthodes plus immédiates, plus précises et moins redondantes[28]. Pour que la RFID simplifie les opérations, les entreprises doivent réviser leur mode de fonctionnement de manière à l'exploiter. Les questions associées aux méthodes opérationnelles concernent les fournisseurs d'application de l'entreprise ainsi que les intégrateurs de système et les experts-conseils en adaptation de processus.

Pour tirer pleinement parti de la RFID, les entreprises devront être capables de réorienter le personnel chargé de tâches telles que le balayage, la recherche et la vérification des produits sur des fonctions à plus forte valeur ajoutée, par exemple celles consistant à offrir un meilleur service à la clientèle[29] ou à anticiper les problèmes et participer à la mise au point de solutions.

Systèmes de TI

L'un des obstacles majeurs à l'adoption de la RFID n'est pas le matériel (marqueurs et lecteurs), mais les intergiciels de bordure de réseau, ou intergiciels RFID, qui relient le matériel de RFID aux divers systèmes de TI de l'entreprise. Selon ABI Research, en 2004, les coûts logiciels par centre de distribution se sont établis dans une fourchette comprise entre 75 000 USD et 125 000 USD, hors coûts d'intégration. Par ailleurs, le coût des licences des logiciels de détail allait de 1 500 USD à 3 500 dollars[30]. Sous l'effet de l'intensification des déploiements et de la pression concurrentielle, ces coûts ont sensiblement diminué. Les grands fournisseurs de solutions de planification de ressources d'entreprises, dont SAP, Oracle, IBM, et d'autres, travaillent fructueusement à la mise au point d'applications destinées à gérer les informations provenant des marqueurs RFID et à les intégrer à des applications existantes.

Le traçage de nombreux objets dotés d'une fonction RFID génère des volumes colossaux de données qui devront être filtrées, stockées et consultées avec efficacité. Pour cela, une gestion fonctionnelle des données, un stockage de grande capacité et très rapidement accessible, et des méthodes permettant de traiter les données inexactes, de vérifier l'intégrité des informations et d'assurer leur transfert entre les différents systèmes s'imposeront. Un analyste a calculé que si Wal-Mart stockait les données RFID de chaque article marqué sur chaque étagère, il produirait près de huit téraoctets de données par jour[31.] Des entreprises comme Cisco, Nortel et Symbol étudient comment adapter les fonctions classiques de gestion sans fil et de réseau à la gestion d'un environnement RFID actif et passif plus complexe, et regroupent déjà les fonctions RFID dans les solutions de provisionnement, de sécurité et de gestion de réseau existantes[32].

Obstacles législatifs

Il existe d'autres problèmes qui concernent les règlements sanitaires et écologiques. En Europe, par exemple, la Directive relative aux déchets d'équipements électriques et électroniques (DEEE) impose le recyclage des marqueurs. Si ceux-ci sont intégrés à des objets tels que des boîtes en carton (et non attachés à l'emballage externe de l'article, par exemple), le recyclage ultérieur des boîtes risque de poser problème dans la mesure où les marqueurs devront d'abord en être retirés.

Un obstacle potentiel : les craintes des consommateurs et des employés pour leur vie privée

La protection de la vie privée est un obstacle de poids à la mise en œuvre de la RFID, tant au niveau du consommateur que des entreprises. En l'absence de règles d'usage établies en matière de divulgation et de transparence, ou de techniques spécialisées pour traiter les données et les consulter convenablement, les personnes qui achètent des produits munis de marqueurs ou travaillent avec des articles marqués risquent de ne pas être averties de l'existence et de l'utilisation de ces marqueurs ; de plus, dans les cas où ceux-ci sont utilisés dans le cadre de programmes de fidélité ou de cartes de crédit pour mémoriser l'identité de la personne et d'autres renseignements privés, les données personnelles d'un individu risquent, si l'application n'est pas suffisamment sécurisée, d'être altérées ou piratées. De la même manière, les syndicats, les groupes de défense de la vie privée et les organismes de protection du consommateur se sont plaints, dans certains pays, que la technique de suivi RFID risquait de porter atteinte à la vie privée des employés[33].

Certains groupes de défense des consommateurs, qui s'inquiètent de l'aspect orwellien de cette technologie, s'opposent à sa mise en œuvre et au suivi RFID[34]. En l'absence d'une analyse minutieuse,

adéquate et transparente des questions relatives à la protection de la vie privée, y compris dans le cadre de programmes de sensibilisation, il est possible que les consommateurs et les citoyens rejettent cette technologie, ce qui pourrait à terme limiter ses avantages et son développement. Les groupes intervenants, comme le Center for Democracy and Technology (CDT) ou le Electronic Privacy Information Center (EPIC) travaillent actuellement à des échanges et des schémas constructifs, notamment à des solutions pratiques visant à renforcer la liberté d'expression et la confidentialité dans les techniques de communication mondiales.

PRINCIPAUX PROBLÈMES ASSOCIÉS A LA RFID EN TERMES D'ACTION PUBLIQUE

L'un des principaux avantages à étudier les problèmes associés à la RFID à ce stade de son développement, et la raison essentielle à l'organisation du Forum de prospective sur la RFID du Comité PIIC, est d'occasionner un débat entre toutes les parties intéressées (industrie, pouvoirs publics, société civile, et communauté technique), d'aborder tôt les problèmes de fond et d'appliquer des solutions à l'infrastructure RFID existante tout en respectant les besoins des pays de l'OCDE d'établir un équilibre entre la neutralité technologique et leur contexte national. La question de l'infrastructure héritée est cruciale, car les systèmes RFID mis au point aujourd'hui pourraient durer des décennies. A la différence de l'Internet, dont les logiciels que les usagers utilisent pour se connecter au réseau peuvent être mis à jour ou corrigés, l'architecture des systèmes RFID est conçue de telle manière que la modernisation de nombreux petits appareils sans fil pourrait s'avérer plus coûteuse. A l'inverse, les restrictions imposées aujourd'hui risquent d'étouffer la technologie dans sa phase (relativement) embryonnaire et l'empêcher de réaliser son vaste potentiel de moteur économique.

Les deux questions que tous les intervenants doivent aborder en matière d'action publique et qui seront débattues au Forum de l'OCDE sur la RFID sont les normes et l'interopérabilité d'une part, la sécurité et la confidentialité d'autre part. La normalisation est le déterminant majeur de l'interopérabilité qui, comme nous l'avons déjà mentionné, peut aussi favoriser l'adoption de règles de sécurité et de confidentialité. A l'avenir, avec le développement de la RFID et l'amélioration des fonctions de lecture des marqueurs, les problèmes de sécurité et de confidentialité (en particulier ceux concernant l'accès non autorisé, les fuites d'information et le suivi et la localisation) pourraient gagner en importance.

Normes et interopérabilité

Face à la dépendance grandissante des économies à l'égard du système commercial mondial, la nécessité d'étudier les coûts et les bénéfices dérivant de l'interopérabilité et de l'harmonisation des normes est allée croissant. D'aucuns estiment que la multiplicité des normes induit des coûts élevés pour le développement des produits et des technologies, et peut également constituer un obstacle non tarifaire de taille. D'autres pensent que la possibilité de mettre au point des technologies concurrentes fondées sur des normes différentes est le meilleur moyen de stimuler l'innovation et l'adoption en donnant un vaste choix au consommateur. Les normes éprouvées ont généralement des caractéristiques communes : elles sont facultatives, déterminées par le marché, ouvertes, transparentes, équilibrées et élaborées dans le cadre d'un système axé sur les résultats et conformément à une procédure établie.

Principales normes en matière de RFID

La technologie RFID a fait et continue de faire l'objet de nombreuses activités de normalisation, à l'échelon régional et international, dans le cadre des organismes et consortiums responsables de l'élaboration de normes tels que l'ISO et EPCGlobal, entre autres. Outre ces deux organisations, divers organismes de normalisation travaillent actuellement sur la RFID, notamment le Comité européen de normalisation (CEN), l'Institut européen des normes de télécommunication (ETSI), le US National Institute of Standards and Technology (NIST), ou la Standardization Administration of China (SAC). Il convient en outre de noter dès maintenant que l'approche d'EPCGlobal suscite des vues divergentes, notamment en ce qui concerne les questions relatives à la propriété intellectuelle.

Il existe des normes et spécifications RFID, en vigueur et proposées, qui spécifient *i)* le format des données contenues dans les marqueurs RFID (la façon dont les données sont organisées ou formatées) ; *ii)* le protocole de l'interface d'air assurant la communication entre les marqueurs et les lecteurs (fréquence, modulation, codage des bits, etc.) ; *iii)* la conformité, les moyens de vérifier que les produits respectent une norme ; *iv)* les applications particulières, par exemple l'emploi des normes pour les applications d'expédition, et *v)* les protocoles « intergiciels » qui spécifient de quelle manière les données et les instructions sont traitées.

