

L'Internet des Objets

Quels enjeux pour les Européens ?

Octobre 2008

Pierre-Jean Benghozi
Directeur de recherche
Chaire Orange Innovation et régulation des services numériques
Pôle de recherche en Économie et gestion, Polytechnique – CNRS
pierre-jean.benghozi@polytechnique.edu

Sylvain Bureau
Professeur permanent ESCP-EAP - Département Information Technologie et Modélisation
Chercheur associé au Pôle de recherche en Économie et gestion, Polytechnique – CNRS
sylvain.bureau@polytechnique.edu

Françoise Massit-Folléa
Programme de recherche Vox Internet II : « Gouvernance Internet : la construction démocratique des normes »
FMSH – CSI – ENS LSH
francoise.massit@voxinternet.fr

*Avec le soutien du Ministère de l'Enseignement supérieur et de la Recherche
Délégation aux Usages de l'Internet – Internet du Futur*

Sommaire

<i>Avant-propos</i>	7
1. Définir l'Internet des Objets	9
1.1. Des définitions en voie de stabilisation	9
1.1.1 <i>Conceptuellement : l'apparition d'identités nouvelles pour les objets</i>	9
1.1.2 <i>Techniquement : extension du nommage et identifiants</i>	9
1.1.3 <i>Une proposition de définition</i>	10
1.2. L'IdO comme système de systèmes	10
1.2.1 <i>Les solutions RFID</i>	11
1.2.2 <i>Les middlewares</i>	13
1.2.3 <i>La standardisation EPCglobal</i>	13
1.2.4 <i>Une combinaison de technologies</i>	13
1.3. L'IdO comme un réseau de réseaux	14
1.3.1 <i>L'informatique ubiquitaire : réseau réel sur réseau virtuel</i>	14
1.3.2 <i>Une extension du système des codes barres</i>	14
1.4. L'IdO comme système socio-technique	15
2. Importance et enjeux de l'Internet des Objets	17
2.1. Un relais de croissance pour l'économie	18
2.1.1 <i>La reconfiguration des secteurs de l'Internet et des télécoms</i>	18
2.1.2 <i>L'apport de nouveaux services pour l'industrie en général</i>	18
2.1.3 <i>Une opportunité de réduire la fracture Nord/ Sud</i>	19
2.1.4 <i>Un des nouveaux vecteurs de la compétition internationale</i>	21
2.2. Les enjeux de gouvernance	21
2.2.1 <i>L'irruption des puces RFID dans la vie quotidienne</i>	21
2.2.2 <i>Apparition de nouveaux usages et besoin de nouveaux arbitrages</i>	21
2.2.3 <i>La nécessité de favoriser un déploiement massif et rapide</i>	22
2.2.4 <i>La nécessité de préserver la neutralité du réseau</i>	22
2.3. Une gouvernance « multilatérale, transparente et démocratique »	23
2.4. Garantir la protection des individus et des entreprises	23
3. Évolutions techniques de l'Internet des Objets	25
3.1. Principaux besoins technologiques	25
3.1.1 <i>Garantir la performance des solutions en contexte d'usage</i>	25
3.1.2 <i>Assurer la pérennité des solutions</i>	26
3.1.2.1 <i>Garantir la flexibilité</i>	26
3.1.2.2 <i>Garantir l'interopérabilité</i>	26
3.1.2.3 <i>Garantir la sécurité</i>	27
3.1.3 <i>Concevoir une gestion efficiente des données</i>	27
3.1.3.1 <i>Une masse de données sans précédent</i>	27
3.1.3.2 <i>Une logique d'indexation à réinventer</i>	28
3.2. Des solutions technologiques en concurrence	28
3.2.1 <i>Les différentes formes de RFID</i>	28
3.2.2 <i>Les solutions alternatives à la RFID</i>	29
3.3. L'avancée de la standardisation dans le secteur de l'IdO	29
3.3.1 <i>La dépendance vis-à-vis des standards existants</i>	29
3.3.2 <i>Un standard de standards</i>	31
3.3.3 <i>La granularité des standards</i>	31
3.3.4 <i>L'interopérabilité des standards</i>	31

4. Quelles performances, quels investisseurs et quels modèles économiques ?	33
4.1. Les facteurs de performance	33
4.1.1 Des performances à mesurer à plusieurs niveaux	33
4.1.2 La recherche de gains d'échelle	33
4.2. Des opportunités de marché pour les nouveaux acteurs	34
4.2.1 Des progrès tirés par la demande	34
4.2.2 L'amélioration des processus industriels	34
4.2.3 L'articulation des différents niveaux de performance	35
4.3. Comment et qui doit investir ?	35
4.3.1 Prendre en compte la complexité des investissements	35
4.3.2 Définir des solutions pour chaque niveau d'investissement	36
4.3.3 Développer de nouveaux services pour les consommateurs	36
4.3.4 Garantir le financement dans l'ensemble de la chaîne de valeur	37
4.3.5 Favoriser les usages publics de l'IdO	37
4.4. Une redéfinition des chaînes de valeur	38
4.4.1 La chaîne de valeur industrielle	38
4.4.2 Les nouveaux entrants dans la chaîne de valeur	38
4.4.3 Des spécificités vis-à-vis du secteur de l'électronique	38
4.4.3.1 Les intermédiaires d'information	39
4.4.3.2 L'ancrage territorial	39
4.4.3.3 L'enjeu central de l'interopérabilité	39
4.5. Une demande en constante évolution	41
5. Diffusion et mise en œuvre : une complexité nouvelle	43
5.1. Comprendre et gérer les risques de l'IdO	43
5.1.1 Gérer les risques environnementaux	43
5.1.2 Prévenir les risques éthiques et juridiques	43
5.1.3 Éviter les risques économiques	43
5.1.4 Maintenir un niveau de protection élevé en Europe	44
5.2. Écouter et informer l'opinion sur l'IdO	44
5.2.1 La crainte d'une utilisation abusive des données	44
5.2.2 L'inquiétude des citoyens relative à leur vie privée	45
5.3. Protéger la vie privée et les données sensibles	45
5.3.1 Protéger la vie privée	45
5.3.2 Différencier RFID ouverte et RFID fermée	46
5.3.3 Rendre possible le « silence des puces »	46
5.3.4 Protéger les données sensibles des entreprises	46
5.4 Les réponses techniques et les autres	47
5.4.1 Les <i>Privacy Enhancing Technologies</i> et leurs limites	47
5.4.2 Un nouveau marché de la confiance	47
5.4.3 La gestion des identités multiples des individus	47
6. La nécessité d'une gouvernance adaptée	49
6.1. La gouvernance technique	50
6.1.1 La gouvernance des normes de l'IdO	50
6.1.2 La gouvernance des fréquences de l'IdO	51
6.2. La gouvernance des infrastructures réseaux	51
6.2.1 Identifier les types de réseaux	51
6.2.2 Protéger le principe de neutralité (<i>end to end</i>)	52
6.2.3 Contrôler la gestion des ressources critiques	52

6.3. La vie privée, entre technique, droit et éthique	53
6.3.1 Des cadres réglementaires en évolution	53
6.3.1.1 La consultation publique européenne sur la RFID	53
6.3.1.2 L'encadrement du commerce électronique	54
6.3.1.3 La protection des données personnelles	54
6.3.1.4 Les enjeux « informatique et libertés » de l'IdO	55
6.3.2 Des incertitudes persistantes	56
6.3.2.1 Quel est « le champ » des données personnelles ?	56
6.3.2.2 Qui contrôle les fichiers ?	56
6.3.2.3 Encourager les « bonnes pratiques » des professionnel	56
6.3.2.4 Définir des droits et des infractions spécifiques à l'IdO ?	57
6.3.2.5 Poser les bases éthiques d'une régulation internationale	57
 <i>Pour conclure.</i>	 59
La nécessité d'aller vers la structuration d'un pôle de recherche européen.	
 <i>Bibliographie sélective</i>	 61

Avant-propos

L'Internet accueille aujourd'hui des milliards de connexions et d'échanges qui en font l'outil le plus puissant jamais inventé pour le partage de l'information. En quelques décennies, il est devenu le moteur de profondes transformations dans la vie des entreprises, des individus et des institutions. Cet élan n'est pas près de cesser et dans tous les pays ingénieurs et techniciens, industriels et sociétés de services, chercheurs de toutes disciplines et responsables politiques sont déjà en train de dessiner l'Internet du Futur¹.

La perspective est celle d'un monde de connexion encore plus dense, entre les hommes mais aussi avec les objets - une connexion permanente et de plus en plus invisible, qui engendre autant de craintes qu'elle est porteuse de promesses. Elle pose sous de nouvelles formes la question des relations entre innovation et marché, entre ressources techniques et applications de services, mais aussi entre sécurité et liberté. Elle perpétue et renforce le besoin d'une gouvernance « transparente, multilatérale et démocratique » qui a irrigué les débats du Sommet mondial sur la société de l'information². L'enjeu est de répondre aux incertitudes tant industrielles que réglementaires et aux préoccupations éthiques d'accessibilité, de diversité culturelle et de protection des libertés.

Entre avancées technologiques et méconnaissance des usages, entre harmonisation des standards et aléas de la compétition économique, l'Union européenne est confrontée à trois défis majeurs :

- Comment articuler de manière partagée, durable et à moindre coût, des réseaux et des applications diversifiés ?
 - Comment guider l'innovation et favoriser la croissance économique ?
- Comment faire en sorte qu'un réseau de réseaux conçu comme « ubiquitaire » ne soit pas excessivement intrusif ?

Le 7^{ème} programme-cadre européen de recherche sur les technologies de l'information et de la communication marque une étape importante. Il est largement consacré aux réseaux et services du futur³. Quatre aspects essentiels y sont abordés :

- les nouvelles infrastructures de réseaux (très haut débit, sans fil, mobile),
 - le développement des logiciels et des plateformes de services,
 - l'exploration des technologies 3D Media,
- l'intégration des puces RFID (*Radio Frequency Identification systems*) et des adresses IP

conduisant à ce qu'on appelle « l'Internet des Objets⁴ ».

En fonction des acteurs, et de leurs intérêts parfois divergents, il est difficile de trancher entre « révolution » ou « évolution » technique. Le web sémantique, les nanotechnologies, les *Next*

¹ European Future Internet Portal : <http://www.future-internet.eu/>,

² www.itu.int/wsis/index-fr.html

³ ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/futint-book_en.pdf

⁴ Par commodité, nous utiliserons généralement par la suite l'acronyme *IDO*.

Generation Networks vont renouveler dans un proche avenir la physionomie de l'Internet. Mais la présente étude a choisi de partir des usages, avérés ou émergents, pour questionner ces mutations. C'est pourquoi elle est consacrée à l'Internet des Objets qui a largement entamé son déploiement, qui focalise un très grand nombre de recherches en cours, aussi bien en sciences et techniques qu'en sciences sociales et, surtout, qui suscite les interrogations les plus pressantes dans le débat public.

La manière dont l'IdO est appréhendé aujourd'hui est très largement structurée par les infrastructures disponibles (réseaux et protocoles Internet), les processus de suivi déjà existants (en particulier les codes-barres) ainsi que les acteurs en place (développeurs, tiers de confiance). Mais son développement ne saurait se limiter aux seules questions techniques de la RFID⁵. Il soulève des enjeux économiques et sociaux, mais aussi politiques, philosophiques, cognitifs, juridiques et éthiques dont la perception, par le grand public comme par les autorités, n'est pas exempte d'ignorance et d'amalgames. Le panorama que nous proposons s'inscrit de plain-pied dans une perspective pluridisciplinaire, pour permettre de porter en parallèle l'ensemble de ces questionnements. Il se situe également dans une perspective d'action, pour concevoir et promouvoir une gouvernance équilibrée et ainsi réussir le développement de l'IdO en Europe.

Après avoir défini l'Internet des Objets (chapitre 1), nous tenterons de comprendre en quoi ses enjeux sont cruciaux (chapitre 2), puis d'évaluer son stade de développement (chapitre 3), en insistant sur la construction de la standardisation. Nous nous interrogerons sur les conditions d'émergence et de succès du marché de l'IdO (chapitre 4) et nous analyserons les représentations qui conditionnent sa mise en œuvre, à la fois pour les industriels, les citoyens et les gouvernements, en mettant en relief la problématique de la protection de la vie privée « *privacy* » (chapitre 5). Le dernier chapitre (6) s'attachera aux principales questions qui doivent être gérées politiquement, en Europe et au delà, pour construire un Internet des Objets profitable, acceptable et « gouvernable ».

*

⁵ *Radio Frequency Identification*.

Chapitre 1. Définir l'Internet des Objets.

L'internet des objets est une notion complexe. Entre les puces RFID, les solutions de nommage ou middlewares, l'internet des objets est composé de nombreux éléments complémentaires ayant chacun leurs propres spécificités. Pour mieux appréhender la notion, nous proposons de définir les grands principes de l'IdO tels qu'ils apparaissent aujourd'hui à la lecture des recherches et rapports réalisés sur la question.

1.1. Des définitions en voie de stabilisation.

Si tout le monde (ou presque) est d'accord pour dire que l'IdO est, sinon l'Internet du Futur, du moins une dimension fondamentale de l'Internet de demain, il n'existe pas de définition standard, unifiée et partagée de l'Internet des Objets. Certaines définitions insistent sur les aspects techniques de l'IdO, tandis que d'autres se concentrent plutôt sur les usages et les fonctionnalités. Il faut réussir à exprimer ce que représente l'internet des objets tout en restant accessible aux non-experts, et suffisamment concret pour représenter son impact dans la vie quotidienne.

1.1.1 Conceptuellement : l'apparition d'identités nouvelles pour les objets.

Certains définissent l'IdO comme des « objets ayant des identités et des personnalités virtuelles, opérant dans des espaces intelligents et utilisant des interfaces intelligentes pour se connecter et communiquer au sein de contextes d'usages variés »⁶. D'autres font l'hypothèse que l'IdO représente une révolution car il permet de connecter les gens et les objets n'importe où, n'importe quand, par n'importe qui. Ces définitions, qui mettent l'accent sur la dimension ubiquitaire de l'IdO, personnifient les objets en leur attribuant intelligence et capacité de communiquer. Elles ne reflètent pas encore la dimension concrète liée aux usages de l'IdO.

1.1.2 Techniquement : une extension du nommage et convergence des identifiants

Techniquement, l'IdO est une extension du système de nommage internet et traduit une convergence des identifiants numériques⁷ au sens où il est possible d'identifier de manière unifiée des éléments d'information numérique (adresses URL de sites web par exemple) et des éléments physiques (comme une palette dans un entrepôt, ou encore un mouton dans un cheptel). Mais l'identification est directe grâce à l'utilisation d'un système d'identification électronique (puces RFID, processeur et communication Bluetooth etc.) Il n'y a pas besoin de saisir manuellement le code de l'objet. Le réseau s'étend jusqu'à lui et permet ainsi de créer une forme de passerelle entre les mondes physique et virtuel.

⁶ Anonyme. 2008. *Internet of Things in 2020. Roadmap for the Future*, 1.1 ed.: 27: Info D.4 Networked Enterprise & RFID; Info G.2 Micro & Nanosystems in co-operation with the working group RFID of the EPOSS. p. 4.

⁷ Pour reprendre le terme utilisé par S. Le Pallec, <http://2005.jres.org/paper/70.pdf>

1.1.3 Une proposition de définition.

Dans cette étude, nous proposons de croiser les approches purement techniques et les approches centrées sur les usages en définissant l'Internet des Objets comme *un réseau de réseaux qui permet, via des systèmes d'identification électronique normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques et ainsi de pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s'y rattachant.*

Dans ce chapitre, nous essaierons de clarifier cette définition. Nous verrons dans un premier temps que l'IdO est un système de systèmes composé d'innovations technologiques récentes et de solutions déjà anciennes. Nous aborderons ensuite la notion de réseau de réseaux et la capacité de l'IdO de prolonger l'Internet dans le monde physique. Enfin, nous montrerons qu'une approche uniquement technique est insuffisante car l'IdO est aussi un système socio-technique qui prendra des formes différentes selon les choix qui seront faits par nos sociétés.

1.2. L'IdO comme système de systèmes.

L'IdO ne se résume certainement pas à une technologie spécifique. Il désigne plutôt diverses solutions techniques (RFID, TCP/IP, technologies mobiles etc.) qui permettent d'identifier des objets, de capter, stocker, traiter, et transférer des données dans les environnements physiques mais aussi entre des contextes physiques et des univers virtuels. Actuellement, l'enjeu majeur n'est pas tant d'inventer de nouvelles technologies que de perfectionner celles qui existent déjà⁸, de les connecter, et de les intégrer .

Nous listons ci-après les principales classes de solutions nécessaires au fonctionnement de l'IdO.

Plutôt que d'en décrire tous les éléments, nous focaliserons l'analyse sur trois composantes considérées comme critiques : les solutions RFID, les solutions logicielles « *middleware* » et le réseau EPCglobal.

⁸ Les technologies de l'IdO ne sont pas toutes récentes. Le système d'identification est ainsi vieux de plusieurs décennies dans le cas des codes barres ou des puces RFID.

Tableau 3 : principaux systèmes technologiques nécessaires au fonctionnement de l'IdO

Type de systèmes	Identification (y compris lecteurs)	Capteurs	Connexion	Intégration	Traitement de données	Réseaux
Enjeux	Reconnaître chaque objet de façon unique et recueillir les données stockées au niveau de l'objet.	Recueillir des informations présentes dans l'environnement pour enrichir les fonctionnalités du dispositif.	Connecter les systèmes entre eux.	Intégrer les systèmes pour que les données soient transmises d'une couche à l'autre.	Stocker et analyser les données pour lancer des actions ou pour aider à la prise de décisions.	Transférer les données dans les mondes physiques et virtuels.
Technologies anciennes (exemples)	Codes barre, solutions RFID simples	Thermomètre, hydromètre...	Câbles, ...	Middlewares...	Excel, ERP, CRM...	Internet, Ethernet...
Technologies récentes (exemples)	Solutions RFID complexes, Surface Acoustic Waves, puces optiques, ADN	Capteurs miniaturisés nanotechnologies	Bluetooth, Near Field Communication (NFC), WiFi...	Middlewares évolués	Datawarehouse 3D (compatible avec les puces RFID), Web sémantique...	Réseau EPCglobal...

1.2.1 Les solutions RFID.

Il existe aujourd'hui de très nombreux ouvrages et rapports qui présentent le fonctionnement de ces solutions et nous nous contenterons ici d'une courte synthèse. Les solutions RFID font partie de la classe des technologies d'identification automatique. Elles sont en général utilisées pour fournir une identité électronique à un objet inanimé ou animé, par exemple dans le secteur de la logistique. Le sigle RFID recouvre un ensemble de technologies et d'applications très variées qui dépendent de paramètres tels que la portée, la bande de fréquence utilisée, le prix, l'encombrement, ou encore la consommation d'énergie. Par ailleurs, au-delà des seules étiquettes (*tags* ou puces), le système RFID est constitué de marqueurs/capteurs, de lecteurs, et de logiciels pour traiter les informations collectées⁹.

Si le principe de fonctionnement est toujours le même, quels que soient les contextes et la complexité d'utilisation des systèmes, il faut néanmoins différencier les types de système en place – fermé ou ouvert – et les types de puces implémentées – passives, actives ou semi-passives.

⁹ En pratique, le lecteur envoie une onde électromagnétique. Cette vague crée un courant électrique dans l'antenne du tag. Le courant électrique produit alors de l'énergie au niveau du tag (dans le cas des puces passives, car une puce active dispose d'une batterie qui lui permet d'avoir sa propre source d'énergie). Les données sont transmises au lecteur via des radiofréquences. Ensuite elles sont téléchargées sur un serveur et deviennent alors disponibles et accessibles via le système d'information d'une organisation ou directement sur l'Internet.

Nous présentons dans les tableaux ci-après ces différents systèmes :

Tableau 4 : boucles RFID ouvertes et fermées

Propriétés	Boucle fermée	Boucle ouverte
Définition	Les puces restent confinées au système.	Le système communique avec d'autres systèmes et échange des données. Les puces circulent au sein de ces différents systèmes.
Enjeux et facteurs critiques	Forte sécurisation (accès interdit sans autorisation)	Interopérabilité Coût élevé
Cas d'utilisation	Chaîne logistique intra-organisationnelle	Chaîne logistique inter-organisationnelle (service IdO <i>post Point of Sale</i>)

Tableau 5 : type de puces RFID utilisées

Propriétés	Puce passive	Puce active	Puce semi-passive
Caractéristiques	Aucune batterie.	Batterie intégrée à la puce avec un transmetteur et un récepteur actifs. Le plus souvent dotée de capteurs.	Batteries mais aucun transmetteur. Souvent dotée de capteurs (ou sensors).
Coût	Min. 5/10 cts d'euros	Quelques euros	Plus ou moins 1 euro
Enjeux et facteurs critiques	<ul style="list-style-type: none"> - Taille des puces réduite - Coût très faible - Lecture de distance faible - Fréquence - Taux de lecture¹⁰ élevé - Environnement non hostile (métallique/ non aqueux) 	<ul style="list-style-type: none"> - Consommation d'énergie à limiter pour augmenter la durée de vie de la puce - Lecture de distance moyenne à grande - Sécurisation forte - Interface avec les capteurs performante 	<ul style="list-style-type: none"> - Coût faible - Consommation d'énergie des capteurs faible - Lecture de distance moyenne - Sécurisation forte - La puce devrait pouvoir rester utilisable comme puce passive une fois la batterie épuisée
Exemples d'utilisation	Logistique : biens de grande consommation	Logistique : produits de soins coûteux	Logistique : chaîne du froid

Pour différencier les solutions RFID, il faut également distinguer les fréquences. En résumé, il existe quatre types de fréquence : basse (125 kHz), haute (13,56 MHz), ultra-haute (800-930 MHz) et hyper (2,45 et 5,8 GHz). Les puces passives ne sont jamais utilisées avec les hyperfréquences. Par ailleurs, il faut savoir que le débit de données a tendance à augmenter avec l'augmentation des fréquences et qu'à l'inverse, plus la fréquence est élevée, plus il est difficile de traverser un milieu.

¹⁰ Le taux de lecture se définit par le nombre de réponses de puces RFID qui peuvent être reçues et décodées par un interrogateur en une seconde (cf. Hawrylak, P. J., Mickle, M. H., & Cain, J. T. 2008. RFID tags. In L. Yan & Y. Zhang & L. T. Yang & H. Ning (Eds.), *The Internet of Things. From RFID to the Next-Generation Pervasive Networked Systems*: 1-32. New York: Auerbach Publications, p. 6).

1.2.2 Les *middlewares*.

Ces logiciels ont un rôle critique dans les solutions RFID car ils permettent de gérer l'interface entre les différents systèmes. Dans le cas des solutions RFID, ils assurent l'extraction des données RFID depuis les lecteurs. Ils permettent également de filtrer les données, de les agréger et de les transmettre après distillation aux systèmes d'information d'entreprise du type *Enterprise Resource Planning* (ERP), *Supply Chain Management* (SCM), ou encore *Customer Relationship Management* (CRM).

1.2.3 La standardisation EPCglobal.

EPCglobal est né d'un accord passé entre l'AutoID Center, EAN international et l'*Uniform Code Council* en juillet 2003. EPCglobal Inc. est l'organisme de référence pour les industriels. Il est piloté par GS1 qui est lui-même un organisme de standardisation privé à but non lucratif, mandaté et gouverné par les utilisateurs des standards qu'il définit et non pas par les fournisseurs de solutions. La mission d'EPCglobal est d'assurer le déploiement du système EPC à travers le monde. Ce système promeut différents standards dont un système d'identification. Il a également défini plusieurs générations de solutions. Actuellement, EPCglobal soutient le développement de la Class-1 Gen-2 (certifiée ISO depuis 2006). Avec ce type de solution, il est théoriquement possible de lire 1000 puces RFID par seconde et au moins 100 puces par seconde dans des environnements hostiles. Ces puces sont inscriptibles à un rythme de 30 puces par seconde dans des conditions optimales et de 5 puces par seconde dans un environnement hostile. La fréquence retenue est la bande 860-960 MHz. EPCglobal a également mis en place un réseau qui s'appuie sur les technologies Internet, comme nous le verrons ci-après.

1.2.4 Une combinaison de technologies.

L'IdO n'est pas une technologie mais bien un système de systèmes qui permet une modularité et une certaine flexibilité. L'interopérabilité entre les systèmes et l'intégration de tous les composants produisent une complexité forte. La capacité à gérer les interfaces sera déterminante pour que l'IdO devienne un véritable réseau de réseaux. Le cas de la grande distribution illustre parfaitement à la fois les potentialités de l'IdO et toute la difficulté de mise en œuvre d'un tel système. En effet, il faut dans un premier temps déployer une solution au niveau local, dans chaque entrepôt et magasin du distributeur (premier système), puis il est indispensable que les données recueillies soient intégrées au système d'information de l'entreprise pour être traitées et analysées par des outils tels qu'un ERP (deuxième système). Il faut par ailleurs, pour profiter pleinement d'une infrastructure de ce type, déployer des dispositifs chez les fournisseurs qui soient interopérables avec la solution du distributeur (troisième système). Enfin, il faut également prévoir un dispositif technique qui puisse fonctionner chez les consommateurs pour permettre des applications domotiques comme la détection de produits périmés dans le réfrigérateur qui assure automatiquement le lancement d'une nouvelle commande auprès du distributeur (quatrième système)¹¹.

¹¹ Les conséquences d'une telle complexité en matière d'organisation de la production et du marché seront examinées au chapitre 4 *infra*.

1.3. L'IdO comme un réseau de réseaux.

1.3.1 L'informatique ubiquitaire : brancher le réseau réel sur le réseau virtuel.

Aujourd'hui, les recherches sur Internet restent cantonnées aux documents (textes, images, sons) qui y circulent. Grâce aux technologies des *Discovery Services*, l'IdO permettra d'étendre le champ des recherches. Car, tout comme un site web a son adressage unique (l'URL), chaque objet pourra être doté d'une identification électronique unique qu'il sera possible de lire et de transmettre via un protocole dans le réseau Internet. L'IdO ne se limite donc pas au monde en ligne et permet potentiellement d'attribuer à chaque objet un *double virtuel*, copie simplifiée des caractéristiques de l'objet présent dans un contexte physique. Ces caractéristiques sont multiples et d'un point de vue purement théorique, elles pourraient être presque infinies. Dans la plupart des cas, il s'agira cependant de définir la nature de l'objet, ses fonctionnalités, les services qu'il offre, sa position dans l'espace, l'historique de ses déplacements, son âge, etc. Pour effectuer ce lien entre physique et virtuel, le dispositif technique doit donc modéliser des contextes réels et les « virtualiser ». Certains utilisent la notion d'*informatique ubiquitaire* pour désigner les solutions qui permettent ce passage. L'objectif des solutions ubiquitaires est d'être en mesure de détecter et de répondre à des changements de contexte. Elles doivent permettre de capturer, stocker et manipuler un contexte pour rendre un service adapté dans une situation bien précise et pour une personne particulière¹². Le terme générique d'informatique ubiquitaire reste encore assez vague et désigne en fait la plupart des technologies présentées au début de ce chapitre : web sémantique, solutions RFID, *Service Oriented Architecture*, etc.

1.3.2 Le développement de EPCglobal : une extension du système des codes barres.

À ce jour, si plusieurs plateformes existent pour permettre de créer cette nouvelle forme de réseau qui fait le lien entre le physique et le virtuel, une seule solution, le réseau EPCglobal, semble être suffisamment normalisée et reconnue pour pouvoir être utilisée au niveau mondial. L'architecture de ce réseau fut conçue par l'Auto-ID Center et développée par la suite par l'EPCglobal. Avec ce nouvel Internet, les données sont portées sur le réseau. Pour ce faire, celui-ci mobilise les puces RFID qui ont une identification unique non ambiguë, héritière enrichie du code-barres, nommée *Electronic Product Code* (EPC). Par ailleurs, les autres données relatives aux objets sont stockées et accessibles via l'Internet que l'on connaît aujourd'hui. Le réseau EPCglobal dispose par ailleurs de l'*Object Naming Service* (ONS) et de l'*EPCInformation Service* (EPCIS). L'ONS attribue une référence à l'information de l'objet sauvegardé via le réseau EPC, ce qui permet de retrouver les objets RFID à travers le réseau (son fonctionnement est calqué sur le *Domain Name System* utilisé pour l'Internet). EPCIS offre quant à lui une interface pour accéder aux données RFID mémorisées. Pour échanger des données RFID entre le réseau EPCglobal et des applications externes, un langage XML est utilisé. L'avantage du réseau EPCglobal sur d'autres solutions est de permettre l'utilisation de puces peu onéreuses et une architecture au périmètre ajustable. Il est important de noter que pour tracer les objets RFID dans le réseau EPCglobal, une des solutions

¹² Pour plus d'informations, voir : Preuverneers, D. & Berbers, Y. 2008. Internet of Things: A Context-Awareness Perspective. In L. Yan & Y. Zhang & L. T. Yang & H. Ning (Eds.), *The Internet of Things. From RFID to the Next-Generation Pervasive Networked Systems*: 287-307. New York: Auerbach Publications.

proposées (Discovery Service) demande à ce que le mouvement de ces objets soit publié de manière continue auprès d'un – ou plusieurs – serveurs-référence de mises à jour.

L'IdO, par sa capacité à élargir progressivement la notion de réseau de réseaux en construisant un réseau de capteurs pour des objets, contribuera également à structurer des types de réseaux inédits en tissant entre objets et individus des formes de structuration aussi nouvelles que celles qu'ont constitué les communautés dans l'Internet. Pour comprendre ces évolutions, il est donc essentiel de ne pas limiter l'analyse à la dimension technique du phénomène mais de considérer ses composantes sociales ainsi que les possibles interactions entre ses utilisateurs.

1.4. L'IdO comme système socio-technique.

Les processus d'appropriation en local seront déterminants quant à la forme et aux modalités que prendront les usages de l'IdO. Ils emprunteront certainement d'autres formes que celles qui sont aujourd'hui imaginées par les chercheurs et les entreprises. D'ores et déjà certaines innovations dépassent la plupart de nos prévisions. Ainsi, pour ne donner qu'un exemple, une société japonaise a développé un système (*Sekai camera*) qui permet, via un iPhone, de prendre connaissance du menu d'un restaurant, ou des caractéristiques d'un produit en pointant le téléphone en direction de la boutique ou de l'objet. Dès que le téléphone capte les données, un petit film ou un message apparaît sur l'écran de l'iPhone. Il n'est même plus nécessaire de lancer une recherche pour accéder à l'information, il suffit de pointer son téléphone vers la vitrine d'un restaurant¹³.

Le défi est alors de définir des principes et des cadres de régulation qui permettront d'orienter les usages, ou tout au moins d'empêcher certains comportements dangereux pour les libertés individuelles et les démocraties, tout en préservant les capacités d'innovations issues de l'IdO.

Nous reviendrons sur cette question essentielle dans le dernier chapitre de cette étude.

¹³ ¹³ http://www.forbes.com/2008/09/10/tonchIdOt-camera-iphone-tech-personal-cx_bc_0910iphone.html?feed=rss_news

Chapitre 2. Importance et enjeux de l'Internet des Objets.

La montée en puissance des applications de l'IdO peut s'observer dans plusieurs secteurs ou registres des activités sociales : des plus personnelles (animaux familiers, santé) aux plus industrielles (gestion logistique). Le large spectre des applications d'ores et déjà observables indique que nous sommes aujourd'hui face à une tendance bien ancrée. Le poids et l'intérêt économiques de certaines applications contribuent à stimuler les investissements de recherche et développement et à installer durablement les utilisations de l'IdO. Ensuite, par son caractère très global, l'IdO est porté par des mouvements profonds de la société : la convergence grandissante, la communication en réseau et les systèmes d'information, le développement de la mobilité et la constitution d'environnements socio-techniques autonomes et centrés sur l'individu, le renforcement de la traçabilité et des processus de contrôle des activités et des personnes. Ainsi, l'IdO sous-tend à la fois un renforcement des outils de simulation et de modélisation et l'amélioration des performances dans la réalité physique, grâce aux possibilités offertes dans la manipulation, le traitement et l'enrichissement des objets physiques identifiés.

Dans un cas, il construit des passerelles entre le monde de l'Internet et le monde réel, en connectant les objets et les informations qui les concernent (identification, localisation, état). Dans le second cas, il prolonge les promesses de l'Internet et des systèmes d'information existants en remplaçant l'observation et la saisie d'informations par l'intégration même des objets dans le réseau. Cette convergence s'exprime aujourd'hui sous des noms différents (réalité augmentée, machines communicantes ou réseaux ubiquitaires notamment) qui expriment la variété des registres dans lesquels se déploie l'Internet du Futur.

Pour comprendre l'importance et les enjeux associés de l'IdO, il paraît utile de revenir sur certains traits saillants qui marquent ce mouvement vers l'Internet du futur. Sans nous attarder sur les aspects plus strictement économiques ou technologiques qui seront traités plus avant, nous rappellerons plutôt ici quelques caractéristiques des sociétés contemporaines. Il est important de garder à l'esprit que l'Internet du futur s'inscrit dans une trajectoire socio-technique déjà ancienne. Les nouvelles directions où il se déploie restent marquées par certaines orientations initiales de l'Internet qui pèsent sur l'infrastructure et les configurations actuelles. Les choix d'aujourd'hui guideront, pour plusieurs années encore, les trajectoires de développement, les structures de gouvernance ainsi que les usages de l'IdO.

2.1. Un relais de croissance pour l'économie

2.1.1 La reconfiguration des secteurs de l'Internet et des télécoms.

L'IdO aura sans aucun doute des effets importants sur la reconfiguration de l'Internet et des services associés : rôle accru des moteurs de recherche, développement des intermédiations électroniques, portabilité et interopérabilité des différents registres d'applications, renforçant d'autant les dynamiques économiques et de développement afférents. Les applications existantes montrent d'ailleurs comment certaines activités radicalement nouvelles peuvent être amenées à se développer, autour des services de sécurité ou de santé par exemple.

À l'heure où le degré d'équipement de télécommunications et de connexion traditionnelle atteint sans doute son niveau de saturation dans les pays développés, l'IdO appelle des investissements importants pour soutenir la recherche et le développement, pour perfectionner les puces, les marqueurs et les lecteurs, pour créer et diffuser de nouveaux services. Ces investissements et ces développements sont opérés au niveau des États, des entreprises comme des individus ; ils devraient constituer un relais de croissance sérieux pour l'Internet. De telles innovations en matière d'usage et de technologies s'observent dans les pays occidentaux comme dans les pays émergents. Ils constituent à ce titre un axe stratégique pour les opérateurs de télécommunications. La multiplication d'applications associées à l'IdO pourrait d'une part contribuer à la valorisation des architectures à haut débit (*Ultra Broad Band*) encore liées à des incertitudes quant aux modes de valorisation des nouveaux réseaux et à la nature des applications à même d'appuyer leur mise en œuvre. Elle pourrait également, dans le cadre d'utilisations élargies disséminées sur tous les territoires, soulever des problèmes importants de bande passante, du fait du flux des connexions et de leurs redondances. Le cas de la Chine est de ce point de vue intéressant : 73 millions d'utilisateurs, soit 29% des internautes, se connectent en effet via leur téléphone mobile et ce chiffre connaît une croissance bien plus importante que celui des connexions par ordinateur portable¹⁴.

2.1.2 L'apport de nouveaux services pour l'industrie en général.

Néanmoins, alors que ce sont les apports de l'IdO pour l'industrie ou pour le consommateur qui sont le plus volontiers mis en avant, il importe de rappeler qu'un des facteurs d'intérêt le plus puissant de l'IdO tient sans doute, au premier chef, à l'enjeu majeur de développement qu'il peut représenter pour l'industrie et l'économie au niveau mondial.

¹⁴ D'après China Internet Network Information, cité par *The Economist*, "The meek shall inherit the web" 4/09/08, http://www.economist.com/science/tq/displaystory.cfm?story_id=11999307.

2.1.3 Une opportunité de réduire la fracture Nord-Sud.

Si l'IdO peut constituer un relais de développement dans les économies européennes et, plus largement, occidentales, il faut souligner qu'il pourrait offrir également un moyen de contribuer à réduire la fracture Nord Sud en créant des opportunités pour développer des coopérations renouvelées avec les pays en développement. L'IdO est à même d'apporter des solutions inédites à certains problèmes spécifiques aux pays en croissance ou disposant d'infrastructures administratives insuffisamment robustes. En ouvrant des formes nouvelles d'automatisation des dispositifs d'information et de suivi, il peut offrir des substituts à des processus de gestion, de gouvernance et de coordination mal consolidés. L'IdO peut trouver, dans ces pays, des opportunités de croissance inattendues, à l'image de celles que l'on peut déjà y constater pour d'autres technologies de l'information et de la communication, telles que le courrier électronique ou la téléphonie mobile.