Une instance très utile est l'ISO, qui a établi des normes pour la RFID en « boucle fermée », notamment des normes d'identification des animaux (ISO 11784 et 11785) et des normes pour le protocole de l'interface d'air des marqueurs RFID utilisés dans les systèmes de paiement et les cartes intelligentes sans contact (ISO 14443) et dans les cartes de voisinage (ISO 15693). Elle en a aussi défini pour vérifier la conformité des marqueurs et lecteurs RFID à une norme (ISO 18047) et pour contrôler leur fonctionnement (ISO 18046).

S'agissant des chaînes d'approvisionnement en « boucle ouverte », où les marqueurs sont conçus pour être réutilisés sur l'ensemble de la chaîne, les applications sont relativement plus récentes que celles déjà citées ; les normes établies sont donc moins nombreuses. L'ISO en élabore actuellement qui portent sur le suivi des conteneurs d'expédition de 40 pieds, des palettes, des unités de transport, des caisses et des articles individuels. Elles ont atteint différentes phases du processus d'approbation.

Depuis 1999, EPCGlobal Inc. participe aux travaux de normalisation pilotés par l'industrie et a mis au point le système EPC™, qui identifie chaque produit et assure son suivi sur l'ensemble de la chaîne d'approvisionnement, tout comme le code universel des produits (CUP) sur les codes-barres. L'objectif du groupe est de simplifier au maximum les marqueurs RFID, ceci dans le but de ramener ultérieurement le prix des puces à moins de cinq cents[35]. EPCGlobal a établi une taxinomie de catégories de marqueurs, des protocoles normalisés de signalisation des fréquences radioélectriques entre les marqueurs et les lecteurs, et des formats pour le stockage de l'identité et des données dans les marqueurs. Le réseau EPC Global est par ailleurs en train d'établir des spécifications et normes pour interconnecter les serveurs des partenaires qui contiennent des informations relatives aux objets identifiés par les numéros EPC. Les serveurs, appelés EPC Information Services (EPCIS) sont accessibles via Internet et reliés, autorisés et accessibles par l'intermédiaire d'un ensemble de services de réseau, comme l'illustre le graphique 3.

En décembre 2004, EPCglobal a ratifié une norme RFID très attendue, la norme UHF (ondes décimétriques) classe 1 génération 2 (EPC Gen2) pour le protocole d'interface d'air des technologies EPC de deuxième génération, ce qui encourage la recherche et le développement d'applications[36]. La norme impose une mémoire de 96 bits, une fonction de chiffrement et la possibilité de désactiver définitivement le marqueur après usage. Elle dissipe les craintes des gros usagers en ce qui concerne l'existence de différentes normes EPC pour la bande UHF, et se présente comme une norme libre de droits ou à droits modérés (même si, techniquement, il faut adhérer au réseau EPCGlobal pour l'utiliser).

Procédures de normalisation RFID en cours

L'ISO est en train d'examiner et de voter la spécification EPC Gen2 en vue de la ratifier dans la série ISO 18000 existante, qui couvre le protocole d'interface d'air concernant les principales fréquences utilisées dans les systèmes RFID mondiaux afin de suivre les produits dans la chaîne d'approvisionnement. A ce stade, elle doit toutefois encore la ratifier.

Par ailleurs, il faut encore définir avec la Chine des normes communes pour la chaîne d'approvisionnement, le suivi des stocks et la gestion des actifs. Celles-ci seront indispensables pour assurer l'interopérabilité des caisses et palettes marquées à l'étranger puisque la Chine, qui exporte de

grosses quantités de marchandises, est l'un des marchés potentiels les plus importants au monde pour la RFID. EPCGlobal a exprimé le souhait que la Chine adopte la norme EPC existante. A l'heure actuelle, le Ministère des sciences et de la technologie et treize autres administrations publiques chinoises, dont le Ministère de l'industrie de l'information et la Standardization Administration of China (SAC) rédigent un livre blanc sur la RFID en Chine qui définira l'orientation globale du développement de cette technologie dans le pays. La SAC a chargé le Groupe de travail national sur les normes des marqueurs RFID[37] de l'aider à décider quelle normes le pays doit adopter à cet égard. La Chine a déclaré qu'elle optera pour des normes qui seront compatibles avec celles d'EPCGlobal et de l'ISO, mais qui feront appel à ses propres droits de propriété intellectuelle afin d'établir une norme libre de droits[38].

Questions relatives aux droits de propriété intellectuelle et à la concurrence

Un examen des droits de propriété intellectuelle des organismes de normalisation, des entreprises et des usagers s'impose. Les problèmes de propriété intellectuelle associée à la RFID, notamment les revendications d'Intermec sur la propriété intellectuelle[39] de la norme EPC Gen2, ont créé une impasse et retardé les projets et programmes d'intégration de la RFID à la chaîne d'approvisionnement. Dernièrement[40], un groupe de 20 fournisseurs de RFID ne comprenant pas Intermec a formé un consortium de « brevets » pour diminuer le nombre de négociations en matière de brevets et faciliter ainsi l'accès à certains brevets RFID jugés « essentiels ». Les entreprises doivent toujours négocier séparément les licences d'Intermec.

Infrastructures d'information associées à la RFID

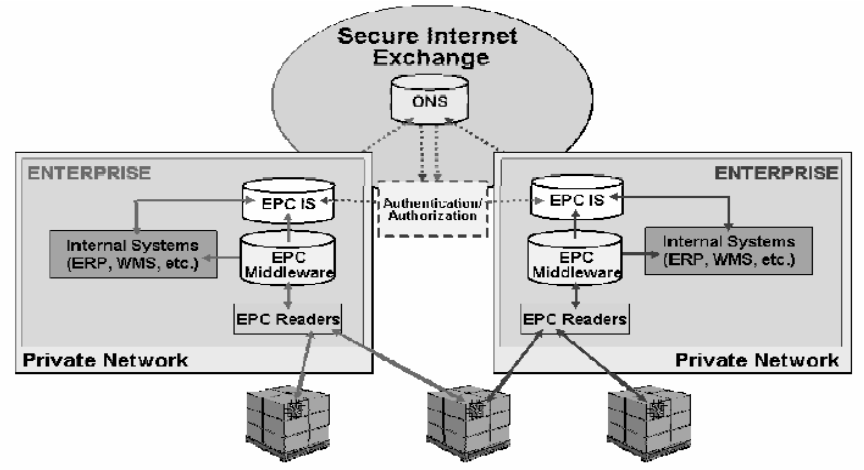
Les infrastructures d'informations associées à la RFID, notamment à l'EPC UHF, sont et seront de plus en plus accessibles par le biais des réseaux IP, des intranets privés et de l'Internet public.

L'économie politique des identificateurs RFID s'apparente à la coordination des espaces de noms et de chiffres dans d'autres médias : fondamentalement, les identificateurs doivent être uniques, et cette unicité exige une coordination. L'Object Name Service (ONS) est une composante majeure du système de RFID mis au point par EPCGlobal pour l'application de la technologie. Du fait que le marqueur RFID mémorise uniquement le code électronique de produit (EPC) d'un objet, l'ONS relie cet EPC aux informations concernant un article particulier identifié par le marqueur. L'ONS établit la connexion entre un bien matériel (identifié par le marqueur RFID qui transmet l'EPC) et les informations qui lui sont associées (formatées au moyen du PML, ou Physical Mark-up Language) via l'Internet[41]. Il peut s'agir d'informations détaillées sur le produit en question, son origine et ses antécédents, ou de la date de commande.

Cet Object Name Service est très similaire au système de noms de domaine de l'Internet, un système de mise en réseau automatisé qui relie une adresse appelée URL (identificateur uniforme de ressources) à une adresse IP (un chiffre), autrement dit un ordinateur qui contient des données. L'ONS gère l'attribution d'un EPC à une URL. EPCGlobal a choisi Verisign, qui administre également le serveur racine du système DNS sur l'Internet, pour développer l'ONS ; elle a également chargé cette société de gérer le serveur racine autorisé du réseau EPC pour la RFID et de fournir une structure de sécurité pour l'authentification, la protection des données et le contrôle de l'accès.

D'autres projets visant à mieux relier les objets à l'information sont en cours. Ainsi, l'entreprise à l'origine du Digital Object Identifier (norme DOI, ou identificateur d'objet numérique) pour l'identification électronique des documents et EPCGlobal mènent ensemble une étude concernant une collaboration et la convergence éventuelle des normes DOI et EPC.

Graphique 3. Illustration de l'infrastructure de réseau d'EPCGlobal



Source : EPCGlobal.