Ce développement pourrait être facilement appuyé par les organismes internationaux dans la mesure où plusieurs de leurs champs d'intervention sont directement concernés par les applications envisageables. C'est le cas de la santé et de la prévention des dangers associés à la contrefaçon des médicaments ; c'est aussi celui de l'amélioration de la gestion de l'eau, ou encore de l'anticipation des risques climatiques et géologiques. Ces exemples ne sont bien sûr pas fournis au hasard mais correspondent chacun à des expérimentations ou des solutions existantes.

Domain	No. of cases
Retail, Consumer goods	400
Financial, Security and Safety	316
Passenger and Public transport	278
Leisure and Sports	228
Land and Sea Logistics, Postal	177
Healthcare	142
Manufacturing	135
Animals and Farming	81
Books, Libraries and Archiving	76
Military	43
Laundry	10
Other	4

Tableau 1 : Répartition des applications RFID par grands domaines sociétaux.

Source : IdTechEx 2006,

cité dans *RFID Technologies : Emerging Issues, Challenges and Policy Options*, JRC Reports 2007.

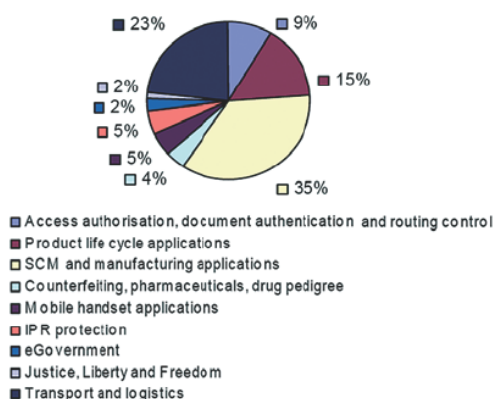


Figure 1 : Projets RFID par types d'applications

Source : *Radio-Frequency Identification tags Portfolio of European research, 2006*

	Application examples in the Private sector	Application examples in the Public sector
Asset utilisation	<ul style="list-style-type: none"> Container management (e.g. small load carriers in the automotive sector) Loading equipment management (e.g. for gears in the automotive supplier sector) Management of dollies at airports Fleet management 	<ul style="list-style-type: none"> Waste management: Container management Health: Location of medical equipment at hospitals
Asset monitoring and maintenance	<ul style="list-style-type: none"> Machine maintenance Tool box maintenance (e.g. for the maintenance of aircraft) Maintenance of parts built in aircraft Smart home applications 	
Item flow control in processes	<ul style="list-style-type: none"> Tagging of parts along the supply chain to correlate information on the tagged item to process steps Goods movement control Quality control of goods Tracing drugs in the pharmaceutical value chain Tracking finished goods for the purpose of diversion control 	<ul style="list-style-type: none"> Health: Tracking of medication from the pharmacy to the hospitalised patient Health: Tracing blood bottles Administration: Document management
Inventory audit	<ul style="list-style-type: none"> Real-time location systems for finished vehicles in the automotive sector Automation of warehouse management Automated sorting and counting of inventory Checking of ingoing and outgoing goods Baggage handling at airports Livestock tagging 	<ul style="list-style-type: none"> Defence: Ammunition management Education: Lending system in libraries Exhibition in museums Science: Tagging animals and plants for research purposes
Theft control	<ul style="list-style-type: none"> Car keys (immobilisers) Electronic Article Surveillance (EAS) systems Tracking products along the supply chain to minimise theft 	
Authentication	<ul style="list-style-type: none"> Persons: <ul style="list-style-type: none"> Company badges Ski passes Event ticketing Sports: recording time during a competition Objects (counterfeiting control): <ul style="list-style-type: none"> Proof of authenticity of spare parts (e.g. in the aviation sector) Proof of authenticity of drugs Proof of authenticity of luxury goods 	<ul style="list-style-type: none"> E-Passports, identity cards Health: Patient authentication for the monitoring of medication in hospitals Leisure/sports: recording time during a competition Traffic: Tolling systems Traffic: Speed control Transport: Access control cards for public transport
Payment systems	<ul style="list-style-type: none"> Tolling systems Contactless cards for financial transactions 	<ul style="list-style-type: none"> Transport: Payment cards for public transport

Tableau 2 : Applications RFID dans les secteurs privés et publics.

Source : *Working Party on the Information Economy : RFID applications, impacts and country initiatives, DSTI/ICCP/IE (2007) 13/FINAL, OCDE 2008*

2.1.4 Un des nouveaux vecteurs de la compétition internationale

En la matière, les investissements importants de la Chine (dans les technologies mais aussi dans les processus même de standardisation) sont intéressants à souligner. Ils indiquent clairement d'une part l'enjeu économique très important associé à l'IdO par ce pays à forte croissance, d'autre part comment cette technologie y est également envisagée comme support de développement en soi.

Le travail de synthèse élaboré à l'OCDE¹⁵ souligne, de manière plus générale, l'importance du marché potentiel des puces RFID et sa croissance, à la fois forte et rapide. Il constate cependant la difficulté de fournir des données précises sur l'impact de ces technologies. Les raisons tiennent à la fois au caractère émergent de la technologie et à l'absence d'études d'impact agrégées au niveau des différents pays. Selon les sources, les estimations du marché des solutions RFID varient ainsi de quelques centaines de millions à plusieurs milliards d'euros. Peu de travaux précis existent donc, mais ceux qui ont été menés, (notamment en Allemagne¹⁶) confirment l'importance de l'impact de l'IdO en termes de productivité tout comme la grande variété des situations observables entre les différents marchés.

2.2. Les enjeux de gouvernance.

2.2.1 Le changement d'échelle lié à l'irruption des puces RFID dans la vie quotidienne.

Du point de vue technique, l'importance des perspectives actuelles de l'Internet du Futur s'explique par l'importance de la miniaturisation et de la réduction des coûts associées aux nanotechnologies et, surtout, par les possibilités d'utilisation désormais permises par la mise en réseau et le couplage, via Internet, avec les systèmes d'informations. Si ces perspectives apparaissent radicales, elles ne sont pas totalement nouvelles. On rappellera que les premières puces RFID ont été développées dès la deuxième guerre mondiale et que leur forme moderne est apparue dans les années 80, avant même que l'Internet ne se développe massivement. C'est la généralisation du couplage entre objets physiques, systèmes d'information et réseaux de communication qui explique le caractère résolument nouveau des développements actuels ainsi que leurs conséquences, souvent occultées par l'accent privilégié mis sur la dimension strictement technique (fréquences, alimentation, etc...).

2.2.2 L'apparition de nouveaux usages et le besoin de nouveaux arbitrages.

Cette dimension informationnelle doit conduire à repenser les équilibres économiques et techniques associés à l'IdO et, par voie de conséquence, sa gouvernance. Les risques associés au développement des puces RFID reposent sur des problématiques complexes. Par exemple, la protection des données personnelles ne relève pas seulement de la réglementation mise en place au niveau des normes. Elle repose aussi sur des questions techniques telles que le droit au « silence des puces, » c'est-à-dire la possibilité ou non de les désactiver. Et elle se rapporte aussi à la manière dont les informations collectées seront mises en réseau et réappropriées, dans des séquences

¹⁵ *Working Party on the Information Economy, RFID applications, impacts and country initiatives*, DSTI/ICCP/IE(2007)13/FINAL, OCDE 2007.

¹⁶ OECD (2007), *RFID Implementation in Germany: Challenges and Benefits*, www.oecd.org/dataoecd/19/23/39693586.pdf, accessed 1 February 2008.

d'applications successives difficilement maîtrisables en tant que telles. Parallèlement, la tentation de disposer prochainement de puces à bas prix pourrait conduire certains acteurs à s'en saisir avant que des pratiques « robustes » de protection des données personnelles et industrielles n'aient pu être développées.

Ces questions ne sont pas neuves. L'IdO risque de redonner une actualité nouvelle à certains points sensibles de l'Internet qui avaient déjà soulevé des débats aigus, ces dernières années, entre les différentes parties prenantes. Nous allons rapidement évoquer les plus importants d'entre eux : les modèles économiques de l'Internet, la gouvernance et la protection des individus.

2.2.3 La nécessité de favoriser un déploiement rapide et massif.

Du point de vue économique, le succès même de l'Internet avait soulevé deux grandes catégories de problèmes que l'IdO risque de rencontrer à nouveau. Les premiers tenaient à la capacité d'assurer un déploiement assez rapide et d'atteindre la masse critique suffisante pour permettre le lancement conjoint d'applications à tous les niveaux d'une même filière. Le cas de la logistique dans la grande distribution alimentaire montre, à cet égard, que la capacité de déployer la technologie sur l'ensemble de la *supply chain* est déterminante pour assurer sa pérennité et en retirer tous les bénéfices. Cette rapidité de mouvement suppose de pouvoir mobiliser des investissements importants, à même de soutenir la construction d'équipements, le développement d'applications massives ainsi que la capitalisation d'entreprises innovantes. Des dynamiques spéculatives et l'éclatement futur des bulles d'investissements sont dès lors à craindre si les retours économiques attendus ne sont pas au rendez-vous, ou pas aussi rapidement qu'espéré. L'autre point économique sensible résulte du découplage qui tend à s'opérer entre d'un côté, les nécessités attachées à la gestion des infrastructures et réseaux de télécommunications, et de l'autre, la dynamique de développement des applications.

2.2.4 Parallèlement, la nécessité de préserver la neutralité du réseau.

Le succès massif de certaines entreprises telles que Google suscite, chez les opérateurs et fournisseurs d'accès, le sentiment que de telles réussites devraient se traduire par une participation au financement des infrastructures. Ils tendent de ce fait à remettre en cause ce qui constituait jusque-là l'un des principes fondateurs de l'Internet : à savoir sa neutralité et le traitement indifférencié des données ou contenus y circulant. Il faut s'attendre à ce que la question se pose rapidement en matière d'IdO. En effet, ce dernier ne peut que renforcer l'écart déjà existant entre les modèles économiques à la base des infrastructures et ceux des utilisateurs ou secteurs applicatifs, qu'il s'agisse d'industriels intégrant l'IdO dans leurs processus de production et leur logistique, ou de fournisseurs de services grand public.

2.3 La nécessité d'une gouvernance « multilatérale, transparente et démocratique. »

La question des formes de la gouvernance d'ensemble du système constitue un autre des grands enjeux de l'IdO.

La gouvernance de l'Internet est actuellement marquée par une polarisation autour d'organismes de normalisation technique. Elle résulte de l'établissement d'un consensus entre opérateurs et acteurs privés, organismes publics et communautés d'utilisateurs. Envisagé d'abord à un niveau national, le processus a été déployé au niveau international. Il répartit les responsabilités entre différentes structures qui prennent chacune un élément en charge : normes techniques d'interface, gestion des noms de domaine, sécurité et évolutions de l'architecture, etc.

Cette gouvernance n'a pas été sans soulever des débats très vifs : sur son degré effectif d'autonomie par rapport aux grands pays ou aux grands opérateurs de télécommunications, ou sur la délégation à des structures privées des ressources-clés de l'Internet (gestion des noms de domaine génériques, notamment).

Plus encore que l'Internet « traditionnel », l'IdO touche des dimensions éminemment stratégiques et des informations critiques. De ce fait, il appelle des formes renforcées de coordination et de gouvernance au niveau national ou régional. En même temps que l'on maintient une véritable *lingua franca* et une interopérabilité de l'IdO, il s'agirait donc d'assurer une certaine « régionalisation » de l'IdO pour permettre à chaque État d'exercer ses prérogatives de souveraineté.

2.4 Garantir la protection des individus et des entreprises.

Enfin, le dernier enjeu important de gouvernance de l'IdO concerne la protection des individus et des entreprises. Les applications de l'IdO soulèvent de manière récurrente la question de la *privacy* ou protection des données personnelles, dans la mesure où elles touchent très directement l'intégrité même des individus : dans leurs actions, dans les objets qu'ils manipulent ou dans leur simple présence. Cela pourrait entraîner une accentuation radicale des difficultés déjà rencontrées sur l'Internet (traçabilité, interconnexion des informations...) et en particulier dans certaines applications récentes (réseaux sociaux, moteurs de recherche, Internet mobile...). Comme l'ont montré, ces dernières années, les réactions suscitées par le développement du *Digital Rights Management* (DRM) et les réglementations associées, la question suppose en effet, de plus en plus, une faculté et une volonté de contrôle des modes d'usage, et donc un *empowerment* des consommateurs.

Les débats suscités par l'IdO autour des données personnelles risquent de se voir renforcés par les différences de traitement de la protection des individus selon les systèmes juridiques : faut-il prioritairement protéger les citoyens de l'action des gouvernements ou de celle des opérateurs privés ? La capacité d'observer des actions dans l'espace public doit-elle rendre *de facto* les informations publiques et accessibles ? Les architectures techniques seront particulièrement

déterminantes dans la manière dont ces questions se poseront (en ouvrant la possibilité de désactiver les puces ou de contrôler les informations véhiculées) ... mais les réponses dépasseront, en tout état de cause, les seuls enjeux techniques.

L'accent légitimement mis sur la question de la *privacy* ne doit pas occulter une autre dimension importante de la protection des données : celles qui ne concernent pas uniquement l'individu ou la personne mais aussi les données sensibles des entreprises. En effet, se posent en la matière des problèmes inédits tenant à l'intégration d'informations qui portent sur les processus de production ou de circulation des objets. L'accès à de telles informations, même partiel, est souvent stratégique pour des partenaires industriels en compétition ou impliqués dans des relations commerciales. On peut dès lors s'interroger pour savoir si la protection des données industrielles ne risque pas d'appeler, dans le futur, une structuration de règles et d'organismes de régulation spécifiques, tout comme les opportunités de croisement des bases de données individuelles avaient suscité, dans le passé, la création de la Commission Nationale Informatique et Libertés (CNIL) et de ses équivalents européens.

Les chapitres qui suivent ont pour objectif d'éclairer ces différentes dimensions de l'Internet des Objets.

Chapitre 3. Évolutions techniques de l'Internet des Objets.

Même si de nombreux progrès ont été réalisés, avant de pouvoir utiliser l'IdO comme l'Internet il reste encore un certain nombre de points à résoudre. Dans ce chapitre, nous listerons dans la première partie les principales nouveautés technologiques qui limitent le développement de l'IdO, puis nous aborderons les problématiques de concurrence entre technologies (deuxième partie) mais aussi les principales démarches de standardisation en cours (troisième partie).

3.1. Principaux besoins technologiques.

Trois enjeux majeurs se posent actuellement : améliorer la performance des solutions, permettre une meilleure interopérabilité des systèmes en garantissant un niveau de sécurité optimal et enfin concevoir une gestion efficace des données.

3.1.1 Garantir la performance des solutions en contexte d'usage.

Il faut distinguer trois types de performance pour bien comprendre les problématiques actuelles : premièrement, la performance technique pure dans un cadre de laboratoire, deuxièmement, la performance technique dans un environnement réel, et troisièmement, l'équation technico-économique de la solution. Sur le premier aspect, les progrès ont été tout à fait impressionnants depuis quelques années. Ainsi, il est désormais possible de trouver des solutions RFID qui fonctionnent même immergées dans l'eau (grâce notamment aux technologies NFC - *Near Field Communication* - et aux ultra-hautes fréquences) ou dans des environnements très métalliques¹⁷. De la même façon, les distances de lecture et les taux de lecture ont considérablement augmenté depuis une décennie. Enfin, la consommation d'énergie requise par les solutions RFID a nettement diminué, même si sur ce point d'énormes progrès restent encore à accomplir pour obtenir des dispositifs qui fonctionnent sur la longue durée et avec un impact écologique faible (cette question est tout particulièrement sensible pour les puces actives ou semi-passives).

À l'inverse, la fiabilité des solutions dans certains contextes d'usage complexe reste à améliorer. Pour ne donner qu'un exemple, une recherche menée par un laboratoire de l'Université d'Amsterdam a récemment montré que les radiofréquences émises par les solutions RFID pouvaient produire des interférences portant atteinte au bon fonctionnement de certains dispositifs médicaux critiques tels que les pacemakers, les ventilateurs ou encore les appareils utilisés pour les dialyses¹⁸.

Enfin, les solutions qui fonctionnent avec une grande fiabilité restent trop chères pour permettre une large diffusion. Il est bien sûr possible de trouver des puces RFID passives à moins de 10

¹⁷ van Liehout, M., Grossi, L., Spinelli, G., Kool, L., Pennings, L., Stap, R., Veugen, T., van der Waaij, B., & Borean, C. 2007. *RFID Technologies: Emerging issues, Challenges and Policy Options*. In I. Maghiros & P. Rotter & M. van Liehout (Eds.): 278. Seville: Institute for Prospective Technological Studies, JRC European Commission. P. 44

¹⁸ van der Togt, R., Jan van Liehout, E., Hensbroek, R., & al., e. 2008. Electromagnetic Interference From Radio Frequency Identification Inducing Potentially Hazardous Incidents in Critical Care Medical Equipment. *JAMA.*, 24(299): 2884-2890.

centimes d'euros sur le marché, mais elles ne seront dotées ni d'un système très sécurisé, ni d'un taux de lecture performant. Pour favoriser une diffusion rapide, il faut donc concevoir des solutions qui respectent mieux les équations technico-économiques des industriels, car à ce jour le coût de changement est souvent trop lourd à supporter. Concrètement, il faudra réussir à produire des solutions moins onéreuses, non seulement au niveau des puces mais aussi de l'ensemble des composants du système (lecteurs, antennes, middlewares, etc.), qui permettent un stockage de données suffisant sur une surface toujours plus petite, et tout cela avec un taux de lecture performant. Pour les puces actives, il faudra également diminuer la consommation d'énergie pour avoir des batteries qui durent plus longtemps – au moins le temps de la durée de vie de l'objet que la puce doit identifier¹⁹. Enfin, il faudra résoudre la question du recyclage des puces et de l'impact écologique des solutions RFID.

3.1.2 Assurer la pérennité des solutions.

Si l'on dépasse la question de la seule performance d'un système, il faut distinguer trois classes de problèmes : premièrement, la flexibilité (la solution mise en œuvre peut évoluer avec le contexte), deuxièmement l'interopérabilité (la solution mise en œuvre peut communiquer avec d'autres solutions), troisièmement la sécurité (la solution est sécurisée à la fois pour les données mais aussi pour les personnes qui l'utilisent).

3.1.2.1 Garantir la flexibilité.

Il ne sert à rien d'acquiescer une solution onéreuse qu'il faudra changer au bout de quelques mois. Dans un contexte de chaîne logistique, il est essentiel que l'ensemble du dispositif puisse évoluer et s'adapter. Il est par exemple impensable d'avoir une solution qui fonctionne par beau temps mais pas lorsqu'il pleut (l'humidité affecte en effet la performance des solutions RFID). De la même façon, si les procédures évoluent, il faut que le système soit suffisamment flexible pour intégrer de nouvelles règles sans remettre en cause l'ensemble du dispositif à la fois au niveau du matériel et des logiciels. De la même façon, si l'entreprise décide de changer d'ERP ou de le faire évoluer, cela implique-t-il le changement du *middleware* ou de toute ou partie de la solution RFID ? Ce cas un peu théorique illustre néanmoins l'enjeu lié à l'évolutivité des solutions RFID.

3.1.2.2 Garantir l'interopérabilité.

Le succès de l'IdO dépendra aussi de l'interopérabilité des systèmes. À un premier niveau, il est essentiel que tous les composants d'une solution soient interopérables. Il faut par exemple que le lecteur RFID soit compatible avec les puces utilisées. Pour résoudre cette question, il est nécessaire de créer une boucle ouverte où les différentes parties prenantes pourront intervenir. Dans ce cas, il faut trouver des solutions qui s'adaptent à des contextes hétérogènes pour garantir un fonctionnement fiable tout au long de l'utilisation. La question de l'interopérabilité se pose également quand on envisage la convergence entre les solutions RFID et les solutions mobiles. À ce jour, la résolution de ce problème reste encore très incertaine. Les actions des entreprises de

¹⁹ Une solution est de transformer une puce active ou semi-passive en puce passive si la batterie est épuisée.

télécommunication seront bien évidemment déterminantes, mais il semble que leur stratégie sur cette question ne soit pas encore pleinement arrêtée.

Comme nous le montrerons plus loin, la question de l'interopérabilité dépasse largement la seule dimension technique. Elle a en effet des incidences juridiques (avec en particulier le problème de la prolifération des brevets), mais aussi économiques (avec toute la question des royalties) et de gouvernance (nous aborderons notamment cet aspect en précisant le rôle de la Commission européenne et des principales institutions de standardisation).

3.1.2.3 Garantir la sécurité.

Il faut également mettre en œuvre un système qui assure une sécurisation des données. Si une solution RFID a été mise en œuvre entre un client et un fournisseur, il faut certes que les deux parties partagent un certain nombre d'informations en commun mais dans le même temps, des données utiles pour le fournisseur n'ont pas nécessairement à être transmises au client. Dans le cas du secteur de la santé, ce type de question est évidemment très sensible car les informations détenues sur chacun des patients ne doivent pas être accessibles par toutes les parties (assureurs, industrie pharmaceutique, employeurs...). Cette problématique n'est certes pas nouvelle mais le dispositif technique de l'IdO peut fortement modifier à la fois les possibilités de stockage de données (quantité et localisation du stockage qui pourra se faire en local, de façon distribuée) et d'accès aux données (il est possible de lire les données contenues dans une puce à distance, aux dépens de son utilisateur). Des systèmes techniques de sécurisation des données et, au delà, un cadre qui oriente et empêche certaines pratiques dommageables ou illicites devront être mis en œuvre. Enfin, le problème des effets des radiofréquences sur le corps humain devra faire l'objet d'études spécifiques (ces questions seront abordées dans les deux derniers chapitres).

Les verrous et leviers techniques sont très nombreux et nous n'avons proposé qu'une brève description des facteurs critiques. D'autres points, tels que les relations de l'IdO avec les nanotechnologies ou encore la robotique, auraient également pu être abordés.

3.1.3 Concevoir une gestion efficace des données.

3.1.3.1 Une masse de données sans précédent.

Selon Venture Development Corporation, Wal-Mart générerait près de 7 téraoctets de données chaque jour s'il y avait une puce sur chaque article vendu²⁰. Que faire de ce « déluge de données » ? Les solutions actuelles utilisées notamment en *Business Intelligence* sont-elles en mesure de gérer correctement à la fois la quantité et la complexité de ces données ? Les données issues des puces RFID sont particulières car elles doivent permettre de prendre en compte à la fois l'espace (la localisation) et le temps (avec notamment la durée de vie des objets). Pour que ces données fassent sens, il faut dans un premier temps les « nettoyer » pour éviter les redondances (mais il ne faut pas non plus oublier, sous prétexte qu'il y a beaucoup de données, que dans certains cas, le problème est plutôt la perte de données critiques !). Il faut également réfléchir à leur « agrégation » car, en

²⁰ Gonzalez, H. & Han, J. 2008. RFID Data Warehousing and Analysis. In L. Yan & Y. Zhang & L. T. Yang & H. Ning (Eds.), *The Internet of Things. From RFID to the Next-Generation Pervasive Networked Systems*: 53-80. New York: Auerbach Publications, p.54.

fonction de la granularité requise, il n'est pas toujours nécessaire d'avoir accès à toutes les données. Dans certains cas, il sera par exemple préférable d'avoir une information au niveau d'une palette et non pas au niveau d'un objet. Enfin, il faudra être capable de structurer ces données. De nouveaux *datawarehouses* (entrepôts de données) devront être inventés pour permettre aux managers d'avoir des tableaux de bord qui puissent les aider à décider. Actuellement, s'il existe des recherches et quelques applicatifs²¹ qui apportent des éléments de solution, le chemin à parcourir est encore long pour permettre une gestion en continu avec une intégration en temps réel des données s'inscrivant dans des ensembles géographiquement distribués.

3.1.3.2 Une logique d'indexation à réinventer.

Au-delà de ces problématiques d'entreprises, on peut s'interroger sur le moteur de recherche qui sera adapté à l'IdO. La question est encore peu abordée dans les travaux existants, mais les outils de recherche seront un enjeu tout aussi déterminant dans l'IdO que dans l'Internet actuel. Les évolutions de *l'Entreprise Search* sont déjà une indication de l'importance potentielle de ces nouveaux marchés. Leur développement suppose sans doute de résoudre des enjeux techniques inédits, associés notamment aux moteurs 2D et 3D.

Les questions qui viennent d'être évoquées ne peuvent pas se comprendre avec une logique purement technique. L'histoire des technologies l'a montré, les solutions les plus performantes ne s'imposent pas toujours. Pour saisir les phénomènes à l'œuvre, il est essentiel d'analyser la concurrence qui existe entre différentes solutions technologiques.

3.2. Des solutions technologiques en concurrence.

3.2.1 Les différentes formes de RFID.

Au-delà du type de puces et de radiofréquences, les solutions RFID disponibles sur le marché sont très nombreuses et se trouvent en concurrence. Les intervenants dominants, qu'ils soient fabricants de puces ou de capteurs, éditeurs de *middleware*, intégrateurs, ou encore cabinets de conseil, poussent leurs technologies, leurs standards ou leurs services. Par ailleurs, de grands utilisateurs (*lead users*) orientent le marché par le volume de leurs commandes tels que Wal-Mart, Metro ou encore le Département de la Défense, qui mobilisent les solutions RFID avec comme objectif principal une reconfiguration efficiente de leur propre chaîne de valeur, et non le développement d'un standard plus général. Dans le cas de la grande distribution, ces solutions doivent notamment améliorer l'intégration verticale de la chaîne logistique, faciliter les systèmes bancaires de paiement, ou encore améliorer la connaissance des clients pour mettre en place des politiques marketing ciblées. Outre leur impact sur le marché, ces grands comptes ont également eu un rôle majeur depuis plusieurs années en finançant les recherches sur le secteur (le cas des Auto-ID labs est significatif), ou en participant directement aux consortia qui travaillent sur la définition des outils et des standards communs (sur ce point, les secteurs agricole et de la santé sont très illustratifs). Finalement, les *pure players* de la RFID sont rares, même si certains

²¹ *ibidem*.

commencent à se développer de manière significative comme TagSys, Verichip ou encore Alien Technology. Le marché reste en effet largement dominé par des acteurs traditionnels et, de ce fait, les solutions RFID développées semblent en partie correspondre à des marchés cloisonnés. Ainsi les acteurs sur le marché des puces fonctionnant à hautes fréquences ne sont pas toujours les mêmes que ceux opérant sur le marché des puces à basses fréquences. Ceci étant, certains doutent du caractère durable d'un tel découpage et évoquent une segmentation du marché fondée sur des questions d'usages plus que des paramètres techniques.

3.2.2 Les solutions alternatives à la RFID.

Nous avons fait l'hypothèse selon laquelle les puces RFID seront indispensables au bon fonctionnement de l'IdO. Mais d'autres solutions pourraient être envisageables. Intel, entreprise qui a investi des sommes importantes dans la R&D liée à la RFID, a récemment vendu toute cette activité à un fabricant californien de lecteurs RFID (Impinj). Cette information n'indique bien sûr pas que l'avenir des RFID soit compromis, car cette opération ne remet pas totalement en cause l'implication d'Intel sur le marché des RFID, mais plutôt les modalités de son investissement (l'accord avec Impinj s'est fait par échange d'actions). Toutefois l'avenir de l'IdO ne sera pas nécessairement lié à celui de la RFID. De nombreux laboratoires et industriels travaillent en effet sur des solutions alternatives qui pourraient supplanter à l'avenir les solutions RFID. Il s'agit par exemple de systèmes d'identification acoustiques, de l'usage des micro-ondes, de systèmes optique, de la détection de l'ADN, ou encore du marquage logiciel. Certains évoquent aussi l'intégration des puces dans la conception même des objets, ce qui modifierait sensiblement les problématiques RFID telles que nous les envisageons à ce jour.

Au cœur de cette concurrence entre technologies, les grands acteurs industriels et publics opèrent des choix stratégiques via les organismes de standardisation.

3.3. L'avancée de la standardisation dans le secteur de l'IdO.

La question des standards est au croisement de problèmes techniques, économiques, juridiques et politiques. Plutôt que de faire une revue exhaustive de ces questions ou une liste des standards importants pour l'IdO, nous centrerons l'analyse sur trois questions critiques : la dépendance des standards actuels aux standards passés, la difficile conciliation entre pertinence et équité des standards retenus et enfin l'enjeu de l'interconnexion des standards.

3.3.1 La dépendance vis-à-vis des standards existants.

Les standards de l'IdO reprennent les grands principes qui sont au fondement de l'Internet (DNS, TCP/IP, etc.) et du système du code-barres. Les principaux acteurs qui interviennent sur ces standardisations sont les mêmes²². Ainsi le protocole TCP/IP et le langage XML restent toujours des références pour l'IdO. L'ONS est un système issu du DNS qui assure le nommage de l'Internet. De la même façon, les logiques de l'*Electronic Product Code* dérivent de celles utilisées pour le système du code-barres.

²² Comme nous l'avons indiqué EPCglobal a ainsi réuni l'EAN international et l'Uniform Code Council, deux institutions qui étaient au cœur du processus de standardisation du code barre.

Cet héritage de l'IdO par rapport à l'Internet et au système de code-barres pourrait limiter techniquement certains développements et applications. Par ailleurs, si des milliards de données supplémentaires devaient transiter par le réseau, la capacité de l'Internet à y faire face est mise en doute à la fois pour des questions physiques liées aux infrastructures (en raison notamment de la capacité des routeurs) et des problèmes logiques (les principes pensés pour l'Internet ne seraient plus viables à long terme pour l'IdO).

Pour répondre à ces nouveaux défis et aux enjeux de sécurité et de fiabilité de l'IdO, certains pensent que des mesures incrémentales peuvent suffire. Le passage de l'IPv4 à l'IPv6 (*Internet Protocol* version 6) est une illustration de cette démarche d'évolution au sein du même paradigme de l'Internet historique. Ce nouveau protocole permettra d'augmenter considérablement la quantité d'adresses disponibles (on passe de $4,29 \cdot 10^9$ adresses à $3,4 \cdot 10^{38}$) mais aussi d'améliorer le fonctionnement des routeurs ou encore de renforcer la sécurité.

À l'inverse, différents groupes²³ prônent le dépassement des standards passés en saisissant l'opportunité de l'IdO pour repartir de zéro (*Clean State*) et repenser complètement les grands principes de fonctionnement de ce nouvel Internet. Entre évolution et révolution, les impacts techniques, économiques et plus largement politiques ne seront pas les mêmes.

3.3.2 Un standard de standards.

Aujourd'hui, la normalisation des réseaux est le fait soit de groupements industriels privés, soit d'organismes de normalisation internationaux. Pour les groupements industriels, EPCglobal est un des acteurs dominants, à la fois public et privé, qui sous-traite les certifications de conformité aux standards EPC à une entreprise privée (MET). AIM Global et Global Data Synchronisation sont quant à eux des structures coopératives privées déterminantes pour la mise en relation des applications, des objets et des firmes. De leur côté, ISO, ITU et ETSI forment la base du réseau des acteurs publics de la normalisation dans le secteur des télécommunications. W3C, IETF, IEEE sont à l'origine des standards de l'Internet. L'ICANN est l'organisme qui assure aujourd'hui la gestion des noms de domaine sur Internet.

Mais l'IdO aura des implications telles sur nos sociétés qu'il est important que les standards retenus fassent l'objet d'un consensus entre acteurs privés et publics, et que leurs choix ne soient pas guidés par les seules logiques économiques mais prennent aussi en compte les questions de vie privée, de souveraineté, etc.

De même, il est important que les standards de l'IdO ne soient pas limités aux normes définies par quelques grands acteurs, ou ne soient pas fragmentés par zones géographiques.

La standardisation représente un enjeu et un verrou technique déterminants à la fois par la nature des choix techniques effectués (fréquence, puissance, encodage...) et par la diversité des niveaux et des registres de standardisation. Les acteurs qui interviennent sur ces questions sont très divers et les modèles alternent entre les solutions propriétaires et privées, volontaires et consensuelles (modèle des normes industrielles), public *de jure* (modèle des télécommunications) et

²³ Un projet de recherche important a notamment été initié à Stanford : <http://cleanslate.stanford.edu/>

l'autorégulation. Mais l'objectif doit rester de parvenir à développer des standards ouverts en promouvant un dialogue transparent entre les différents acteurs. C'est une condition nécessaire au développement de la concurrence et à l'harmonisation des solutions sur le marché.

3.3.3 La « granularité » des standards.

L'enjeu de la granularité des standards est important. Il consiste à ce que chaque standard soit viable à la fois au niveau international, national, régional mais également au niveau de chaque industrie spécifique.

La question de la granularité est tout aussi importante pour éviter le risque de fragmentation, faute d'anticipation des interfaces avec les systèmes techniques associés comme les nanotechnologies, les capteurs ou encore autour des ONS. Il est essentiel de la penser en amont, sous peine de ralentir ou empêcher le développement d'applications innovantes, source de création de valeur.

À ce jour, certains standards commencent à s'imposer grâce à l'action d'organisations comme EPCglobal, mais il ne faudrait pas que les autres parties prenantes soient écartées des décisions. Il est essentiel de réfléchir à l'équité du processus de standardisation. On peut notamment s'interroger sur le rôle que devrait jouer l'Europe pour participer aux choix de ces standards.

3.3.4 L'interopérabilité des standards.

Au-delà de la question de l'élaboration de standards, il est fondamental de penser à leur interopérabilité, et ce d'autant plus que l'IdO est un système de systèmes qui nécessite un niveau d'interopérabilité élevé. Actuellement, certaines avancées notables ont eu lieu sur cette question pour les technologies dites NFC (*Near Field Communication*). Les solutions NFC permettent, via un système sans fil, de connecter deux dispositifs électroniques à courte distance pour les faire interagir (ce type de système est tout particulièrement utilisé au Japon comme moyen de paiement). Depuis le début de l'année 2008, les membres de l'ETSI (*European Telecommunications Standards Institute*) ont ainsi sélectionné le protocole du logiciel qui permet de contrôler la communication entre le dispositif NFC et une carte SIM. Ce type de standardisation est critique pour envisager la production à grande échelle. De la même façon, des évolutions très positives ont eu lieu sur le marché de la téléphonie mobile ces derniers temps avec l'adoption par de nombreux acteurs de poids (AT&T, China Mobile, Vodafone, Verizon, Motorola, Nortel, etc.) du standard LTE (*Long Term Evolution*). Cette tendance est une clef pour mieux préciser les contours de la 4G (quatrième génération) car jusqu'à présent un flou relatif entourait la définition de ce standard, ce qui pouvait décourager les investisseurs.

Au-delà des avancées dans le marché de la téléphonie mobile, le rôle des institutions publiques reste fondamental pour promouvoir des standards qui garantissent l'interopérabilité. À travers IDABC, la Commission européenne défend ainsi le principe de standard ouvert²⁴. L'objectif est d'assurer

²⁴ Un rapport de 2004 de l'IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens) définit le standard ouvert de la façon suivante : *“the standard is adopted and will be maintained by a not-for-profit organisation, and its ongoing development occurs on the basis of an open decision-making procedure available to all interested parties (consensus or majority decision etc.). The standard has been published and the standard specification document is available either freely or at a nominal charge. It must be permissible to all to copy, distribute and use it for no fee or at a nominal fee.*

une gouvernance du standard par une organisation sans but lucratif qui permette à l'ensemble des parties prenantes de gérer de façon démocratique la création et l'évolution du standard. Par ailleurs, la diffusion d'un tel standard est large et gratuite (ou alors au coût nominal). Enfin, la copie et la distribution se font également sans entraves (absence de licences, notamment). La Commission européenne défend et finance par exemple le projet BRIDGE (*Building Radio Frequency IDentification solutions for the Global Environment*)²⁵, initié en 2006, qui permettra de mettre en place un standard ouvert fondé sur l'application développée par EPCglobal pour l'utilisation de solutions RFID aptes à gérer la traçabilité des produits tout au long de la chaîne logistique.

The intellectual property - i.e. patents possibly present - of (parts of) the standard is made irrevocably available on a royalty-free basis. There are no constraints on the re-use of the standard." (IDABC (2004): "European Interoperability Framework for Pan-European eGov-ernment Services", p. 9).

²⁵ <http://www.bridge-project.eu/>

Chapitre 4. Quelles performances, quels investisseurs et quels modèles économiques ?

Un des facteurs-clé de succès de l'Internet des Objets tient à ce que son développement offre des opportunités de rentabilité et d'amélioration de la qualité de services dans presque tous les registres d'activités et à plusieurs niveaux, aussi bien local que global. Son enjeu économique doit donc être envisagé selon deux axes différents mais complémentaires. Le premier tient à la manière dont l'amélioration des performances facilite les conditions d'investissements d'une organisation déterminée et peut être valorisée. Le second correspond aux opportunités de croissance offertes par la transformation des modèles d'affaires et les nouvelles relations entre parties prenantes et acteurs économiques contribuant aux mêmes activités.