Centre de commutation Internet sécurisé ONS
Entreprise Systèmes internes (ERP, WMS, etc.) EPCIS Intergiciels EPC Lecteurs EPC Réseau privé
Authentification/autorisation
Entreprise EPCIS Intergiciels EPC Lecteurs EPC Systèmes internes (ERP, WMS, etc.) Réseau privé

Spectre et limitations en puissance

La RFID utilise les ondes radioélectriques de différentes fréquences, ce qui signifie que la bande spécifique dans laquelle les systèmes d'identification par radiofréquence fonctionnent est intégrée à leur conception dès les toutes premières phases. Les fréquences radioélectriques sont réglementées à l'échelon national, soit par une instance de réglementation des télécommunications, soit par un organisme spécialisé. Le tableau 3 de l'annexe 3 présente certains des principaux organismes gouvernant l'attribution des fréquences pour la RFID. La puissance d'émission dans les fréquences radioélectriques est limitée dans la plupart des pays. Autrement dit, les lecteurs RFID peuvent seulement émettre une puissance donnée, généralement jusqu'à deux watts, ce qui limite leur portée.

En général, les fréquences utilisées par les applications RFID sont exemptes de licences. La RFID fait aussi bien appel à des fréquences basses (LF : 125 – 134,2 kHz et 140 – 148,5 kHz) qu'à des fréquences élevées (HF : 13,56 MHz). Les basses fréquences interviennent pour des applications telles que le suivi des animaux, les hautes fréquences étant pour leur part largement utilisés dans les badges d'identification et le contrôle d'accès aux bâtiments, le suivi des livres de bibliothèque, des bagages dans le transport aérien, des articles d'habillement et des palettes.

Il n'existe cependant pas de norme mondiale unique pour les bandes décimétriques (UHF : 850 MHz-950 MHz) qui sont jugées essentielles aux applications de gestion de la chaîne d'approvisionnement en « circuit ouvert ». En Amérique du Nord, les ondes décimétriques sont exemptes de licence dans la bande des 902–928 MHz, mais des restrictions s'appliquent à la puissance radio émise (par les lecteurs). En Europe, l'Institut européen des normes de télécommunication (ETSI) a publié la norme ETSI EN 302 208 portant sur « le matériel d'identification des fréquences radioélectriques opérant dans la bande des 865 MHZ-868 MHZ à une puissance maximale de 2 Watts ». Néanmoins, quelques pays européens n'ont pas encore appliqué les règles recommandées par la CEPT pour les systèmes RFID opérant dans la bande des 865-868 MHZ pour des raisons d'incompatibilité avec les systèmes radioélectriques existants. En Chine, il n'existe pas de règlement gouvernant l'utilisation des bandes UHF. Dans ces pays, chaque application destinée à la bande décimétrique est assujettie une licence de site, qui

doit faire l'objet d'une demande aux autorités locales. En Australie et en Nouvelle-Zélande, la bande des 918-926 MHz est libre de licence, mais la puissance d'émission est soumise à des restrictions.

Bien qu'il n'existe pas de norme mondiale unique pour la bande UHF, des « lecteurs agiles » font leur apparition qui sont capables de lire différents protocoles d'étiquettes.

Encadré 1. Bandes de fréquences et normes pour la RFID

Les bandes de fréquences les plus couramment employées pour la RFD et les normes associées à leur utilisation :

Basse fréquence : 25 kHz HF –- Champ proche, intégralement passive	– ISO 18000-2
Haute fréquence (HF) : 13,56 MHz HF –- Champ proche, essentiellement passive	– ISO 18000-3 Mode 1, Mode 2 – ISO 14443 Type 1, Type B – ISO 15693 – EPCglobal Classe-1 HF
Décimétrique : 900 MHz UHF –- Champ lointain, en partie active	– EPCglobal Gen2 – ISO 18000-6 Type A, Type B
Hyperfréquences : 2,5 GHz UHF –- Champ lointain, en partie active	– ISO 18000-4 Mode 1, Mode 2

Source : D'après la National Academy of Science des États-Unis, 2005

Sécurité et protection des données personnelles intégrées

Selon plusieurs spécialistes de la sécurité[42], les problèmes de confidentialité et de sécurité soulevés par la RFID doivent être pris en considération avant que les normes ne soient établies et appliquées à grande échelle. De leur point de vue, l'intégration de sauvegardes techniques aux normes, à titre facultatif ou obligatoire, permettrait de maintenir un compromis entre ceux qui s'inquiètent du bon déroulement des opérations et ceux qui craignent pour la protection de la vie privée. Cette approche pourrait s'avérer plus efficace à terme.

Un document du groupe de travail des autorités européennes chargées de la protection des données des États membres de la Commission européenne (CE), dit « groupe de travail protection des données – Article 29 », qui porte sur la RFID et la protection de la vie privée, assure par ailleurs que le mode d'élaboration des normes et des produits RFID pourrait avoir une influence majeure sur l'application efficace des droits de protection des données[43] reconnus par l'article 12 de la Directive 95/46 de la CE relative à la protection des données.

Il serait possible d'intégrer des modalités plus strictes de protection des données dans les spécifications techniques de nombreux projets de normalisation pour la RFID. Ainsi, des universitaires ont proposé en 2004[44] de modifier la norme du protocole de communication entre lecteurs et marqueurs mise au point par l'ISO de manière à appliquer, au niveau technique, les dispositions des Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel.

Toujours au niveau de la définition des normes, des études de vulnérabilité conduites par des groupes de travail peuvent évaluer la sécurité des données sur différentes sortes de systèmes RFID. C'est par exemple pour cela que la norme relative aux scellés électroniques est retardée à l'ISO. Par ailleurs, les dispositifs de protection des données d'une norme permettraient, au besoin, le chiffrement des données, comme dans le cas déjà cité des scellés électroniques.

Questions de sécurité et de confidentialité associées à l'utilisation de la RFID

La collecte et l'emploi d'informations nominatives via les technologies RFID représentent un défi pour l'action publique ; l'absence de protection des données privées ou les carences de la sécurité risquent

de freiner le développement et l'utilisation de ces technologies. Avec le développement du marquage RFID au niveau des articles dans les toutes prochaines années, et l'utilisation, effective ou envisagée, de cette technologie par les pouvoirs publics à des fins d'authentification et d'identification (cartes d'identité, passeports ou plaques minéralogiques), les problèmes associés à la vie privée et à la sécurité des individus prennent une place de premier plan. Il est bel et bien probable que les données personnelles seront de plus en plus souvent obtenues par le biais de la RFID. Dans le même temps, les problèmes de sécurité et de protection de la vie privée liés à cette technologie peuvent considérablement varier selon le type de système utilisé et selon son mode de déploiement dans les limites des cadres juridiques en vigueur.

A ce stade, néanmoins, la majorité des craintes soulevées par certaines applications commerciales de la RFID en termes de vie privée et de sécurité ont trait à la collecte, à l'utilisation et au stockage des données produites via cette technologie à l'échelon du client individuel, sur le point de vente ou après. On se demande par exemple s'il convient de prévenir les clients de l'utilisation de la RFID au niveau des articles, et par quel moyen ; s'il faut leur donner la possibilité de désactiver le marqueur ; quelles données recueillir et comment les utiliser ou les diffuser ; et pendant combien de temps et à quelles fins les conserver. Certains défenseurs de la vie privée craignent que les marqueurs RFID ne demeurent actifs après l'achat et que des tierces parties puissent accéder aux informations qu'ils contiennent ou suivre le mouvement des articles, à l'insu de leur détenteur. En bref, il s'agit de savoir quand, par qui et comment les marqueurs peuvent être désactivés, et ce que deviennent les données qu'ils contiennent ou qui y sont recueillies. Mis à part les problèmes de confidentialité, il convient de noter que les consommateurs, pour des raisons diverses, pourraient souhaiter que le marqueur demeure actif, pour suivre leur approvisionnement en médicaments par exemple.

Interdépendance des questions de sécurité et de protection de la vie privée

Les questions de sécurité et de protection de la vie privée sont étroitement dépendantes les unes des autres et une application RFID peut soulever les deux types de problèmes. En matière de sécurité, il s'agit des risques concernant l'infrastructure et de l'accès non autorisé à des informations personnelles **confidentielles.** S'agissant de la vie privée, le danger vient de la possibilité de faire appel à la RFID pour localiser ou suivre les personnes. D'autres problèmes tiennent au fait que même les marqueurs RFID qui ne contiennent pas d'informations nominatives (un code produit par exemple) pourraient être associés à l'identité d'un individu.