4.1 Les facteurs de performance.

4.1.1 Des performances à mesurer à plusieurs niveaux.

Dans le cadre des usages « traditionnels » de la RFID, les facteurs de performance de l'IdO ne sont pas uniques mais ils apparaissent à la fois au niveau d'une organisation et d'une filière d'activité. La variété des sources de productivité et de performance associées à la mise en œuvre de l'Internet des Objets trouve sa source à la fois dans l'amélioration de la qualité de service ou des performances accessibles aux individus et consommateurs, et dans l'augmentation de l'efficacité des processus industriels des entreprises. Dans le premier cas, on peut identifier des retours sur investissement positifs dans le cadre d'un projet spécifique. Cela facilite le déploiement mais en limite l'ampleur : l'installation de puces sur des palettes de produits agroalimentaires pour réduire les coûts de logistique et de manutention en est un exemple. Dans d'autre cas, les facteurs de performance tiennent à la capacité de rationaliser globalement la gestion de l'ensemble des processus de production pour permettre une meilleure intégration des flux physiques et des systèmes d'informations, en s'interfaçant notamment avec les applications d'ERP ou de CRM. Enfin, la capacité de dégager une rentabilité dans l'utilisation de l'IdO peut résulter, plus fondamentalement, de la constitution de nouveaux modèles d'affaires et de nouvelles opportunités de facturation : en vendant par exemple les informations récoltées, ou en proposant de nouveaux services à valeur ajoutée.

4.1.2. La recherche de gains d'échelle.

Les gains visés sont plus ambitieux (mais souvent plus difficiles à atteindre) quand ils visent une efficacité « collaborative » et une amélioration de la productivité d'ensemble. Les gains de performance se répartissent dans ce cas sur l'ensemble d'une filière ou d'une industrie. Pour toutes les technologies d'information et de communication, un tel déploiement ne peut être que progressif et transversal pour assurer une bonne intégration et optimisation des flux physiques et des flux d'information : du fabricant au distributeur, du distributeur aux clients, en passant par les réseaux de transporteurs, les plateformes d'intermédiation et de transaction. La question dans ce cas est classique en économie : elle porte sur la manière dont les gains réalisés – la rente - sont

partagés et répartis entre l'ensemble des parties prenantes et peuvent contribuer aux investissements nécessaires. L'IdO peut se heurter, en l'occurrence, à une forme de banalisation qui conduirait chacun des acteurs économiques à attendre que ce soient ses partenaires qui fassent les investissements nécessaires. Les gains de productivité pourraient alors connaître de grandes disparités au sein des mêmes filières, conduisant de ce fait à une forme de « paradoxe de la productivité » : une multiplication de l'usage des puces, sans réelle valeur ajoutée globale au bénéfice de la société et de l'économie, les gains étant soit noyés dans des stratégies d'attente sous-optimales, soit captés au bénéfice de d'un nombre restreint de firmes.

4.2. Des opportunités de marché pour les nouveaux acteurs.

Nous l'avons noté, la montée en puissance de l'IdO tient à la convergence de plusieurs facteurs de performance. Les puces désormais disponibles couplent une capacité de mémoire très largement supérieure aux technologies existantes ou aux codes barres, avec des prix de revient en baisse constante, qui rendent désormais leur intégration au processus industriel envisageable à court terme. Cette mise en œuvre et ce déploiement bénéficient, en outre, de l'affaiblissement du prix des dispositifs de lecture et des applications de traitement : en effet ces coûts sont très directement indexés sur la montée en puissance des réseaux de communications (fixes et mobiles) et l'enrichissement parallèle des terminaux (ordinateurs, téléphones mobiles...).

4.2.1 Des progrès tirés par la demande.

La variété de ces facteurs de performance explique pour une grande part le large spectre des applications couramment évoquées aujourd'hui en matière d'IdO. La première source de performance identifiable ne se situe sans doute pas au niveau de l'offre mais à celui de la demande. Il s'agit de l'amélioration des services ou des applications proposées aux individus, qui leur permet de bénéficier d'économies directes, en termes de temps ou d'argent, et justifie que ces gains puissent, dans certains cas, susciter des facturations ou échanges monétaires. On trouve de telles situations dans la gestion de flux de transports tels que les péages autoroutiers ou les accès de parking ; on peut aussi évoquer des utilisations telles que le suivi des groupes lors de manifestations sportives comme les marathons. D'autres exemples souvent mentionnés concernent les cartes individuelles couplant paiement et contrôle d'accès : qu'il s'agisse de transports en commun, de bibliothèques, de stations-service, de bâtiments publics ou de participation à des événements ou spectacles. Enfin certaines applications spécifiques, plus inédites, sont associées au domaine de la sécurité : voitures communicantes, traçabilité des animaux familiers, suivi et aide aux personnes fragiles ou dépendantes.

4.2.2 L'amélioration des processus industriels.

Un second registre de performance de l'IDO résulte de l'augmentation d'efficacité des processus industriels. Là encore, les exemples sont très nombreux. Un premier champ d'amélioration touche à la logistique. L'automatisation des processus de repérage et de gestion des flux de produits permet de normaliser le suivi et la sécurisation des conteneurs, d'optimiser la gestion et de la réception des palettes, le suivi des stocks ou la gestion des flottes de véhicules. La rationalisation

des opérations de maintenance s'inscrit dans le prolongement de telles améliorations et bénéficie en outre de l'intégration et de l'articulation avec différentes technologies de capteurs : elle s'appuie sur une meilleure prévention et identification des pannes ou un meilleur suivi des objets défectueux. Les performances permises par l'IdO concernent également les processus de production des biens et services : gestion des documents et des plans, suivi et visibilité des encours, rationalisation et coordination des fonctions d'assemblage. L'IdO permet aussi aux entreprises de mieux assurer le suivi commercial des ventes, en disposant d'une gestion en temps réel des sorties de stock. Enfin, il offre plus généralement aux acteurs économiques l'opportunité d'assurer une amélioration globale de la qualité des services fournis : qu'il s'agisse de réduire les erreurs en garantissant la pertinence des offres ou des biens offerts à la vente, de garantir une meilleure sécurité ou d'éviter les contrefaçons en permettant une authentification des produits, ou encore de permettre de produire ou fournir des services plus rapidement.

4.2.3 L'articulation des différents niveaux de performance.

La présentation successive de ces différents registres de performance occulte le fait que tous sont, en pratique, étroitement liés. Car les acteurs des filières envisagent la réorganisation de leur activité de manière globale. Ainsi, en réduisant le nombre d'entrepôts et en centralisant leurs opérations logistiques, producteurs et distributeurs optimisent les circuits d'approvisionnement et font de la fonction logistique un moteur central des stratégies de diversification en termes de services.

4.3. Comment et qui doit investir ?

Cette variété des sources de performance n'est pas seulement utile pour mieux comprendre les dynamiques de développement de l'IdO, elle a aussi des conséquences très directes sur les choix des acteurs économiques et la manière dont s'effectuent les décisions d'équipement. Les facteurs que nous venons d'évoquer créent en effet un environnement incitatif favorable pour les firmes mais ne constituent pas *ipso facto* un facteur automatique d'adoption. Pour comprendre les conditions de déploiement de l'IdO, il convient de garder à l'esprit que les choix d'investissement des organisations répondent à des processus de décision structurés et séquentiels.

4.3.1 Prendre en compte la complexité des investissements.

La rentabilité des applications doit notamment s'envisager en distinguant les équipements initiaux (la mise à niveau des infrastructures et des équipements) et les opérations courantes. L'amélioration économique des processus de production ne suffit pas toujours à justifier une décision d'investissement car elle dépend aussi de la manière dont les équipements de départ (puces et lecteurs) sont pris en charge et amortis. Ces investissements en amont (reconfiguration des processus et R&D) sont d'autant plus lourds que l'Internet des Objets recouvre un ensemble de technologies très diversifié et suppose de maîtriser un large portefeuille d'outils et de composants, allant des puces aux capteurs et aux *middlewares*. En outre, le coût de l'IdO pour une entreprise ne se résume pas simplement à l'acquisition de ce système technique (puces, lecteur, middleware) et à l'accompagnement de son installation. L'expérience montre qu'en matière de technologies de

l'information et de la communication, il convient de ne pas oublier les coûts cachés des mises en œuvre. Ceux-ci s'avèrent souvent extrêmement élevés et - comme l'ont montré certains équipements tels que les ERP - conduisent parfois à remettre en cause les investissements initiaux. En effet, au-delà des équipements techniques, les paramétrages des applications et l'apprentissage de l'organisation pour maîtriser les flux associés peuvent être longs, difficiles et coûteux.

4.3.2. Définir des solutions économiques propres à chaque niveau d'investissement.

Chaque facteur de performance et mode de valorisation correspondent donc à des solutions économiques spécifiques pour rentabiliser les nombreux investissements à conduire : R&D, infrastructure, développement de nouvelles applications, équipement d'un secteur ou d'une activité en puces, lecteurs et capteurs. Si l'on envisage l'opportunité de dégager des gains d'ensemble pour un secteur économique, l'absence de retour sur investissement clairement identifiable à court terme est pénalisante ; dans ce cas, ce sont plutôt les opérateurs et fournisseurs de technologie qui seront incités à prendre en charge les investissements nécessaires pour assurer l'amorçage du marché et atteindre une masse critique d'applications. À l'inverse, quand des économies sont réalisables au niveau des chaînes logistiques et dans l'articulation entre systèmes d'information et gestion des ressources matérielles, les industriels intermédiaires (plateformes ou distributeurs) peuvent être en première ligne. En effet, ils bénéficient alors directement des gains de performance logistique et de la baisse des coûts de transaction ; ils peuvent envisager, dans le même temps, de facturer des services associés aux industriels partenaires, voire directement aux consommateurs. Ainsi, quand les applications apparaissent comme pouvant générer directement des économies, les acteurs industriels sont en mesure d'assurer leur autofinancement grâce aux gains de productivité dégagés et à un retour sur investissement favorable : optimisation logistique et maintenance, réduction des stocks, réduction des coûts de contrôle de gestion...

4.3.3 Développer de nouveaux services pour les consommateurs.

La création de nouveaux services à valeur ajoutée donne également la possibilité d'envisager un paiement par le consommateur ou l'utilisateur final en reconfigurant de nouvelles offres. Ces dernières peuvent prendre plusieurs formes. Elles peuvent d'abord résulter de l'agrégation de marchés de niche : c'est le cas des applications à destination des animaux qui s'appuient sur le même type de puces pour structurer des applications sensiblement différentes selon qu'il s'agit de bovins, d'équidés, de chiens ou de chats par exemple. Les nouvelles offres peuvent également s'articuler sur des marchés traditionnels, en élargissant la gamme des services proposés : les possibilités ouvertes par le marquage des véhicules et l'électronique embarquée fournissent ainsi matière à de nouveaux services à valeur ajoutée, parfois regroupés sous le terme de « voiture communicante » : ce sont des services d'assistance (*e-call*), de sécurité active pour la conduite, mais aussi des formes nouvelles d'assurance (*pay as you drive*). Enfin, les nouvelles offres s'appuient sur la création de marchés nouveaux comme ceux de la protection personnelle (surveillance des jeunes enfants ou des personnes âgées, sécurité des biens, sécurisation des accès...). Ces nouveaux services en phase de création ne sont pas isolés, on les retrouve dans tous les types d'activité.

4.3.4 Garantir le financement de l'ensemble de la chaîne de valeur.

Dans tous les cas cependant, le déploiement de l'IdO peut se heurter à la tentation de chacun des acteurs industriels de s'abstraire des coûts d'investissement en reportant les charges sur d'autres acteurs de la chaîne de valeur. Cette menace n'est pas purement théorique. Les exemples récents de l'EDI ou le développement des plateformes de marché électroniques montrent que les acteurs dominants des filières sont toujours tentés de saisir de telles innovations pour renforcer leur contrôle sur l'ensemble des processus de production et sur les acteurs associés, qu'il s'agisse des sous-traitants, des fournisseurs ou des consommateurs. Dans de tels cas, selon les modèles économiques retenus, le risque n'est pas négligeable de voir les PME exclues des processus de modernisation et de performance associés à l'IdO ou, au contraire, obligées d'en supporter principalement le coût, au seul bénéfice des grands donneurs d'ordre.

Ce point est particulièrement sensible car le succès des applications de l'IdO repose, quels que soient les domaines d'applications, sur leur déploiement en parallèle dans toutes les composantes de l'activité et chez tous les partenaires concernés : des producteurs et donneurs d'ordre jusqu'aux distributeurs ou aux usagers. Quand ce n'est pas le cas, l'intégration des informations tout au long du processus devient impossible, le succès et l'intérêt même de l'application pour l'ensemble de ces partenaires sont compromis. Pour promouvoir le déploiement de l'IdO dans les différents secteurs, il s'avère donc essentiel de s'assurer du financement effectif des investissements à tous les niveaux des filières intéressées : cela peut être envisagé par le cadre d'actions industrielles (cautionnement public par exemple) ou en incitant les partenaires d'une filière donnée à mutualiser leurs engagements (dans un cadre de consortium par exemple).

4.3.5 Favoriser les usages publics de l'IdO.

Le rôle des pouvoirs publics peut s'avérer d'autant plus important que les exemples d'applications présentées plus haut nous montrent que les profits de l'IdO ne bénéficient pas seulement à certains acteurs de la chaîne de valeur. Dans nombre de cas, le déploiement sur l'ensemble des filières contribue à améliorer globalement le bien-être social, au-delà des avantages particuliers de tel ou tel acteur.

C'est le cas, tout naturellement, dans les secteurs d'activités qui relèvent déjà traditionnellement, en Europe, de la sphère publique : santé, éducation, culture ou administration. Les exemples abondent déjà d'applications à l'utilité incontestable : suivi des dépenses de santé, lutte contre les risques de contrefaçon, amélioration du traitement des patients et personnes dépendantes, meilleure accessibilité des bibliothèques publiques, sécurisation des documents administratifs.

Mais les gains pour la société peuvent aussi naître dans les produits et services relevant, de plein droit, des activités privées. Dans la grande distribution alimentaire par exemple, il est important de noter que quels que soient les profits qu'en retireront les grands distributeurs, la généralisation des puces RFID sera, sans aucun doute, une source prépondérante d'amélioration de la chaîne de traitement des déchets. Ces technologies seront aussi à la base du développement des « villes durables » ainsi que des « villes intelligentes ».

4.4. Une redéfinition des chaînes de valeur.

La variété des déploiements associés à chaque application, la multiplicité des sources de performance et des modes d'engagement dans l'IdO, modifient les stratégies individuelles des acteurs économiques. Elles contribuent, en parallèle, à transformer et redéfinir les marchés et les chaînes de valeur associées, côté demande, aux secteurs d'applications et, côté offre, à ceux de l'industrie de l'électronique et des télécommunications.

4.4.1 La chaîne de valeur industrielle.

Le paysage industriel de l'IdO est souvent dessiné en identifiant ses grandes catégories d'acteurs techniques. Les éditeurs de logiciels et offreurs de technologie développent les outils logiciels mobilisés comme support de l'IdO. Les fournisseurs techniques fabriquent et assurent la configuration des puces et le marquage. Les prestataires peuvent suivre les objets, gèrent les droits d'accès et recouvrent éventuellement les paiements en assurant une fonction d'intermédiation entre l'utilisateur final et les acteurs du processus de production. Plusieurs auteurs académiques ont proposé de catégoriser une telle structure. La plupart de ces travaux distinguent les firmes selon les traditionnelles couches techniques successives (*layers*)²⁶ : les fabricants de puces (Hitachi, Motorola, Philips, Siemens, Texas), les développeurs de composants et assembleurs (Allen, Avid, Sirit, UPM Raflatac, Zebra), les intégrateurs de systèmes (Checkpoint, Savi, RF Code), les éditeurs de logiciels (Cisco, Microsoft, Oracle, Sybase, TIBCO), les SSII et sociétés de conseil (Accenture, Atos, CapGemini, IBM, Lockheed, SAP, SUN MS).

4.4.2 Les nouveaux entrants dans la chaîne de valeur.

Une telle caractérisation trouve cependant ses limites dans la mesure où l'IdO crée une nouvelle chaîne d'opérations entre encodeurs, serveurs, terminaux, gestionnaires des droits : la chaîne « technique » s'entremêle désormais avec la chaîne, plus traditionnelle, de production des biens et services. Ainsi, le poids du B2B fait que certains secteurs utilisateurs lourds (grande distribution ou aéronautique, notamment) peuvent avoir un poids décisif dans la structuration de l'IdO ; parallèlement, les industries de contenus (culturelles par exemple) sont tout aussi puissamment motrices dans les transformations (c'est en particulier le cas dans la musique enregistrée). L'écosystème de l'IdO est donc marqué par le développement des réseaux, des partenariats et des interrelations complexes, une transformation des chaînes de valeur, des reconfigurations industrielles et de marchés, le brouillage des frontières traditionnelles des firmes et des secteurs. Une telle perspective doit conduire à aller au delà de la caractérisation par couches techniques habituelle dans les anciens secteurs entrés en convergence (télécommunications, technologies de l'information, électronique grand public, Internet et médias).

4.4.3 Des spécificités vis-à-vis du secteur de l'électronique.

Le paysage de l'IdO est marqué par des caractéristiques qui le distinguent de l'écosystème traditionnel de l'électronique.

²⁶ Cf. en particulier, *RFID Technologies : Emerging Issues, Challenge and Policy Options*, JRC 2007, op. cit.

4.4.3.1 *Les intermédiaires d'information.*

L'IdO est d'abord marqué par l'importance de strates nouvelles dans les filières industrielles existantes. Ces nouvelles couches résultent du poids des activités associées aux *middlewares* et à la gestion des données : stockage, historique, réponses aux requêtes, traitements de données massives. Les transformations correspondantes se traduisent par l'apparition de nouveaux intermédiaires qui peuvent être des acteurs spécifiques au monde des RFID (cf. EPCglobal), représentant des intermédiaires d'information communs à plusieurs technologies concurrentes (nommage des objets, information logistique) ou spécialisés sur certaines applications et filières associées (environnement, médecine, culture, etc.)