- *Risques pour l'infrastructure :* ce problème n'est pas particulier à la RFID, mais les infrastructures d'entreprise dont la RFID constituerait l'un des éléments critiques pourraient voir leur vulnérabilité augmenter, par exemple face à de nouvelles formes d'attaques par saturation via le brouillage des signaux radioélectriques.
- *Écrémage et interception des données :* Il y a écrémage lorsque des informations sont subrepticement recueillies sur une puce RFID par une personne non autorisée. Des malfaiteurs peuvent par exemple utiliser des lecteurs RFID pour déterminer le contenu du sac d'un individu. Il y a interception de données quand celles-ci sont interceptées en cours de lecture par un lecteur RFID non autorisé.
  - *Suivi illicite* : Un problème de sécurité fondamental concernant l'utilisation de la RFID par les pouvoirs publics ou par les entreprises est le suivi illicite des marqueurs RFID qui, si ceux-ci peuvent être lus arbitrairement, risque non seulement de porter atteinte à la vie privée mais aussi de violer la sécurité militaire ou celle des entreprises. Il peut également constituer une source d'espionnage industriel au sein de la chaîne d'approvisionnement.
  - *Clonage et vol d'identité:* Une autre inquiétude a trait à la duplication non autorisée, ou clonage, des marqueurs RFID : certains d'entre eux peuvent être balayés à distance et à

l'insu de leur détenteur, ce qui pose problème pour les marqueurs contenus dans les cartes d'accès aux bâtiments ou les systèmes de paiement sans contact, de même que pour les passeports, cartes d'identité, voire les objets, dotés d'une fonction RFID.

- Risques pour la vie privée

  - L'éventuelle invisibilité des étiquettes et des lecteurs RFID est vue comme l'un des inconvénients potentiels majeurs de la RFID en termes de protection de la vie privée. Il serait ainsi possible de collecter des informations sur un produit donné et également, selon les circonstances, sur la personne qui le transporte, sans que cette dernière le sache ou y consente.

  - Une application RFID pourrait recueillir de grandes quantités de données. Si un article marqué est, par exemple, réglé par carte de crédit ou en association avec l'utilisation d'une carte de fidélité, il sera possible de rattacher l'identité unique de cet article à celle de l'acheteur. Les données personnelles, obtenues par l'intermédiaire de la RFID, pourraient alors servir à établir le profil d'un individu, lequel serait utilisable à des fins diverses, par exemple pour évaluer la valeur d'un consommateur pour une entreprise.

  - En théorie, les applications RFID permettent de suivre les personnes par l'intermédiaire des marqueurs RFID que celles-ci portent ou transportent. Ce phénomène gagnera en importance si différentes applications RFID sont intégrées dans un système plus vaste. Le système d'EPC Global, par exemple, crée pour chaque produit muni d'un marqueur un identificateur unique à l'échelle mondiale.

Opinions et réactions des consommateurs et citoyens

Du point de vue de la vie privée et de la liberté individuelle, les scénarios envisagés plus haut sont indésirables. Les entreprises et les pouvoirs publics devront cependant gérer ces problèmes avec délicatesse. Les défenseurs de la vie privée, comme l'EPIC (Electronic Privacy Information Center) ou Consommateurs contre l'invasion de la vie privée et la numérotation dans les supermarchés (CASPIAN) craignent que les informations détaillées concernant les achats des consommateurs et leur façon d'y procéder ne soient conservées dans des bases de données et éventuellement utilisées à des fins pernicieuses. Plusieurs campagnes publiques célèbres, comme celles menées contre Benetton, Gillette et TESCO, sont parvenues à interrompre les essais de RFID des entreprises[45]. De plus en plus, les parties intéressées organisent des dialogues et des débats constructifs sur les enseignements acquis dans le but de concilier les besoins de l'industrie, des pouvoirs publics et de la société civile.

Solutions législatives

Applicabilité des lois existantes en matière de protection de la vie privée

Il convient de déterminer si les cadres réglementaires en vigueur, autrement dit les lois et mécanismes d'autoréglementation relatifs à la protection des données privées, sont applicables, adaptés et efficaces pour remédier aux problèmes associés à la RFDI. Dans la plupart des cas, les lois sur la protection de la vie privée en existence, lorsqu'elles sont neutres sur le plan de la technologie, sont applicables.

En Europe, les lois mettent en application la Directive 95/46/CE et sont jugées applicables à la collecte et au traitement des données personnelles au moyen de la RFID. La Directive 2002/58/CE est considérée applicable dans les cas particuliers où la RFID est utilisée en conjugaison avec des téléphones cellulaires. Le 19 janvier 2005, le groupe des autorités européennes de protection des données de la

Commission européenne (CE) a publié un document sur les questions relatives à la protection des données[46]. Il s'agit d'un document de travail qui vise *i)* à donner aux entreprises qui déploient la RFID des indications quant à l'application des principes fondamentaux énoncés dans les Directives de la CE[47], et *ii)* d'informer les fabricants de la technologie ainsi que les organismes de normalisation de la RFID quant à leur responsabilité dans la conception d'une technologie respectueuse de la vie privée.

Aux États-Unis, la Federal Trade Commission protège les informations concernant les consommateurs par l'application de la section 5 de la loi FTC, qui interdit les actes déloyaux ou trompeurs ou ceux qui portent préjudice au commerce. La FTC a eu recours à cette section pour obliger les entreprises qui collectent des renseignements sur les consommateurs à respecter leurs promesses en matière de sécurité et de confidentialité.

Le traitement des données personnelles par la technologie RFID est également assujetti aux principes contenus dans les Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de 1980 (cf. encadré 2 ci-dessous). Celles-ci ont constitué l'assise de bon nombre de lois actuelles sur la protection de la vie privée, comme la Directive 95/46/CE de l'UE et le Cadre juridique sur la protection de la vie privée du groupe de coopération économique Asie-Pacifique (APEC), et servent de fondement à de nombreuses lois américaines à cet égard.

Cela posé, il existe plusieurs définitions de ce qui constitue des données personnelles, et ces subtilités ont leur importance lorsqu'il s'agit de la RFID[48]. Par ailleurs si, dans la plupart des cas, les lois sur la protection de la vie privée en vigueur dans l'UE sont applicables lorsque la technologie RFID sert à mémoriser et à traiter des données personnelles, la situation doit être nuancée quand un marqueur RFID contient des renseignements qui, en eux-mêmes, ne sont pas associés à un individu. Par exemple, un code produit contenu dans un marqueur attaché à un produit ne constitue pas une information personnelle tant que l'article est manipulé dans la chaîne d'approvisionnement ou reste aux mains du vendeur. Dans ce cas, les lois de l'UE sur la protection de la vie privée ne s'appliqueraient donc pas. En revanche, si un particulier achète le produit et que, sur le point de vente ou après, l'identité de cette personne est révélée, le code produit contenu dans le marqueur peut lui-même devenir une information personnelle indirecte, et les lois sur la protection de la vie privée pourraient s'appliquer. En outre, tout renseignement concernant un individu qui est d'abord collecté par l'intermédiaire de la technologie RFID sans que l'identité de l'individu soit connue peut devenir une information personnelle quand cette identité est ultérieurement associée à ces données.

L'application des lois ou principes sur la protection des données et de la vie privée requiert, entre autres, que les particuliers soient avertis de l'utilisation de la technologie RFID, des données recueillies, de l'objet du traitement, de l'identité du maître du fichier[49], et que des mesures soient prises pour permettre aux individus d'exercer leur droit de consultation de leurs données et de les faire effacer, rectifier, compléter ou modifier, le cas échéant. Les maîtres de fichiers devraient par ailleurs limiter la collecte de données personnelles à celles qui sont nécessaires pour satisfaire aux objectifs de l'application, veiller à ce que leur utilisation soit compatible avec les objectifs spécifiés et appliquer des sauvegardes de sécurité pour prévenir la perte, l'accès non autorisé, la destruction, l'utilisation, la modification ou la divulgation des données personnelles traitées dans les applications RFID.

L'OCDE a par ailleurs élaboré des Lignes directrices régissant la sécurité des systèmes et réseaux d'information qui s'appliquent à tous les participants à la nouvelle société de l'information. Celles-ci indiquent qu'une plus grande sensibilisation aux problèmes de sécurité et une meilleure compréhension de ces problèmes s'imposent, et qu'il convient notamment de créer une « culture de la sécurité » - autrement dit, privilégier la sécurité dans la mise en place de systèmes et de réseaux d'information et l'adoption de nouveaux modes de pensée et de comportement pour utiliser les systèmes et réseaux d'information et

communiquer avec eux. Ces lignes directrices forment la base de travaux visant à créer une culture de la sécurité dans l'ensemble de la société.

Encadré 2. Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (1980)

Les Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, adoptées le 23 septembre 1980, demeurent l'expression d'un consensus international quant aux orientations générales concernant la collecte et la gestion des informations à caractère personnel. Parce qu'elles établissent des principes fondamentaux, elles jouent un rôle essentiel en aidant les pouvoirs publics, les entreprises et les représentants des consommateurs à protéger la vie privée et les données personnelles, et en évitant les restrictions inutiles aux flux transfrontières de données, par voie électronique ou autre.