4.4.3.2 *L'ancrage territorial*

La chaîne de valeur de l'IdO appelle aussi l'émergence de nouveaux acteurs locaux dans des secteurs à l'ancrage territorial avéré : distribution, tourisme, culture, patrimoine environnemental, notamment. On peut se demander si le poids de tels intermédiaires ne rendra pas moins aisée, pour l'IdO, la délocalisation des services, contrairement à ce que l'on observe souvent dans les services en ligne actuels. Il fait toutefois peu de doute que des investissements et des engagements importants dans les *middlewares* et les systèmes d'information s'avéreront indispensables pour pouvoir tirer le meilleur parti des ressources d'une localisation européenne.

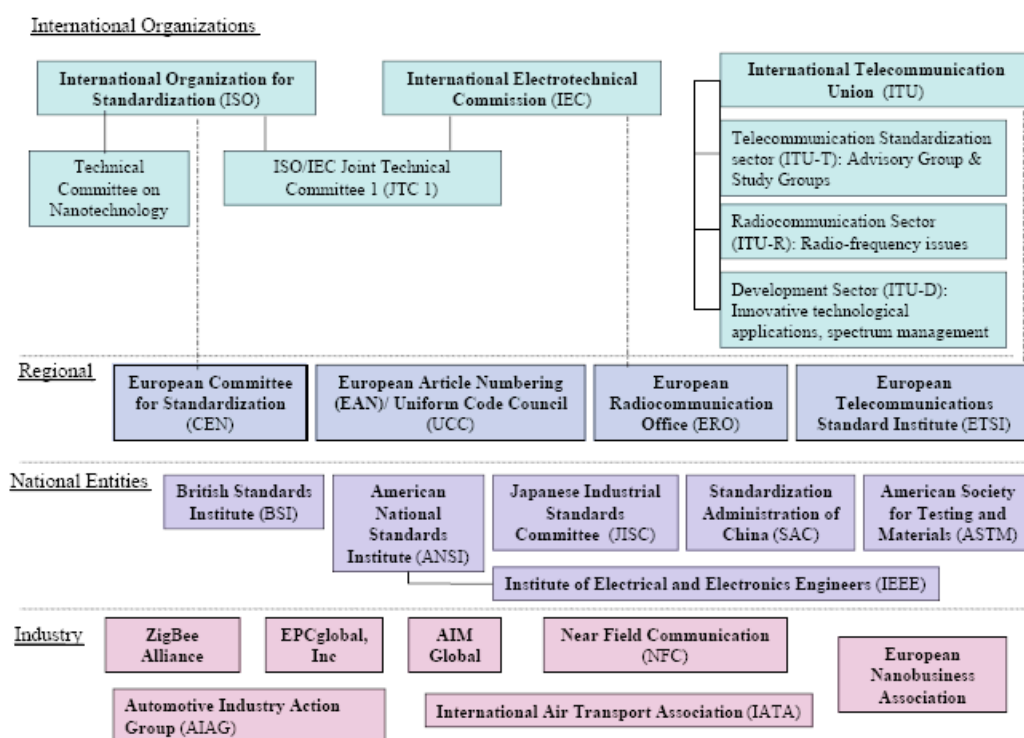
4.4.3.3 *L'enjeu central de l'interopérabilité.*

Les reconfigurations de filières tiennent aussi au caractère central des enjeux d'interopérabilité : par le biais de passerelles entre applications ou via le développement de *mashups* contribuant à démultiplier les effets et les applications de l'IdO. Plusieurs initiatives attestent déjà des transformations portées par cette interopérabilité : par exemple les possibilités ouvertes par les outils de reconnaissance des puces ou de lecture des codes barres que l'on trouve déjà sur certains téléphones mobiles. Au delà de ses enjeux économiques, l'ouverture de possibilités d'interconnexion et d'interopérabilité crée de fortes opportunités de développement en stimulant les possibilités d'innovation. Dans le monde de l'Internet, elles ont constitué un facteur de croissance incomparable pour des entreprises comme Google ou comme certains fournisseurs d'accès. Il devrait en être de même dans le monde de l'IdO. Certains parlent déjà des applications M2M - de machines à machines - comme des futures applications « tueuses » : qu'il s'agisse d'électroménager (réfrigérateurs se réapprovisionnant tout seuls, ou machines à laver « dialoguant » avec les vêtements pour adapter leurs programmes), outils gérant directement leur maintenance, ou encore plus récemment des applications proposées sur l'iPhone par l'intermédiaire de l'Apple Store.

Cette notion d'interopérabilité est régulièrement au cœur des questions de l'économie de l'Internet. Outre la simple interconnexion qui assure la compatibilité entre composants *hardware* et *software*, moyennant la définition d'interfaces de transports et de formats d'application, l'interopérabilité correspond à la définition de standards communs sous la forme de standards ouverts, de telle sorte que ceux-ci puissent être réutilisés par l'ensemble des acteurs au sein des solutions techniques qui leur sont propres. Très tôt a émergé l'idée qu'il devrait s'agir d'une des préoccupations majeures des politiques publiques et des acteurs privés. La complexité des

technologies et des connaissances mobilisées dans les réseaux interconnectés pose en effet des limites aux stratégies d'intégration : les acteurs spécialisés sur un des composants techniques peuvent devenir extrêmement puissants et imposer les contraintes de leur architecture spécifique (technique et économique) à l'ensemble du système.

La convergence des technologies et des systèmes de communication contribue à rendre le processus de standardisation particulièrement complexe : l'IdO relève ainsi de plusieurs instances de normalisation. Ce sont d'abord des organisations internationales telles que *l'International Telecommunication Union (ITU)*, *l'International Organization for Standardization (ISO)* ou *l'European Telecommunications Standards Institute (ETSI)*. De telles instances sont à vocation généraliste et leurs différents comités de normalisation couvrent tout le spectre des technologies de l'IdO. Parallèlement, il existe des instances plus spécifiques. Elles sont souvent d'ordre régional, national ou sectoriel, et se focalisent sur une dimension technique ou une partie spécifique du processus (normes RFID, protocoles réseaux, codage des données, allocation des fréquences, etc.). Le mouvement de normalisation et de déploiement de l'IdO se construit ainsi en combinant les différentes formes de standardisation : systèmes propriétaires, normalisation sectorielle volontaire, régulation publique, comités multistakeholders, etc.



Cartographie des instances internationales de standardisation de l'IdO

Source ITU, d'après FMI-ADC1 TAG, « The Roadmap to International Auto-ID Standards », janvier 2003.

4.5. Une demande en constante évolution.

La littérature scientifique rend compte de la structuration de ces domaines d'applications en listant, en général, les différents secteurs industriels et les activités supports de déploiement de l'IdO. À cette occasion, on constate que le développement des puces est très avancé dans le secteur des TIC (téléphones mobiles, géolocalisation). Dans le domaine vétérinaire, la RFID s'est développée pour le marquage des animaux en prolongement de systèmes préexistants (bovins, chiens et chats) et par l'élargissement ou la systématisation de telles applications (bovins ou équidés). Le domaine de la santé est aussi une bonne illustration du caractère très large du registre d'applications susceptibles d'être développées : suivi des objets (instruments chirurgicaux) ou des personnes (malades), contrôle de qualité (médicaments), optimisation des processus et de la qualité de service (gestion des traitements à l'hôpital), rationalisation des pratiques de soin (projet de DMP). Dans le cas des usages liés à la santé, des mesures spécifiques concernant la sécurité et la confidentialité des données sont aussi envisagées. Le secteur des documents d'identité (passeports biométriques) offre un exemple d'application massive dont le *driver* n'est absolument pas économique. Les systèmes de paiement dans les transports (autoroutiers ou publics comme avec Oyster, Navigo, Velib) fournissent un exemple d'application dont le développement est largement autofinancé par les opérateurs de transport dans l'espérance de gains de productivité (coût du contrôle, réduction de la fraude), d'amélioration de la qualité de service offert (simplicité d'usage) et dans la perspective de proposer des services à valeur ajoutée (raffinement de la tarification, CRM, marketing...). Loisirs, patrimoine et sports constituent enfin des domaines importants pour le développement des applications (billets de spectacle, suivi des sportifs – déjà expérimenté pour le marathon de New York - et contrôle des accès). Paradoxalement ce secteur est rarement évoqué alors qu'il montre que certaines applications à base de puces RFID peuvent connaître des déploiements massifs tout en étant parfaitement acceptées des usagers.

Notons toutefois que les études prospectives font le plus souvent état des mêmes applications-phares et entreprises emblématiques. Sont ainsi très régulièrement mis en avant les – mêmes - exemples de Metro, WalMart, Gillette, Tesco, Marks & Spencer, Benetton, Procter & Gamble, Frakt, ou Carrefour : à la fois pour le succès et l'ampleur de leurs applications ou, dans le cas récent de Benetton par exemple, pour les oppositions que ces applications sont susceptibles de susciter parmi les consommateurs.

À cet égard, il est utile de noter que ces acteurs issus de la distribution feront bientôt partie de l'écosystème des services de l'Internet, au même titre que Google, eBay, Amazon, etc.

Chapitre 5. Diffusion et mise en œuvre.

L'Internet des Objets est à la fois fondé sur des technologies antérieures et générateur de complexité nouvelle. Il est porteur de promesses de rationalisation et de croissance économiques, mais il suscite aussi des interrogations nouvelles. En rapportant les perceptions du public aux aléas de la technique et des marchés, il s'agit de réaffirmer que les questions d'acceptabilité sont majoritairement liées au couple sécurité-liberté et que des réponses claires sont nécessaires et attendues dans ce domaine. Les réticences, voire les résistances, qui se manifestent au sein de la société civile témoignent d'inquiétudes concrètes, qu'elles proviennent d'associations ou de particuliers. L'objectif est aussi bien d'améliorer l'information et la compréhension de ce qu'est l'IdO que d'attester que toutes les garanties seront prises au niveau de ses usages.

5.1. Comprendre et gérer les risques de l'IdO.

Le sentiment dominant est que l'évolution des techniques est cumulative et que leur pouvoir impose une espèce de fuite en avant dont la contrainte serait dans le même temps anonyme et non maîtrisable. Et quand les acteurs industriels et les pouvoirs publics évoquent les gains en termes de croissance et de sécurité, de nombreuses opinions publiques mettent en avant les risques et menaces pour les personnes.

5.1.1 Gérer les risques environnementaux.

La question des déchets de l'informatique actuelle n'est pas résolue de manière satisfaisante, mais il faudra en plus trouver des solutions pour gérer les pollutions nouvelles générées par les puces RFID. De même, les normes relatives à l'environnement radio-électrique devront faire l'objet d'une attention particulière en raison de l'augmentation du nombre d'émetteurs ambiants. Enfin, il faudra prendre en compte les risques de l'interaction entre les puces RFID et leur environnement, par exemple quand il sera question d'utiliser des capteurs implantables qui peuvent être susceptibles de perturber les appareils médicaux. Ces technologies de puces implantables devront aussi faire la preuve de leur innocuité dans la durée.

5.1.2 Prévenir les risques éthiques et juridiques.

D'abord, il conviendra de s'assurer que les personnes refusant d'être appareillées ne risquent pas d'être victimes de discriminations. Ensuite, il faudra peut-être réviser les règles de la responsabilité pour prendre en compte l'intermédiation des matériels électroniques.

Enfin la possibilité d'exercer de multiples « identités actives » dans l'univers numérique pourrait déboucher sur un éparpillement du sujet de droit qu'il conviendra de maîtriser.

5.1.3 Éviter les risques économiques.

Du côté de l'économie, des risques indirects sont liés à l'existence d'incidents dans des activités structurées et organisées autour de l'IdO. Il pourra s'agir de problèmes d'erreurs ou de pertes physiques accidentelles des tags, de *bugs* logiciels et fonctionnels du *middleware* et du *software* ou

des défaillances des terminaux et des lecteurs. En outre, l'hyper-interdépendance des éléments de production et de distribution exigera des prouesses d'organisation et de sécurisation, non seulement pour les particuliers, mais aussi pour la lutte contre l'espionnage industriel. Il faut donc bien peser les bénéfices attendus. Les industriels les évaluent en fonction du coût d'un processus de réingénierie qu'ils hésitent parfois à engager. Le grand public ne les ignore pas tout à fait puisque le suivi des malades d'Alzheimer, la traçabilité animale ou le repérage des jeunes enfants ont dépassé le stade expérimental. Toutefois il exprime plus de craintes que d'impatience, notamment en ce qui concerne la protection des données personnelles.

5.1.4 Maintenir un niveau de protection élevé en Europe.

Les citoyens et les entreprises européens jouissent aujourd'hui d'un niveau de protection parmi les plus élevés du monde. Il importe de s'assurer que le développement de l'IdO n'entraînera pas la remise en question de cet équilibre à leur détriment, mais qu'il sera au contraire l'occasion de l'améliorer. Il pourrait ainsi être question pour l'Europe de créer pour l'IdO de nouveaux standards internationaux de qualité en matière de protection des individus.

5.2. Écouter et informer l'opinion sur l'IdO.

Parmi les nombreuses enquêtes réalisées ces dernières années, presque toutes s'attachent à mesurer la perception par les citoyens des risques concernant l'implémentation de la RFID. Nous en retiendrons deux à titre d'exemple.

5.2.1 La crainte d'une utilisation abusive des données circulant via l'IdO.

La première, réalisée en 2005 par CapGemini, constate que le premier sujet d'inquiétude porte sur le fait que les données personnelles collectées puissent être utilisées sans que l'on sache par qui, ni pourquoi. En deuxième position, vient la crainte de pouvoir être tracé en permanence. Ensuite apparaissent les risques pour la santé. La comparaison entre l'Europe et les États-Unis montre une plus faible sensibilité à ces risques de l'autre côté de l'Atlantique, qui peut s'interpréter comme la résultante d'une plus grande familiarité avec ces technologies, ou bien d'une plus forte mobilisation des associations civiques. Mais ceci peut changer très vite. L'enquête a également comparé « l'impact *privacy* » de différentes technologies connexes (cartes bancaires, téléphone mobile, cartes de fidélité, badges d'accès, vidéosurveillance, etc.) : il en ressort que pour la RFID cet impact est au moins égal ou supérieur aux autres. L'université Humboldt de Berlin a conduit en 2006, auprès du public plus averti de ses étudiants, un travail similaire sur les risques majeurs perçus en terme de *privacy*. L'accès non autorisé aux informations, ou *skimming* vient en tête, le traçage des objets grâce aux données en second, suivis de la récupération des informations sur les réseaux sociaux, du « paternalisme » technologique et du transfert de responsabilité sur les objets aux utilisateurs.

5.2.2 L'inquiétude des citoyens relative à leur vie privée.

La *privacy* individuelle est le risque le plus souvent mis en avant dans les sondages et les débats publics²⁷, sans doute parce qu'elle est la plus facile à appréhender, et que la RFID est une technologie plus récente pour le grand public. La perception des risques concerne, on l'a vu, la capture, le traitement et l'utilisation des données personnelles tant par les gouvernements que par les entreprises. La nature des risques perçus est très variée : l'usage indu (interdit ou non autorisé pour l'application envisagée) des informations personnelles disponibles (sur la carte de santé, par exemple) ; la traçabilité généralisée ou sélective des individus (grâce à leurs badges, par exemple, au travail, en bibliothèque, etc.) ou de leurs actions (manipulation des objets associés) ; l'agrégation d'informations personnelles à des fins de surveillance policière ou de profilage marketing. Elle focalise des interrogations et des positions divergentes sur plusieurs points dont le statut légal des données personnelles, l'exercice du consentement, la désactivation fonctionnelle ainsi que la marchandisation de la sécurité des données.

Ces questions commencent à être prises en compte. En France, le Forum des droits sur l'internet (FDI), en association avec la Commission nationale informatique et libertés (CNIL), vient de lancer une consultation publique, ouverte jusqu'au 15 janvier 2009. L'objectif est de « récolter le point de vue des Français » sur des thématiques telles que le contrôle de l'image et de l'identité sur le Net, les données privées face à l'État et la protection de la vie privée dans l'univers numérique de demain.

5.3. Protéger la vie privée et les données sensibles.

Il faut différencier les questions qui relèvent des applications grand public (protection de l'anonymat et des données personnelles) de celles qui relèvent des applications industrielles (intelligence économique, compétition verticale entre producteur et distributeur, ou captation de la valeur ajoutée).

5.3.1 Protéger la vie privée.

La première acception de la *privacy* concerne le respect de l'intimité, de la confidentialité, des informations privées individuelles et/ou le respect de l'intégrité morale et physique des personnes. Traduite en français, elle s'étend à la protection juridique des données personnelles et touche aux libertés d'expression et de mouvement. Les menaces qui pèsent sur ces éléments concernent l'ensemble des technologies d'information et de communication (comme les moteurs de recherche, les plateformes de commerce et les réseaux sociaux), mais elles pourraient être alourdies si le développement de la RFID était mal régulé, notamment du fait de la miniaturisation des supports, de l'interconnexion des serveurs et de la géolocalisation.

²⁷ Dans une enquête menée en France en décembre 2007 par le CREDOC, c'était le sujet d'inquiétude n°1 pour 27% des sondés.

5.3.2 Différencier RFID ouverte et RFID fermée.

Il faut cependant opérer une deuxième distinction, entre la RFID « ouverte » et la RFID « fermée », autrement dit entre les systèmes dont les données ne sortent pas (par exemple sur une chaîne logistique de biens manufacturés) et ceux qui communiquent avec d'autres systèmes et qui échangent avec eux des données personnelles (comme dans le cas d'une compagnie de transports publics qui établit l'identité des usagers et travaille avec des chaînes de magasins). Dans les deux cas, cependant, la question est posée à la technique du choix entre la minimisation du nombre de données et la maximisation des garanties. C'est tout le débat entre les *Privacy Enhancing Technologies* et les *Trust Enhancing Technologies* (voir *infra*).

5.3.3 Rendre possible le « silence des puces ».

Différentes solutions technologiques sortent des laboratoires, même si aucune n'est encore appliquée de manière massive. Entre désactivation obligatoire, ou facultative, configuration *opt in* ou capacité de blocage, voire de brouillage, voici quelques exemples qui concernent les droits du citoyen ou ceux des consommateurs.