Les Lignes directrices renferment les huit principes suivants :

1. **Principe de la limitation en matière de collecte** : Il conviendrait d'assigner des limites à la collecte des données de caractère personnel et toute donnée de ce type devrait être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement.

2. **Principe de la qualité des données** : Les données de caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour.

3. **Principe de la spécification des finalités** : Les finalités en vue desquelles les données de caractère personnel sont collectées devraient être déterminées au plus tard au moment de la collecte des données et lesdites données ne devraient être utilisées par la suite que pour atteindre ces finalités ou d'autres qui ne seraient pas incompatibles avec les précédentes et qui seraient également déterminées dès lors qu'elles seraient modifiées.

4. **Principe de la limitation de l'utilisation** : Les données de caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées, si ce n'est a) avec le consentement de la personne concernée ; ou b) lorsqu'une règle de droit le permet.

5. **Principe des garanties de sécurité** : Il conviendrait de protéger les données de caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation, ou divulgation non autorisés.

6. **Principe de la transparence** : Il conviendrait d'assurer, d'une façon générale, la transparence des progrès, pratiques et politiques, ayant trait aux données de caractère personnel. Il devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données de caractère personnel, et les finalités principales de leur utilisation, de même que l'identité du maître du fichier et le siège habituel de ses activités.

7. **Principe de la participation individuelle** : Toute personne physique devrait avoir le droit a) d'obtenir du maître d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant ; b) de se faire communiquer les données la concernant (dans un délai raisonnable ; moyennant, éventuellement, une redevance modérée ; selon des modalités raisonnables ; et sous une forme qui lui soit aisément intelligible) ; c) d'être informée des raisons pour lesquelles une demande qu'elle aurait présentée conformément aux alinéas (a) et (b) est rejetée et de pouvoir contester un tel rejet ; et d) de contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.

8. **Principe de la responsabilité :** Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.

Encadré 3. Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information (2002)

Il convient de lire ces Lignes directrices en parallèle aux recommandations complémentaires concernant la protection de la vie privée (encadré 2) et la cryptographie (annexe 2).

Les Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information renferment les neuf principes suivants :

1. **Sensibilisation** : Les parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité.

2. **Responsabilité** : Les parties prenantes sont responsables de la sécurité des systèmes et réseaux d'information.

3. **Réaction** : Les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité.

4. **Éthique** : Les parties prenantes doivent respecter les intérêts légitimes des autres parties prenantes.

5. **Démocratie** : La sécurité des systèmes et réseaux d'information doit être compatible avec les valeurs fondamentales d'une société démocratique, notamment la liberté d'échanger des pensées et des idées, la libre circulation de l'information, la confidentialité de l'information et des communications, la protection adéquate des informations de caractère personnel, l'ouverture et la transparence.

6. **Évaluation des risques** : Les parties prenantes doivent procéder à des évaluations des risques qui permettent de déceler les menaces et vulnérabilités, qui doivent être suffisamment larges et permettent de déterminer le niveau acceptable de risque.

7. **Conception et mise en œuvre de la sécurité** : Les parties prenantes doivent intégrer la sécurité en tant qu'un élément essentiel des systèmes et réseaux d'information

8. **Gestion de la sécurité** : Les parties prenantes doivent adopter une approche globale, dynamique et anticipative de la gestion de la sécurité, fondée sur l'évaluation des risques et couvrant tous les niveaux d'activités des parties prenantes et tous les aspects de leurs opérations.

9. **Réévaluation** : Les parties prenantes doivent examiner et réévaluer la sécurité des systèmes et réseaux d'information et introduire les modifications appropriées dans leurs politiques, pratiques, mesures et procédures de sécurité.

Promulgation de dispositions particulières relatives à la RFID

Certains pays, dont le Japon[50], l'Italie[51], la Corée et les États-Unis (au niveau des États)[52] ont proposé ou envisagent de proposer des lignes directrices ou des règlements spécifiques concernant la RFID.

D'autres, comme les Pays-Bas, sont parvenus à la conclusion provisoire que de nouvelles lois portant spécifiquement sur la RFID sont inutiles à ce stade du développement de la technologie. Ils estiment par ailleurs qu'une législation prématurée retardera et freinera très vraisemblablement le développement et l'application ultérieurs de la RFID, sans nécessairement contribuer à améliorer la protection de la vie privée et des libertés individuelles. Dans certains cas, il sera peut-être moins nécessaire d'élargir la protection de la vie privée que d'accroître la transparence des régimes en vigueur et de renforcer l'application du régime juridique.

Autoréglementation de l'industrie

Un exemple d'approche par autoréglementation nous est donné par les lignes directrices (2005)[53] publiées par EPCglobal pour que l'utilisation de l'EPC soit conforme aux principes fondamentaux de la

protection de la vie privée, à savoir la notification, le choix et la sécurité– ainsi que la formation du consommateur. La *notification* signifie qu'une étiquette normalisée marque le produit ou l'emballage des produits dotés d'un marqueur RFID. Il faudra du temps pour *former* les consommateurs à reconnaître les produits munis de marqueurs RFID. Selon certains intervenants sectoriels, cette opération nécessitera une campagne multimédia similaire à celle qui a été conduite pour les étiquettes des ingrédients[54]. Le *choix* signifie que les consommateurs seront informés de la possibilité de jeter, retirer ou désactiver les marqueurs RFID des produits qu'ils achètent. S'agissant de *l'utilisation des données enregistrées, de leur rétention et de la sécurité,* les lignes directrices établissent que le « code produit électronique ne contient, ne collecte ou ne mémorise aucune information nominative ». Néanmoins, les futures applications grand public qui requièrent la mise en correspondance des numéros EPC avec les informations nominatives appelleront probablement de nouvelles formes de notification.

Parmi ces lignes directrices, la question du choix est aujourd'hui complexe, à moins que les marqueurs ne figurent sur les emballages, qui sont jetables. Si les *protocoles* EPC permettent de « tuer » les marqueurs, les lecteurs RFID capables à la fois de les lire et de les désactiver sont coûteux et ne seraient pas entièrement efficaces. En 2004, un lecteur bidirectionnel coûtait plusieurs milliers de dollars[55]- somme qui, multipliée par le nombre de caisses d'un magasin dans un pays, pourrait atteindre un montant prohibitif pour certaines entreprises, et donc contrecarrer l'objectif d'optimisation de la chaîne d'approvisionnement via la RFID.

Solutions techniques proposées pour la protection de la vie privée et la sécurité

Certaines applications exigent des protocoles de communication sécurisés ; le dispositif d'émission doit donc être doté d'une fonction de chiffrement. Par exemple, le chiffrement de l'interface d'air et l'authentification mutuelle permettent de protéger les applications d'identification sans fil par carte intelligente contre le vol ou le traçage d'identité[56]. Ce degré de sécurité requiert néanmoins des moyens financiers et administratifs plus importants.

La plupart des dispositifs RFID bon marché ne sont cependant pas dotés des moyens de calcul nécessaires pour utiliser les techniques de chiffrement standard. En l'absence de chiffrement des données ou de l'émission, le numéro d'identité unique émis par le marqueur RFID peut être intercepté. Cette identité unique étant généralement un chiffre aléatoire qui indique simplement un champ dans une base de données, l'information n'aura en soi guère d'intérêt, à moins qu'elle ne soit reliée à d'autres renseignements utiles.

Pour résoudre le problème de la protection des données à caractère personnel des consommateurs, des fournisseurs et usagers de dispositifs RFID ont participé à la mise au point des marqueurs EPC Gen2 d'EPCGlobal de manière à ce que ceux-ci puissent être « tués », autrement dit définitivement neutralisés, sur le point de vente. Or, s'ils répondent aux préoccupations en matière de protection de la vie privée, ces marqueurs risquent de limiter le nombre d'applications RFID utiles aux consommateurs, de freiner la diffusion de la technologie RFID et la mise au point de solutions innovantes qui apportent des avantages aux acheteurs. Il convient donc de trouver le moyen d'assurer à la fois la protection des données personnelles et l'utilité de l'application. Différentes instances, dont le Groupe de travail sur la RFID d'EICAR[57] ou des laboratoires de recherche, consacrent actuellement de nombreuses études aux solutions technologiques.

Plusieurs solutions techniques ont été proposées qui visent à conjuguer protection de la vie privée et utilité en créant les moyennes de limiter les émissions ou de traiter l'information[58]. On citera par exemple le « bit de confidentialité »[59] mis au point par RSA Labs, qui a pour objectif de donner aux concepteurs la possibilité de compléter la norme EPC Gen2 actuelle.

Les chercheurs de l'Auto-ID Lab de l'Université de St. Gallen et d'ETH Zurich ont avancé des idées d'inspiration similaire à celle du bit de confidentialité ; ils se sont penchés à la fois sur leur application par l'intermédiaire de dispositifs de traçage et sur leur correspondance avec les lignes directrices de l'OCDE pour la protection des informations à caractère personnel.

Une autre solution proposée pour les marqueurs RFID est l'insertion d'un mécanisme d'activation/désactivation qui les désactiverait par défaut lors de la procédure de paiement aux caisses et donnerait aux consommateurs un mot de passe leur permettant de les réactiver en cas de besoin[60].

Pour protéger les consommateurs d'un balayage intempestif des marqueurs RFID attachés à des objets qu'ils transportent ou des vêtements qu'ils portent, plusieurs techniques protectrices de la vie privée (TPVP) ont été proposées : le « blocage sélectif », comme le dispositif RSA®Blocker Tag des Laboratoires RSA, fait intervenir un dispositif RFID passif bon marché qui brouille localement les signaux RFID en interrompant un protocole anti-collision standard, ce qui permet à l'usager d'empêcher l'identification s'il le souhaite. On citera également le blindage des marqueurs RFID au moyen d'une « cage de Faraday », à savoir un conteneur constitué de filet métallique ou d'aluminium imperméable aux signaux radioélectriques (de certaines fréquences) et au brouillage actif des signaux RF[61].

Plusieurs solutions cryptographiques, notamment le blocage de la fonction de hachage (« hash lock »), le chiffrement par OU exclusif sur la voie de retour, les tiers de confiance et l'authentification LPN , ont été proposées[62].

D'autres, comme les fondateurs de Matrics, ont proposé d'autres méthodes que EPC Gen 2 pour obtenir un degré élevé de sécurité RFID. Estimant que la clé à la sécurité RFID est la simplicité et une assise fondamentalement sûre, ils proposent de stocker dans une mémoire en lecture seule un chiffre aléatoire qui constituerait le marqueur d'identification[63].

ANNEXE 1. SOURCES

DOCUMENTS D'ORIENTATION :

US Federal Trade Commission (FTC), 2005, « RFID: Applications and Implications for Consumers. A Workshop Report from the Staff of the FTC », mars – http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf

US Department of Commerce, 2005, « Radio Frequency Identification – Opportunities and Challenges in Implementation », Washington, avril– www.technology.gov/reports

OCDE, 2004, Digital Delivery in Distribution and Logistics, avril, DSTI/ICCP/IE(2004)17/FINAL– www.oecd.org/dataoecd/19/8/34884379.pdf

OCDE, 2004, Perspectives des technologies de l'information, pp. 272-274 – www1.oecd.org/publications/e-book/9304021E.pdf

OCDE, 2004, L'économie de la sécurité, chapitre 4. RFID : Le concept et l'incidence, Programme de l'OCDE sur l'avenir.

Commission européenne - Article 29 Groupe de travail protection des données, 2005, Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification), janvier, 10107/05/EN WP 105 http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

AUTRES :

National Academy of Sciences, 2004, Radio Frequency Identification Technologies: A Workshop Summary www.nap.edu/catalog/11189.html

Pratiques optimales de l'industrie et de la société civile.

ANNEXE 2. LIGNES DIRECTRICES PERTINENTES DE L'OCDE

Encadré 4. Autres lignes directrices pertinentes de l'OCDE

Lignes directrices de l'OCDE régissant la politique de cryptographie (1997) (extraits)

Les Lignes directrices de l'OCDE régissant la politique de cryptographie énoncent huit principes interdépendants, qui prennent chacun en compte un sujet de préoccupation majeur des pouvoirs publics et devraient être mis en œuvre comme un tout de manière à concilier les différents intérêts en jeu :

1. Confiance dans les méthodes cryptographiques : Les méthodes cryptographiques devraient susciter la confiance afin que les utilisateurs puissent se fier aux systèmes d'information et de communication.

2. Choix des méthodes cryptographiques : Les utilisateurs devraient avoir le droit de choisir toute méthode cryptographique, dans le respect de la législation applicable.

3. Développement des méthodes cryptographiques guidé par le marché : Les méthodes cryptographiques devraient être développées en réponse aux besoins, aux demandes et aux responsabilités des personnes, des entreprises et des gouvernements.

4. Normes applicables aux méthodes cryptographiques : Des normes, critères et protocoles techniques applicables aux méthodes cryptographiques devraient être élaborés et instaurés aux échelons national et international.

5. Protection de la vie privée et des données à caractère personnel : Les droits fondamentaux des individus au respect de leur vie privée, notamment au secret des communications et à la protection des données de caractère personnel, devraient être respectés dans les politiques nationales à l'égard de la cryptographie et dans la mise en œuvre et l'utilisation des méthodes cryptographiques. Les Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel fournissent des orientations générales concernant le recueil et la gestion des informations de caractère personnel, qui devraient être appliquées conjointement avec les dispositions pertinentes de la législation nationale lors de la mise en œuvre des méthodes cryptographiques.

6. Accès légal : Les politiques nationales à l'égard de la cryptographie peuvent autoriser l'accès légal au texte en clair ou aux clés cryptographiques de données chiffrées. Ces politiques doivent respecter dans toute la mesure du possible les autres principes énoncés dans les Lignes directrices.

7. Responsabilité : Qu'elle soit établie par contrat ou par voie législative, la responsabilité des personnes et entités qui proposent des services cryptographiques ou détiennent des clés cryptographiques ou y ont accès, devrait être clairement énoncée.

8. Coopération internationale : Les gouvernements devraient coopérer en vue de coordonner les politiques à l'égard de la cryptographie. Dans le cadre de cet effort, les gouvernements devraient veiller à la levée, ou éviter de créer au nom de la politique de cryptographie, des obstacles injustifiés aux échanges.

Déclaration ministérielle relative à la protection de la vie privée sur les réseaux (1998) (extraits)

Les Gouvernements des pays Membres de l'OCDE déclarent :

Qu'ils prendront, dans le cadre de leurs lois et pratiques respectives, les mesures nécessaires pour garantir la mise en œuvre efficace des Lignes directrices de l'OCDE sur la protection de la vie privée en ce qui concerne les réseaux mondiaux, en veillant notamment :

- à encourager l'adoption de politiques en matière de vie privée, qu'elles soient mises en œuvre par le recours à des mécanismes juridiques, administratifs, technologiques ou d'autorégulation ;
- à encourager la notification en ligne aux utilisateurs des politiques en matière de vie privée;
- à garantir l'existence de mécanismes efficaces de mise en œuvre permettant à la fois de régler les problèmes de non respect des principes et des politiques de vie privée et de garantir l'accès à des moyens de réparation ;
- à promouvoir l'éducation et la sensibilisation des utilisateurs aux problèmes de respect de la vie privée en ligne et aux moyens dont ils disposent pour protéger leur vie privée sur les réseaux mondiaux ;
- à encourager l'utilisation de technologies permettant d'améliorer la protection de la vie privée ;
- à encourager l'utilisation de solutions contractuelles et le développement de solutions contractuelles type pour les flux transfrontières de données en ligne.

ANNEXE 3. EXEMPLES DE POLITIQUES NATIONALES EN MATIÈRE DE RFID

Tableau 2. Exemples de mesures spécifiques de sauvegarde la vie privée et de protection des données

Italie	Disposition du 9 mars 2005 de la Directive italienne sur les sauvegardes appliquées à l'utilisation de dispositifs RFID : La disposition exige des maîtres de fichiers publics et privés qu'ils respectent les principes de protection des données énoncés dans la loi, à savoir : minimisation des données ; avis d'information ; consentement ; spécification des finalités. La Directive italienne établit par ailleurs des dispositions spécifiques concernant l'utilisation de dispositifs RFID dans le cadre de l'emploi et des implantations sous-cutanées.
Japon	Le 30 mars 2004, le « Groupe de recherche et d'étude sur l'utilisation et l'application avancées de marqueurs électroniques à l'ère des réseaux ubiquitaires » du MIC (anciennement MPHPT) japonais a élaboré une « Structure d'orientation pour la protection de la vie privée dans l'utilisation des marqueurs RFID » contenue dans le rapport final « Travaux préalables à l'utilisation et à l'application avancées de la RFID ». Le 16 mars 2004, le Ministère de l'économie, du commerce et de l'industrie (METI) a mis au point les « lignes directrices en vue de protéger la vie privée en ce qui concerne les marqueurs RFID ». Par la suite, les deux ministères susmentionnés, le MPHPT et le METI, ont établi conjointement les « Lignes directrices pour la protection de la vie privée à l'égard des marqueurs RFID » dans le cadre d'un consensus entre les parties intéressées, dont les prestataires de services et les groupes de consommateurs. Ces lignes directrices ont été publiées le 8 juin 2004 et sont entrées en vigueur, mais elles ne sont pas contraignantes. Leur application est recommandée dans le cadre de toutes les activités commerciales qui font intervenir des marqueurs RFID et des produits qui en sont munis. Les deux ministères vont mener des compagnes de sensibilisation destinées à faire connaître les lignes directrices aux organismes compétents et aux consommateurs.
Corée	Les « Lignes directrices pour la protection de la vie privée à l'égard de la RFID » ont été élaborées et publiées par le Ministère de l'information et des communications (MIC). Le 7 juillet 2005, mais n'étaient pas encore entrées en vigueur le 19 septembre 2005. Elles ne sont pas obligatoires mais, si leur promulgation s'avère nécessaire, le gouvernement coréen créera une loi qui en tiendra compte. Du fait qu'elles ne sont pas entrées en vigueur, les Lignes directrices sont applicables au secteur public comme au secteur privé. Néanmoins, si elles sont promulguées sous forme de loi, quelques exceptions s'appliqueront peut-être au secteur public.