Aux États-Unis, le « passeport à cage de Faraday » a été imaginé suite à une mobilisation de l'opinion publique : la puce ne peut être lue que si le passeport est ouvert. Dans le secteur de la distribution, l'association CASPIAN (*Consumer Against Supermarket Privacy Invasion*) exige quant à elle la neutralisation du *tag* dès la sortie du magasin. RSA security a créé en 2003 un *blocker tag* qui permet d'empêcher la lecture non autorisée d'une puce. De son côté Open Business Innovation au Danemark a développé l'approche « *Zero Knowledge* », où le porteur peut contrôler sa puce en activant un mode « privé » ou non. Et le Distributed Systems research group du Swiss Federal Institute of Technology de Zurich a créé un *watchdog tag* qui permet au porteur de la puce d'avoir sur un écran ou sur son téléphone portable des informations sur le lecteur de la puce, sa localisation, etc. Le principe est dit du « *user-controlled identity management* » : l'utilisateur contrôle ses identités partielles en fonction des situations (face à un médecin, à un ami, etc...) en disposant d'un code spécifique pour chaque identité partielle, par exemple un pseudo et des mots de passe différents. Ici, la charge de lecture ou de mémorisation pour l'utilisateur est lourde, et d'autres travaux recourent à plus d'automatisation. Ainsi, au VIP (Virtual Identity and Privacy Research Center) de l'Université de Berne a été développé en 2001 le concept de « *virtual persons* », l'idée d'un masque virtuel protégeant les identités, avec un même masque couvrant plusieurs personnes, et une personne pouvant utiliser plusieurs masques, configurés pour effectuer certaines actions en son nom. RFID Guardian est quant à lui un projet collaboratif de pare-feu, qui permet à une petite batterie intégrable à des téléphones ou ordinateurs portables de brouiller les ondes RFID. Cet outil à destination du grand public est développé depuis 2004 ; il implique aujourd'hui une quinzaine d'universitaires (Vrije Universiteit, Technical University de Delft, Hogeschool Inholland) et d'industriels (Riscure, Beyond Security).

5.3.4 Protéger les données sensibles des entreprises.

Pour la « *privacy* industrielle », les problèmes nouveaux posés par l'IdO concernent l'identification des gammes de produits et services, les composantes de produits et services, les données logistiques, les flux de consommation ou de circulation et enfin la contextualisation des

données. La tension classique entre sécurité et qualité de service, d'une part, respect de la *privacy*, d'autre part, est très atténuée pour certaines applications comme la protection des véhicules et objets de luxe, des animaux domestiques ou de race.

5.4. Les réponses techniques et les autres.

Les solutions de protection de la *privacy* peuvent être prises en charge simultanément ou de façon complémentaire par la technique, la conception initiale de l'architecture et les fonctionnalités définies, les procédures d'utilisation, le droit et la gouvernance.

5.4.1 Les Privacy Enhancing Technologies et leurs limites.

La protection de la vie privée, associée à la sécurité, est devenue un marché pris en charge par des entreprises spécialisées. Au contraire, les « PETs », alias *Privacy Enhancing Technologies*, proposent un éventail de solutions techniques à usage individuel dont certaines sont très avancées (dans le domaine de l'anonymisation et de l'identification).

Cependant, leur utilisation reste limitée, peut-être faute d'information, de sensibilisation, ou en raison du coût élevé des puces les plus complexes. Il conviendrait donc peut-être d'envisager des mécanismes d'intégration des *PETs* dès la conception des services de l'IdO, afin de les intégrer dans les coûts initiaux et d'éviter les inconvénients des solutions plaquées *a posteriori*.

5.4.2 Un nouveau marché de la confiance dans l'univers de l'IdO.

Le marché de la confiance recouvre aussi bien la confiance des consommateurs envers les offreurs, celle des offreurs envers la demande, que celle des utilisateurs envers les procédures et les institutions de régulation.

Il peut engager l'innovation dans la voie de la *Privacy by Design* ou des *Trust Enhancing Technologies*. Ce serait une façon d'accroître l'acceptabilité des technologies en diminuant l'asymétrie des échanges d'information, c'est-à-dire en aidant les utilisateurs de ces technologies à accéder à la connaissance des données qui les concernent.

Une difficulté supplémentaire tient aux différentes définitions que peuvent recouvrir les données personnelles. Les conceptions de la société, de l'identité ou de la vie privée sont propres à chaque culture. De sorte que le degré d'acceptabilité des PETs sera différent entre différents publics. Or, nous manquons aujourd'hui de comparaisons internationales dans ces domaines.

5.4.3 La gestion des identités multiples des individus.

Les usages divers de l'Internet ont fait naître un peu partout dans le monde des comportements atypiques, tels que la multiplication des adresses électroniques, le recours aux pseudonymes dans les blogs, aux avatars dans les mondes virtuels, etc. Ces « identités multiples » sont plus difficiles à saisir qu'un numéro de passeport, de sécurité sociale ou de compte bancaire.

Elles font aussi émerger des revendications comme le « droit à l'oubli », le droit à l'anonymat chaque fois que l'identification n'est pas indispensable, le droit au brouillage ou au mensonge s'il s'agit de protéger quelqu'un d'un danger - toutes formes du droit au « silence des puces » que les industriels sont chargés de construire et les autorités de garantir.

Cependant, il ne faut pas surestimer les problèmes de sécurité et de confiance. Rappelons que l'on avait observé le même phénomène sur l'Internet au début des années 2000 au moment du développement du commerce électronique. L'expérience montre que les craintes exprimées touchaient moins la sécurité effective des paiements que la découverte et l'exploration de pratiques nouvelles de consommation.

Finalement, on rencontre souvent le « paradoxe de la *privacy* ». On désigne ainsi « le fait que, quelles que soient les valeurs ou les inquiétudes dont ils témoignent publiquement, certains n'hésitent pas à fournir beaucoup d'informations sur eux-mêmes, surtout s'ils estiment que la contrepartie en vaut la peine. Ils ne sont pas pour autant inconscients des risques, mais ils les gèrent, ils arbitrent. On passerait alors peut-être d'un droit centré sur la protection des individus à un droit centré sur la maîtrise par les individus de leurs données, de leurs manifestations, de leur image, etc »²⁸.

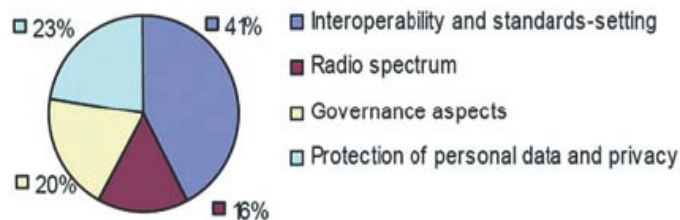
²⁸ D'après un rapport du groupe de travail « Identités actives » de la Fondation Internet Nouvelle Génération (Paris).

Chapitre 6. La nécessité d'une gouvernance adaptée.

La gouvernance des systèmes techniques est une composante majeure de la gouvernance des sociétés modernes. Le Sommet mondial sur la société de l'information (SMSI ou *WSIS*) qui s'est tenu entre 2003 et 2005 sous les auspices des Nations-Unies a eu pour ambition de trouver les voies et moyens d'une gouvernance « transparente, multilatérale et démocratique » de l'Internet. Mais il n'y est pas encore parvenu malgré la poursuite du dialogue entre les parties prenantes (États, entreprises, société civile) au sein de *l'Internet Governance Forum*.

La réflexion sur la gouvernance de l'Internet du Futur est d'autant plus fondamentale que celui-ci multiplie les incertitudes normatives : normes génériques RFID, normes d'infrastructures réseaux, normes d'identifiants, mais aussi normes sectorielles des entreprises, normes juridiques, normes socio-culturelles, normes sanitaires, etc. Et cela dans un univers où l'on prévoit des milliards de connexions en temps réel.

Contrairement à ce qu'indique la figure ci-dessous, extraite du rapport *Radio-Frequency Identification tags Portfolio of European research* (CE-INFSO, 2006), la « gouvernance » n'est pas une dimension de l'IdO parmi d'autres. Elle englobe au contraire les questions techniques, juridiques, économiques et politiques sous sa bannière.



La France et l'Europe disposent de nombreux atouts dans ces domaines. Le SMSI avait été l'occasion de propositions articulées autour d'un certain nombre de principes qui doivent encore aujourd'hui guider la réflexion et l'action : l'interopérabilité, l'ouverture et le principe du *end to end* (ou principe de neutralité).

Sur ces questions, l'Europe dispose d'instruments juridiques et de pratiques de coopération qui sont à évaluer, voire à amender, en fonction des évolutions en cours et à venir. Elle dispose également, sur l'Internet et les technologies convergentes, de résultats de recherche tangibles, en matière de technologie, de droit et d'éthique, qui pourraient être mieux diffusés et mieux exploités.

Le tableau que nous proposons ci-après présente les différents domaines dans lesquels l'Internet des Objets prolonge ou amplifie les questions posées par la gouvernance de l'Internet telle que nous la connaissons.

Grands domaines de gouvernance	Actions et instruments
<i>Gouvernance des ressources techniques</i>	<i>Politique industrielle et innovation</i>
Gestion du spectre	Accords internationaux
Normalisation	Co-production
Interopérabilité	Concertation amont et aval
<i>Gouvernance de l'architecture-réseau</i>	<i>Internationalisation</i>
Nommage et adressage	Centralisation distribuée
Évolution ou révolution	Principe du « end-to-end »
<i>Gouvernance socio-politique</i>	<i>Construction de la confiance</i>
Réglementation	Directives, lois, contrats
Auto-régulation	Codes de conduite, chartes, guide-lignes,
Ethique	Débat public, éducation, diversité culturelle
<i>Mots-clés</i>	droits fondamentaux - harmonisation – loyauté - proportionnalité – co-régulation – sensibilisation

Enfin, avant d'évoquer plus précisément les enjeux de normalisation technique, rappelons brièvement qu'il existe un ensemble de normes sanitaires portant sur l'exposition du corps humain aux champs électromagnétiques : la recommandation européenne 1999/519/CE, la directive 2004/40/CE du Parlement et du Conseil européens pour la protection des travailleurs, les guides établis par l'ICNIRP (*International Committee for Non-Ionising Radiation Protection*) pour limiter les temps d'expositions aux rayonnements (EMR), entre autres dispositions.

6. 1. La gouvernance technique.

6.1.1 La gouvernance des normes de l'IdO.

Dans le domaine de la RFID, des normes internationales génériques existent, par exemple sur la compatibilité électromagnétique, le mode de codage de l'information, les protocoles de communication entre la puce et l'interrogateur, etc. D'autres sont en cours d'élaboration sur la conformité ou les capteurs. Mais rien n'empêche un pays ou une entreprise de travailler à la création de normes et à promouvoir leur diffusion, ce qui pourrait conduire à des déséquilibres ou à une fragmentation du système global d'échanges numériques.

Ainsi, d'une part, l'adaptation à la RFID des normes d'infrastructures de réseaux locaux (LAN) ou étendus (WAN) de télécommunications mérite une attention particulière, dans la mesure où les systèmes d'information d'entreprise, les réseaux privés et les réseaux publics vont être amenés à s'interconnecter. D'autre part, les nouveaux secteurs d'activité n'ont pas encore tous rejoint les secteurs les plus avancés (la production animale, les transports) dans les comités de normalisation sectorielle.

Enfin, concernant l'étiquetage des objets, l'efficacité de la traçabilité suppose que l'on s'accorde sur le principe d'un identifiant unique, ainsi que sur ses conditions d'attribution et d'usage.

D'aucuns suggèrent la mise en place éventuelle d'une agence ou autorité indépendante chargée d'y veiller. Tous ces enjeux normatifs relèvent du domaine technique, mais il est clair que des luttes d'influence considérables sous-tendent le choix et le contrôle de telle ou telle solution et que les

pouvoirs publics, par nature garants de l'intérêt général, n'en sont pas exempts, soit au sein d'un même pays, soit dans la compétition internationale. En tout état de cause, il est souhaitable de rester vigilant quant à la nature ouverte des standards choisis, ainsi qu'à celle des acteurs de leur normalisation.

6.1.2 La gouvernance des fréquences de l'IDO.

Concernant la gestion du spectre, la Communauté européenne a publié en 2002 une décision²⁹ dans le but d'harmoniser les disponibilités et l'allocation de bande du spectre radioélectrique pour favoriser le marché intérieur (676/2002/EC). Les puces passives posent un problème spécifique dans la mesure où leur bande passante est utilisable par d'autres systèmes sans fil (Wifi, Bluetooth, ZigBee, par exemple). Mais la situation est encore plus complexe pour la bande UHF car la gestion des fréquences, actuellement assurée sur une base nationale, nécessite un effort d'information, puis d'harmonisation entre des réglementations différentes ou soumises à des agendas d'évolution mal connus. Il n'est pas certain que les dissonances entre les normes ISO et EPC pourront perdurer dans le domaine des *air interfaces*.

Pour ce qui est de l'allocation des fréquences, des arbitrages sont nécessaires entre les acteurs issus du monde des télécommunications, de l'audiovisuel et de l'Internet, moins pour des raisons techniques qu'au nom d'intérêts économiques et politiques. La révision de la Directive européenne appelée « paquet télécoms », pour nécessaire qu'elle apparaisse, n'a pas été de tout repos mais son adoption, prévue d'ici la fin de l'année 2008, devrait poser de nouveaux repères.

On notera ici qu'outre-Atlantique, la situation est tout aussi délicate : à l'occasion du lancement par Google du portail web de la campagne « *free airwaves* »³⁰, Lawrence Lessig, célèbre juriste et défenseur d'un Internet ouvert, a rappelé les termes de la controverse sur le caractère de « bien public » des infrastructures de l'Internet³¹.

6.2. La gouvernance des infrastructures-réseaux.

6.2.1 Identifier les types de réseaux.

En matière d'infrastructure de communications, on l'a souligné plus haut, l'IdO fédère un nombre toujours croissant de réseaux personnels et locaux, régulés et non-régulés.

Cette ouverture engendrera une expansion vers une grande variété de réseaux, selon leur type d'architecture, d'interconnexion et de niveaux de sécurité : *Wide Area Networks* ou *Personal Area Networks*, *Body Area Networks*, *Ad Hoc Objects Networks* etc., supportant chacun des applications dédiées.

Il faudra gérer cette complexité. Déjà, dans le B2B, on considère désormais que les réseaux « privés » (reconnus aujourd'hui par la RFC 1918) tombent sous le coup de la réglementation quand ils recoupent les réseaux publics.

²⁹ http://europa.eu.int/information_society/policy/radio_spectrum/index_en.htm

³⁰ Voir le portail www.freeairwaves.org.

³¹ Cf. le Colloque *Spectrum Policy: Property or Commons?* Stanford Law School, Stanford, California, 1-2 mars 2003.

La connectivité est ainsi appelée à devenir plus adaptative, localisée et flexible et elle exigera des solutions de reconfigurabilité.

6.2.2 Protéger le principe de neutralité (ou principe du *end to end*).

Face aux tentatives de segmentation sélective ou de remise à plat radicale de l'architecture de l'Internet, il convient de garder en mémoire l'apport positif du principe du *end to end*, qui a permis de placer « l'intelligence » aux extrémités du réseau.

Il correspond en effet à un triple impératif en termes d'innovation sociale et de développement économique :

- établir la compétition et la diffusion des innovations sur l'ensemble des segments de l'architecture de l'Internet (pas seulement au niveau de la couche des contenus mais aussi sur les applications qui sont désormais le vecteur dominant de la création de valeur sur l'Internet) ;
- autoriser de nouveaux acteurs isolés et des structures de petite taille à proposer et diffuser des innovations à grande échelle (comme le web ou les systèmes pair à pair) ;
- favoriser l'innovation via une régulation « anti-monopole » de l'Internet qui permettra aux nouveaux entrants d'établir de nouveaux modèles économiques.

6.2.3 Contrôler la gestion des ressources critiques.

Les enjeux transnationaux associés à la gestion des ressources critiques de l'Internet devront faire l'objet d'une attention particulière.

L'Internet des Objets va impliquer l'apparition de nouveaux acteurs moins familiers des principes et valeurs qui ont participé au développement du réseau³².

D'abord, il convient de développer des standards ouverts et ne pas reposer uniquement sur des technologies propriétaires. Par exemple, le premier ONS (*Object Name System*) développé par EPCglobal pour les étiquettes RFID est calqué sur le DNS actuel, avec la même arborescence centralisée et le même prestataire privé (l'américain VeriSign). Mais le système de nommage et d'adressage des objets va s'élargir bien au delà de la chaîne logistique des grands distributeurs. Comme le disait un professionnel du secteur : « le passage à la notion générique d'Internet des Objets amène à envisager des solutions alternatives ou, à tout le moins, la mise en perspective des différentes solutions proposées pour un même besoin ».³³

Ensuite, il faut continuer dans la direction donnée par la création de racines distribuées : annoncée en décembre 2007, la plateforme commune GS1-EPCglobal et Orange Business Service pour une racine française de l'ONS « entend constituer la première racine européenne de l'Internet des Objets. L'étape suivante du développement de cette initiative correspondra à la mise en œuvre de technologies qui permettront l'interopérabilité avec la racine américaine ainsi qu'avec celles qui ne manqueront pas d'être créées bientôt, en Asie et dans le reste du monde »³⁴.

La nature de cette gouvernance repose sur une collaboration étroite entre pouvoirs publics et

³² Cf l'intervention de Mathieu Weill, directeur de l'AFNIC, au colloque EGENI 2008.

³³ voir le blog S.I.A.I.G.E (Systèmes d'information appliqués à l'intelligence et à la guerre économique).

³⁴ *Réf.* : discours de Mme Valérie Pécresse, Ministre de l'enseignement supérieur et de la recherche, 3 décembre 2007.

grands acteurs économiques, qui reste à harmoniser à tous les niveaux (national, régional, international).

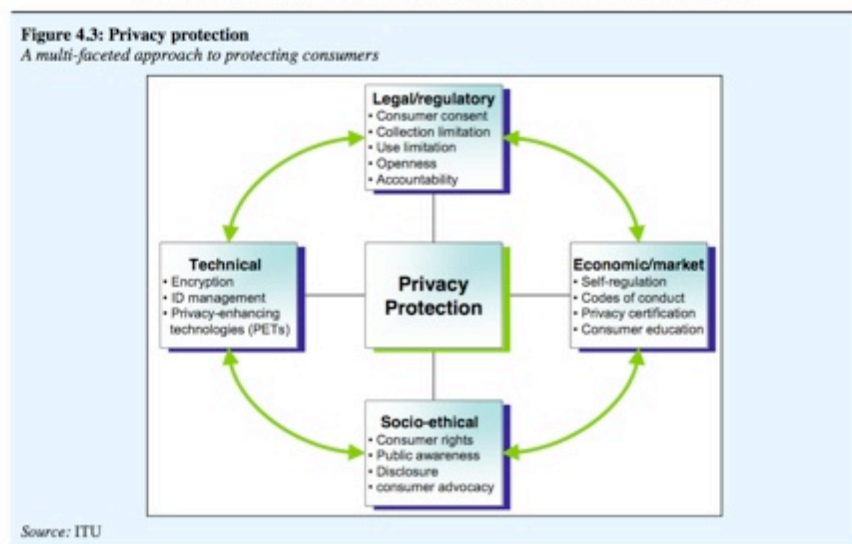
Enfin, il faudra associer le public à ces développements. Les consommateurs et les citoyens doivent pouvoir participer à l'évolution du devenir de leurs données personnelles et conserver la maîtrise de leur environnement.