Tableau 3. Exemples d'instances de réglementation et réglementations principales appliquées à la RFID en bande décimétrique (UHF)

Chine	Les fréquences de la bande UHF dans laquelle la norme mondiale de prochaine génération Gen 2 opérera (à savoir la bande des 860 MHz-960 MHz) est largement occupée par les dispositifs de télécommunications GMS et AMRC. L'autorité chinoise de gestion des fréquences radioélectriques teste actuellement diverses fréquences et accorde des licences temporaires dans la bande décimétrique[64].
Union européenne	ERO, CEPT, ETSI. Les administrations nationales doivent ratifier l'emploi d'une plage de fréquences donnée avant qu'elle ne puisse être utilisée. L'Institut européen des normes de télécommunication (ETSI) a publié une norme technique (EN 302 208) ETSI 300 328 pour le matériel d'identification par radiofréquence opérant dans la bande 865 MHz-868 MHz qui autorise une puissance d'émission rayonnée (des lecteurs) maximale de 2 Watts. La Conférence Européenne des postes et télécommunications (CEPT) a préconisé dans sa recommandation sur les appareils de faible portée que le spectre des 865 MHz-868 MHz soit alloué sans licence à la RFID (CEPT/ERC/Rec 70-03).
Japon	Le Ministère des affaires intérieures et des communications (MIC), l'instance de réglementation responsable de la gestion du spectre, a institutionnalisé en avril 2005 un système de marqueurs passifs à grande puissance qui fait appel à la bande des 952 MHz-954 MHz, et prévoit d'institutionnaliser le système de marqueurs passifs à faible puissance qui utilise la bande des 952 MHz-955 MHz et le système amélioré de marqueurs passifs à forte puissance aux environs de février 2006.
Royaume-Uni	L'Ofcom britannique, l'instance de réglementation responsable du spectre, a publié le 9 août 2005 un projet de réglementation[65] couvrant la RFID, qui recommande que les équipements de RFID dans la bande des 865 MHz-868 MHz soient exemptés de licences de télégraphie sans fil. Ce projet est ouvert à la consultation du public jusqu'au 12 septembre 2005.
États-Unis	La Federal Communications Commission (FCC) autorise l'utilisation des bandes de fréquences des 902 MHz-928 MHz par les dispositifs industriels, scientifiques et médicaux (ISM) non détenteurs de licences. Des normes spécifient la puissance de sortie maximale.

GLOSSAIRE

AIDC	Identification et acquisition de données automatiques
Auto-ID Labs	Le Centre Auto-ID était une association à but non lucratif d'entreprises privées et d'universités qui a fait œuvre de pionnier dans le développement d'une infrastructure de type Internet pour assurer le traçage des produits à l'échelle mondiale au moyen de marqueurs RFID assortis de codes électroniques de produit (EPC). Le centre a fermé ses portes en septembre 2003. EPCGlobal a été créée pour poursuivre la commercialisation de la technologie EPC ; les laboratoires Auto-ID continuent les travaux de recherche du centre dans différentes universités de par le monde.
CEPT	Conférence européenne des postes et télécommunications
GRC	Gestion des relations clients
DHS	Ministère américain de la sécurité intérieure
DNS	Système de noms de domaines
DOI	Identifiant d'objets numériques
DoD	Ministère américain de la défense
EAN	Numérotation européenne des articles
EAN International	Organisme responsable des normes de codification des codes à barres
EPC	Code électronique de produit
EPCGlobal	Organisme à but non lucratif établi par le Uniform Code Council et EAN International, les deux organismes responsables des normes de codification des codes-barres, pour commercialiser la technologie EPC. EPCglobal. EPCGlobal est composé de chapitres dans différents pays et régions. Il commercialise la technologie initialement mise au point par le Centre Auto-ID.
ERO	Bureau européen des radiocommunications
PRE	Planification des ressources de l'entreprise
PAR	Puissance apparente rayonnée
ESTI	Institut européen des normes de télécommunication
GSM	Système mondial de communications mobiles
HF	Haute fréquence
IANA	Internet Assigned Numbers Authority
TIC	Technologies de l'information et des communications
IEEE	Institute of Electrical and Electronics Engineers
IP	Protocole Internet
ISO	Organisation internationale de normalisation
LAN	Réseau local d'entreprise
NFC	Communication en champ proche
ONS	Object Name System
PDA	Assistant numérique personnel
TPVP	Technologies protectrices de la vie privée

GLOSSAIRE
(suite)

PML	Physical Markup Language
RTPC	Réseau téléphonique public commuté
QoS	Qualité de service
RF	Radiofréquence
RFID	Identification par radiofréquence
ROI	Taux de rendement du capital investi
TCP	Protocole de contrôle de transmission
UID	Identificateur/identification unique
UCC	Uniform Code Council
UHF	Ondes décimétriques : de 300 MHz à 3 GHz (les marqueurs RFID opèrent généralement entre 866 MHz et 960 MHz)
UPC	Code universel des produits
URL	Identificateur uniforme de ressources
WAN	Réseau étendu
WEEE	Directive relative aux déchets d'équipements électriques et électroniques
WLAN	Réseau local sans fil

NOTES

1 Les marqueurs passifs coûtent généralement entre 20 centimes d'USD lorsqu'ils sont achetés en gros volume et plusieurs dollars quand ils sont intégrés à des porte-clés ou à des étuis en plastique protecteurs. Le prix des marqueurs actifs est compris entre 10 USD et 50 USD, voire plus, selon la taille de la pile, la quantité de mémoire de la puce et l'emballage du transpondeur. Les lecteurs UHF coûtent de 500 USD à 3 000 USD selon leurs fonctions. http://www.rfidjournal.com/article/articleview/1336/1/129/

2 Research and Markets, RFID Industry— A Market Update, juin 2005, http://www.researchandmarkets.com/reports/c20329

3 Organisation internationale de normalisation.

4 EPCglobal est une coentreprise formée par EAN International et le Uniform Code Council. Pilotée par l'industrie, elle compte parmi ses membres Gillette, METRO AG, Novartis Pharma AG, Procter & Gamble, Unilever, Target, Carrefour, Tesco, Kimberly Clark, Cisco Systems, Hewlett-Packard, ainsi que des universités telles que le Massachusetts Institute of Technology.

5 OCDE, 2004, Perspectives des technologies de l'information 2004, pp. 272-274.

6 OCDE, 2004, L'économie de la sécurité, chapitre 4. RFID : Le Concept et l'incidence, Programme de l'OCDE sur l'avenir.

7 Néanmoins, une distinction est souvent établie entre la RFID et les cartes intelligentes sans contact. Voir par exemple http://www.smartcardalliance.org/pdf/alliance_activities/rfidvscontactless_final_121704.pdf.

8 Surveillance électronique des objets – le système EAS, appliqué dans les magasins de nombreux pays depuis les années 60.

9 http://www.vnunet.com/vnunet/news/2124563/nokia-brings-rfid-mobile-phones

10 Merloni Unveils RFID Appliances, 4 avril 2003, http://www.rfidjournal.com/article/view/369/1/1/

11 http://www.rfidjournal.com/article/articleview/1332/1/129/

12 Toensmeier, Patrick, Plastics Engineering, février 2005, As RFID Applications Increase, Suppliers Look To Lower Its Cost

13 http://www.reed-electronics.com/electronicnews/article/CA6261023.html?industryid=21376

14 Toensmeier, Patrick, Plastics Engineering, février 2005, As RFID Applications Increase, Suppliers Look To Lower Its Cost.

15 Rapport de AMR Research et ABI Research.

16 Elizabeth Board, EPCGlobal, conversation du 25 juillet 2005.

17 http://www.fda.gov/bbs/topics/news/2004/NEW01133.html

18 http://www.nal.usda.gov/fsrio/research/fsheets/fsheet12.htm

19 Product Recalls Pushing RFID, E-week, 16 août 2004, http://www.eweek.com/article2/0,1895,1636342,00.asp

20 Customs-Trade Partnership Against Terrorism (C-TPAT), programme dirigé par le bureau américain des douanes et de la protection des frontières, une branche du Ministère de la sécurité intérieure.

21 ABI Research, 2004, Electronic Container Tracking White Paper.

22 ABI Research, 2004, Electronic Container Tracking White Paper.

23 Roberti, Mark, RFID's Case of Schizophrenia, 1er août 2005 http://www.rfidjournal.com/article/articleview/1762/1/128/

24 Gaughan, Dennis, « RFID Technology Assessment 2005-2007: Where Is the ROI? », 20 juillet 2005

25 http://www.rfidjournal.com/article/articleview/219#Anchor-Won't-6296

26 National Academies of Science, 2005, Radio Frequency Identification Technologies: A Workshop Summary, janvier.

27 http://www.amrresearch.com/Content/View.asp?pmillid=17856&docid=12118

28 http://www.rfidjournal.com/article/articleview/1684/1/82/

29 Garfinkel, S. et Rosenberg B., 2005, RFID Applications, Security, and Privacy, Addison Wesley, Chapitre 27, P&G: RFID AND PRIVACY IN THE SUPPLY CHAIN, Sandy Hughes.

30 ABI Research, 2004, RFID Middleware Market Competition Heats Up, février.

31 ABI Research, 2005, Multi-Site Active & Passive RFID Deployments Drive Demand for Better Network Management Solutions, 28 avril -- http://www.abiresearch.com/products/insight/Multi-Site_Active_and_Passive_RFID_Deployments_Drive_Demand

32 ABI Research, 2005, Multi-Site Active & Passive RFID Deployments Drive Demand for Better Network Management Solutions, 28 avril -- http://www.abiresearch.com/products/insight/Multi-Site_Active_and_Passive_RFID_Deployments_Drive_Demand

33 http://www.rfidgazette.org/2005/07/union_wants_eur.html

34 On citera Katherine Albrecht, opposante énergique à la RFID, Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID, à paraître.

35 Garfinkel, S.L.; Juels, A.; Pappu, R., RFID privacy: an overview of problems and proposed solutions, Security & Privacy Magazine, IEEE, mai-juin 2005, pp 34- 43.

36 Il s'agissait de créer une norme mondiale unique qui serait plus étroitement alignée sur les normes ISO.

37 http://www.informationweek.com/story/showArticle.jhtml?articleID=60405010&tid=5978 et http://www.bdachina.com/content/en/features/analyses/B1122966499/

38 http://www.informationweek.com/story/showArticle.jhtml?articleID=60405010&tid=5978 et http://www.bdachina.com/content/en/features/analyses/B1122966499/

39 Intermec détient quelque 140 brevets fondamentaux associés à la technologie RFID.

40 Semaine du 15 août 2005.

41 Le langage PML simplifie l'échange de données entre les entreprises.

42 Dont Burt Kaliski de RSA Security, http://www.theregister.co.uk/2005/02/18/rsa_rfid/

43 A savoir la communication, la rectification et l'effacement des données.

44 Christian Floerkemeier, Roland Schneider, Marc Langheinrich, 2004, Scanning with a Purpose - Supporting the Fair Information Principles in RFID protocols, Institute for Pervasive Computing, ETH Zurich, Switzerland.

45 http://www.nap.edu/books/0309095433/html/21.html

46 http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf. La consultation publique s'est achevée à la fin de mars 2005.

47 Notamment la Directive relative à la protection des données (Directive 95/46/CE du 24 octobre 1995) et celle portant sur la Directive vie privée et communications électroniques (Directive 2002/58/CE du 12 juillet 2002).

48 Garfinkel, S. et Rosenberg B., 2005, RFID Applications, Security, and Privacy, Addison Wesley, chapitre 4, RFID and Global Privacy Policy, Stephanie Perrin.

49 Les Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de 1980 définissent le terme « maître du fichier » comme suit: 1. a) 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.

50 Cf. Annexe 3, tableau 1.

51 Cf. Annexe 3, tableau 1.

52 Le Maryland, l'Utah, et la Virginie ont déposé des projets de loi afin d'examiner plus profondément la question et de formuler des recommandations en vue d'une loi ultérieure. Le Missouri et l'Utah ont soumis un projet de loi qui exigerait que tous les produits contenant des marqueurs RFID soient convenablement étiquetés. L'Utah a présenté un autre projet de loi qui exige que des instructions soient données sur la façon de désactiver le marqueur RFID, ou un avis indiquant que celui-ci restera actif après l'achat. L'État de New York, la Virginie et l'État de Washington ont également soumis des projets de loi qui donnent un caractère confidentiel aux informations nominatives recueillies par les systèmes de péage routier automatique (comme EZ-Pass). En Californie, la législation proposée pour réglementer l'utilisation de la technologie RFID imposait aux entreprises faisant appel à des systèmes RFID 1) d'informer leurs clients qu'elles utilisent un tel système ; 2) d'obtenir leur consentement explicite avant de collecter des informations, et 3) de détacher et de détruire les marqueurs RFID attachés aux produits avant que les clients ne quittent le

magasin. Aucune de ces propositions n'a encore été votée. Source : Ministère américain du commerce : « Radio Frequency Identification – Opportunities and challenges in implementation », Washington D.C, avril 2005, p. 36 – www.technology.gov/reports/. La loi sur la RFID proposée par le Sénateur Joe Simitian sera peut-être promulguée en Californie en septembre 2005. Cette proposition, SB682 (http://www.etopiamedia.net/empnn/pdfs/sb682-1.pdf), établirait les normes d'utilisation de la technologie RFID dans les organismes publics californiens.

53 http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html

54 Garfinkel, S. et Rosenberg B., 2005, RFID Applications, Security, and Privacy, Addison Wesley, chapitre 27, P&G: RFID AND PRIVACY IN THE SUPPLY CHAIN, Sandy Hughes.

55 Garfinkel, S. et Rosenberg B., 2005, RFID Applications, Security, and Privacy, Addison Wesley, chapitre 27, P&G: RFID AND PRIVACY IN THE SUPPLY CHAIN, Sandy Hughes.

56 Voir par exemple le dispositif de « contrôle d'accès de base » (BAC) de l'OACI envisagé pour l'utilisation de la technologie RFID dans les passeports lisibles à la machine, qui a pour objectif d'empêcher l'écrémage (c'est-à-dire la lecture électronique du document à l'insu de la personne qui manipule le document) et l'interception de données lors de la communication entre la puce RFID contenue dans un passeport et un dispositif de lecture autorisé (par chiffrement des données durant la transmission), dans – Rapport technique OACI : ICP sur les documents de voyage lisibles à la machine offrant un accès CPI en lecture seule), Version 1.1, publié le 1er octobre 2004, http://www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf

57 http://www.eicar.org/rfid/information_material.htm

58 Garfinkel, S.L.; Juels, A.; Pappu, R., RFID privacy: an overview of problems and proposed solutions, Security & Privacy Magazine, IEEE, mai-juin 2005, pp 34- 43.

59 http://www.rsasecurity.com/rsalabs/node.asp?id=2115, Rapports de recherches de RSA Labs

60 Cf. Spiekermann, S., Berthold O.: Maintaining privacy in RFID enabled environments - Proposal for a disable-model, in: Robinson, Philip; Vogt, Harald; Wagealla, Waleed (Eds.): Privacy, Security and Trust within the Context of Pervasive Computing. Series: The International Series in Engineering and Computer Science, Vol. 780 http://www.wiwi.hu-berlin.de/~sspiek/SPPC_spiekermann-edited.pdf

61 Trois types d'approche ont été proposées pour « le marqueur RFID intelligent » : la méthode de hachage, la méthode de rechiffrement (sous plusieurs formes), et le protocole du « silent tree-walking ». Pour de plus amples informations, se reporter à Garfinkel, S. et Rosenberg B., 2005, RFID Applications, Security, et Privacy, Addison Wesley, Part IV Technical Solutions.

62 Notamment le blocage de la fonction de hachage (« hash lock »), le chiffrement par OU exclusif sur la voie de retour, les tiers de confiance et l'authentification LPN.

63 Garfinkel, S. et Rosenberg B., 2005, RFID Applications, Security, and Privacy, Addison Wesley, Chapitre 22, Randomization; Another Approach to Robust RFID Security, Michael Arneson, William Brandy.

64 http://www.informationweek.com/story/showArticle.jhtml?articleID=60405010

65 http://www.ofcom.org.uk/consult/condocs/wireless865_868/wireless865_868.pdf