6.3. La vie privée, entre technique, droit et éthique.

L'IdO repose sur le recueil, l'agrégation et le traitement de données portant sur les objets et « au besoin », sur les personnes qui les utilisent. Les progrès dans la transmission des informations passent par l'intégration de l'adresse IP et des paramètres de géolocalisation. Au delà des aspects de normalisation technique se posent donc des questions de validation des identifiants, de statut et de propriété des données et de moyens à mettre en oeuvre pour le respect de la vie privée. La construction de la confiance est un défi majeur pour que les promesses de l'Internet du Futur bénéficient au plus grand nombre.

Sur la RFID, la polémique est déjà vive et il est nécessaire de savoir si la législation existante est appropriée ou suffisamment appliquée, s'il est besoin de créer des « droits nouveaux » ou de mieux articuler les différentes composantes du droit. La figure ci-après fournit un aperçu des différentes problématiques relatives à la vie privée dans l'IdO.

Les facteurs qui influenceront la protection de la vie privée lors du développement de l'Internet des objets
(Source : International Telecommunication Union³⁸)



6.3.1 Des cadres réglementaires en évolution.

6.3.1.1 La consultation publique européenne sur la RFID.

Au sein des pays de l'Union européenne, les cadres réglementaires concernant l'utilisation de la RFID sont encore disparates. La Commission européenne a organisé en 2007 une large

consultation sur les usages de la RFID³⁵. Il a été décidé de ne pas instaurer de régulation du marché des « puces », mais la Commission a toutefois émis le souhait que les usagers puissent les désactiver.

La mise en place de ce droit à la désactivation aurait pu être obtenue par la modification de la législation sur la protection des données personnelles mais, en l'absence d'une perception commune de ce qu'est la *privacy* et d'une entente sur le degré acceptable d'identification et de profilage, le « silence des puces » est pour l'instant laissé à l'appréciation des industriels, qui incluent ou non des mécanismes de désactivation en fonction du rapport coût-bénéfice. Il n'est pas encore question de réversibilité de la désactivation des puces.

Mais au-delà de la mise en place d'un cadre pour la RFID, il existe déjà d'autres instruments applicables.

6.3.1.2 L'encadrement du commerce électronique.

En matière économique, la Directive européenne 2000/31/CE a instauré le cadre juridique de base pour le commerce électronique dans le marché intérieur. Elle établit des règles harmonisées sur les exigences en matière de transparence et d'information imposées aux fournisseurs de services en ligne, les communications commerciales, les contrats par voie électronique ou les limites de la responsabilité des prestataires intermédiaires. De même les *Lignes directrices* de l'OCDE *régissant la protection des consommateurs dans le contexte du commerce électronique* (1999) appellent les entreprises à fournir « des informations exactes et facilement accessibles qui décrivent les biens ou services offerts, et qui soient suffisantes pour permettre aux consommateurs de décider en connaissance de cause de s'engager ou non dans la transaction ». Ces principes d'information générale devront s'appliquer à toutes les parties intervenant dans la fourniture de puces RFID aux particuliers.

6.3.1.3 La protection des données personnelles.

Les *Lignes directrices* de l'OCDE *sur la protection de la vie privée*, adoptées en 1980, et sa recommandation sur la coopération transfrontalière (2007), tout comme la Résolution 45/95 de l'Assemblée des Nations-Unies (1990) sont non-contraignantes mais elles sont le fruit d'un consensus international. Leur mise en oeuvre dans le contexte de la RFID pourrait être facilitée par différents principes et outils relevant des pouvoirs publics. L'Organisation Internationale de la Francophonie s'est également saisie de la question lors du Sommet de Bucarest en 2006. Au niveau international, le Conseil de l'Europe a établi dès 1981 une Convention (n°108) pour la protection à l'égard du traitement automatisé des données à caractère personnel, ouverte à l'ensemble des pays. L'Union européenne a promulgué en 1995 une directive sur la protection des données (95/46/EC). Une autre directive européenne (2002/58/EC) s'applique au traitement des données personnelles collectées via les services et réseaux de communication publics. Sa révision est en cours, pour prendre en compte leur interconnexion avec les systèmes privés d'applications RFID. Le rôle du Contrôleur européen à la protection des données, charge créée en 2004, pourrait en

³⁵ cf. <http://www.rfidconsultation.eu/>

sortir renforcé. Enfin, le Traité européen, dans son article I-50-titre VI sur la « vie démocratique de l'Union » réaffirme que la Charte des droits fondamentaux de l'Union européenne (2000 et 2007) a la même valeur juridique que les Traités et que l'Union adhère à la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales.

6.3.1.4 Les enjeux « informatique et libertés » de l'IdO.

Au niveau européen, le *groupe Article 29*³⁶, qui regroupe les différentes autorités de protection des données personnelles des États Membres, rappelle que les informations collectées ou stockées via des solutions RFID sont soumises aux règles établies dans la directive européenne de 1995. Ses principes de base sont clairs : la collecte doit avoir un objet précis et ne doit concerner que les informations pertinentes ; la durée de conservation des données doit être justifiée par rapport à la réalisation de cet objet.

Dès lors, le consentement préalable des individus à la collecte d'informations par RFID apparaît comme une condition *sine qua non*, de même que l'affichage des informations sur l'objet de la collecte et sur les personnes qui la mettent en œuvre, et l'existence de droits d'accès et de rectification sur les données conservées.

La protection des enfants fait l'objet d'une attention toute particulière. Le groupe a créé une *Charte Informatique et Libertés* qui s'est progressivement étendue à 80 pays (francophones et hispanophones) et plusieurs de ses membres (dont les Français) estiment que la Convention européenne pourrait fournir la substance d'une Convention mondiale bâtie sous les auspices des Nations-Unies.

À l'échelle nationale, dès 2003, la CNIL soulevait quatre « pièges » soulignant l'importance cruciale des enjeux « Informatique et Libertés » de l'IdO :

- celui de l'insignifiance des données (avant qu'elles ne soient agrégées et exploitées),
- celui de la priorité des objets (tant que les applications relatives aux personnes ne sont pas massivement déployées),
- la logique de mondialisation (où les premiers entrants définissent les règles du jeu),
- la non-vigilance individuelle (du fait de l'automatisation des processus d'activation, de saisie et de contrôle).

La CNIL préconise aujourd'hui la mise en place de mécanismes de désactivation des « étiquettes intelligentes » dans certaines situations et surtout selon le libre choix des personnes – ce qui pose

³⁶ Le groupe a été établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 14 de la directive 97/66/CE. Ses principales missions peuvent être résumées comme suit :

- donner à la Commission un avis autorisé au nom des États membres sur les questions relatives à la protection des données;
- promouvoir l'application uniforme des principes généraux des directives dans l'ensemble des États membres au moyen de la coopération entre les autorités de contrôle de la protection des données;
- conseiller la Commission sur toute mesure communautaire ayant une incidence sur les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel et de la protection de la vie privée;
- émettre des recommandations destinées au grand public et, en particulier, aux institutions communautaires sur toute question concernant la protection des personnes à l'égard du traitement des données à caractère personnel et de la protection de la vie privée dans la Communauté européenne.

problème si cela conduit à neutraliser certaines applications comme la lutte contre le vol.

6.3.2 Des incertitudes persistantes.

Des zones d'ombre subsistent cependant et l'harmonisation des politiques publiques européennes fait face à deux questions cruciales qui encadrent celles de l'harmonisation des techniques et du comportement des marchés.

6.3.2.1 *Quel est le « champ » des données personnelles ?*

La collecte et le traitement des données via la technologie RFID ne relèvent de la Directive européenne de 1995 que lorsque les informations stockées dans la puce peuvent être qualifiées de données personnelles. Les interprétations de cette notion peuvent varier d'un pays à l'autre. Il importe donc d'harmoniser cette situation au niveau européen et international³⁷.

D'autre part, certains États Membres excluent la sécurité publique du champ de la Directive. Dans ce cas, il faudra s'assurer que le niveau de protection promu par l'article 8 de la Convention européenne des Droits de l'Homme (« nécessaire, proportionnel et respectant la dignité humaine ») sera bien garanti.

6.3.2.2 *Qui contrôle les fichiers ?*

La législation s'applique en priorité à la protection des données personnelles, mais elle laisse dans l'ombre les conséquences que l'IdO aura sur certaines libertés constitutionnelles, notamment via le profilage des comportements individuels et collectifs par agrégation et recoupement de données.

Le statut légal des « profils » ainsi constitués grâce au *data mining* (ou aux moteurs de recherche) devra être éclairci.

Également, du fait de l'invisibilité et de la pérennité des *tags*, la plupart des personnes ignoreront à quel point leurs données sont collectées et transmises, et ne disposeront ni du temps ni des ressources nécessaires pour exercer leur droit à connaître les logiques des dispositifs. Il conviendra donc de mettre en œuvre des mécanismes simplifiés permettant aux citoyens d'exercer leurs droits.

Enfin, le développement rapide du système RFID implique la dissémination de puces à bas coût et à fonctionnalités limitées. Ceci risque de limiter les efforts de construction d'une *privacy by design* chère à Adam Greenfield. Mais ne devrait pas empêcher le « marché des puces » de se conformer au respect des droits fondamentaux de la personne humaine.

6.3.2.3 *Encourager les « bonnes pratiques » des professionnels.*

À cet effet, les différents codes de conduite et autres chartes professionnelles des industriels du secteur des nouvelles technologies n'ont pas manqué de prendre en compte certaines menaces introduites par l'IdO. C'est ainsi, par exemple, que dans ses « *Guidelines for Consumer Products* » établis en collaboration avec la Chambre de commerce internationale, EPCglobal stipule que « les consommateurs seront avertis clairement de la présence de l'EPC sur les produits ou leur

³⁷ En France, la CNIL vient de reconnaître ce caractère à l'adresse IP.

emballage, et seront informés de l'utilisation de la technologie EPC. Cette information se fera par l'apposition d'un logo ou d'un identifiant EPC sur les produits ou leur emballage ». Ce document en appelle également à « de nouvelles méthodes efficaces, rentables et fiables pour accroître la faculté de choix du consommateur ».

Il s'agit ici d'une démarche de responsabilité qui mériterait d'être étendue à l'ensemble du système, dans tous les secteurs d'activité concernés, y compris dans l'administration. Mais elle ne lève pas toutes les craintes de capture et de mésusage des données. Des associations et des chercheurs développent une approche plus exhaustive, « holistique » selon les termes du réseau de recherche européen FIDIS³⁸.

6.3.2.4 Définir des droits et des infractions spécifiques à l'IdO ?

Entre autres exemples, les rapports du projet FIDIS citent un projet de « *RFID Bill of Rights* » proposé par l'américain Simon Garfinkel³⁹, qui énumère les droits des consommateurs :

- le droit de savoir si un produit contient des étiquettes RFID,
- le droit au « silence des puces » pour que les puces soient ôtées ou désactivées une fois l'achat effectué,
- le droit d'utiliser des services à base de RFID sans étiquettes RFID,
- le droit d'accès aux données stockées sur les puces,
- le droit de savoir quand, où et comment les données sont lues.

L'application de ces exigences devrait permettre de répondre aux revendications des usagers.

6.3.2.5 Poser les bases éthiques d'une régulation internationale de l'IdO.

Comme nous avons affaire avec l'Internet à une infrastructure mondiale et à des activités globalisées, un noyau de principes communs est nécessaire. Mais la préoccupation éthique est rendue plus complexe par la richesse des arrière-plans historiques, culturels, religieux, qui déterminent les valeurs fondamentales des différentes sociétés : les notions de propriété et de vie privée ne sont pas envisagées de la même façon en Occident, en Afrique ou en Asie ; l'usage de la cryptographie reste illégal dans certains pays ; les programmes de recherche-développement de l'IdO portent des noms différents, sous-tendus par des visions politiques et des options techniques qui peuvent être divergentes.

Comme la dimension interculturelle de l'éthique de l'information est de mieux en mieux documentée⁴⁰, la conquête des marchés tout comme l'efficacité des politiques publiques ne sauraient s'en abstraire.

³⁸ *Future of Identity in the Information Society*, cf www.fidis.net.

³⁹ <http://scrawford.net/courses/RFIDBillOfRights.pdf>

⁴⁰ cf *l'International Review of Information Ethics*, dirigée par Rafael Capurro.

Pour conclure : la nécessité d'aller vers la structuration d'un pôle de recherche européen.

La construction de la confiance passe par de multiples chemins. La gouvernance de l'Internet du Futur devra être multipolaire et multi-acteurs. La gouvernance actuelle de l'Internet vise un *outil*. Dans le cadre de l'IdO, elle devra évoluer pour s'appliquer à un *environnement*.

Les repères de la vie privée, de la souveraineté territoriale ou du temps et de la mémoire, sont eux-mêmes en phase de transformation. Il conviendra de bâtir des régulations susceptibles de favoriser et de garantir un réordonnement partagé des valeurs.⁴¹

Pour « penser » la gouvernance Internet en termes politiques l'idéal-type de la neutralité de la technique est nécessaire, mais non suffisant. L'économie et la politique numériques diffusent de manière insidieuse des contraintes puissantes et, dans le même temps, la mobilité et la connexion généralisées ouvrent des possibilités inédites pour le fonctionnement démocratique des sociétés et pour un accès mieux partagé à la connaissance. Bien averties de ces paradoxes, les institutions publiques, au niveau national comme aux niveaux européen et international, ont avantage à soutenir les recherches en sciences humaines et sociales tout comme elles accompagnent les efforts de recherche-développement.

Au terme de cette étude, nous ne pouvons que constater la nécessité de poursuivre les recherches. Sans répondre à l'ensemble des questions posées par l'Internet des Objets, nous avons surtout soulevé de nouvelles manières de poser des problématiques dont les solutions sont loin d'être évidentes : vie privée, gouvernance, normalisation, coopération, etc.

Chacun de ces sujets mériterait d'être traité en tant que tel, et de manière coordonnée, dans la perspective du développement de l'Internet des Objets. De plus, le besoin de réflexion dans ce secteur semble urgent, tant le développement des solutions techniques et des nouvelles applications s'accélère chaque jour.

Dans ces conditions, il convient sans doute de rassembler un effort de recherche au niveau européen pour aborder simultanément les questions techniques, économiques, sociales et juridiques. C'est une condition indispensable à une meilleure compréhension de l'Internet des Objets, ainsi qu'à la capacité de l'Europe à défendre les valeurs de ses citoyens dans le nouvel environnement numérique.

*

⁴¹ Cf Mireille Delmas-Marty, "Les Forces imaginantes du Droit", 3 tomes, Seuil, Paris.

Bibliographie sélective

ÉTUDES ET RAPPORTS OFFICIELS

BESSON Eric, « 27 pistes de travail ouvertes à la concertation pour préparer le plan de développement de l'économie numérique », *Assises du Numérique*, 29 mai 2008, Paris, Secrétariat d'état chargé de la prospective, de l'évaluation des politiques publiques et du développement de l'économie numérique.

<http://assisesdunumerique.fr/pdf/27pistes.pdf?f=2>

CGTI (J-C. Gorichon, F. Roure & E. Sartorius), *Les Technologies de Radio-Identification : enjeux industriels et questions sociétales*, rapport n°II-B.9, Paris, janvier 2005

<http://www.cgti.org/rapports/rapports-2004/II-B-9-2004-RFID.doc>

Commission européenne, *Technologies convergentes, Façonner l'avenir des sociétés européennes*, GEHN, Rapport 2004.

http://www.eurosfair.pr.fr/7pc/doc/1140686232_technologies_convergentes_report_nordmann.pdf

Commission européenne, *Radio-Frequency Identification tags Portfolio of European research*, 2006.

http://ec.europa.eu/information_society/doc/factsheets/5-1-rfid-research-portfolio.pdf

Commission européenne (2007a), *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, Commission européenne, COM(2007)96 final, Bruxelles.

http://ec.europa.eu/information_society/policy/rfid/doc/rfid_en.pdf

Commission européenne, *The Future of the Internet, A compendium of European Projects on ICT Research*, 2008.

ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/ch1-g848-280-future-internet_en.pdf

Commission européenne, *Préparer l'avenir numérique de l'Europe, Examen à mi-parcours de l'initiative i2010*, Communication au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions, 14 avril 2008.

<http://www.dsa-asn.org/home.php4?main=archive&id=118>

Direction Générale des Entreprises, Ministère de l'Économie, des Finances et de l'Industrie, *Étude sur les étiquettes électroniques et la traçabilité des objets*, mars 2007.

<http://www.telecom.gouv.fr/rubriques-menu/organisation-du-secteur/dossiers-sectoriels/etiquettes-electroniques-rfid/etiquettes-electroniques-tracabilite-757.html>

OCDE, *RFID: Drivers, challenges and public policy considerations*, 2006.

<http://www.oecd.org/dataoecd/57/43/36323191.pdf>

OCDE, *L'identification par radiofréquence (RFID) : Sécurité de l'information et protection de la vie privée*, Direction de la science, de la technologie et de l'industrie, Comité de la politique de l'information, de l'informatique et des communications, groupe de travail sur la sécurité de l'information et de la vie privée, avril 2008.

[http://www.olis.oecd.org/olis/2007doc.nsf/LinkTo/NT00005A7A/\\$FILE/JT03244945.PDF](http://www.olis.oecd.org/olis/2007doc.nsf/LinkTo/NT00005A7A/$FILE/JT03244945.PDF)

OCDE & Internet Technical Community, *Memorandum on the Future of the Internet in a Global Economy*, OECD Ministerial Meeting on the Future of the Internet Economy, 17 et 18 juin 2008, Séoul, Corée du Sud.

<http://www.apnic.net/news/docs/OECD-Memorandum.pdf>

OCDE, *Broadband Growth and Policies in OECD Countries*, 2008
<http://www.oecd.org/dataoecd/32/57/40629067.pdf>

UIT Internet Reports, *The Portable Internet*, 2004
<http://www.itu.int/osg/spu/publications/portableinternet/>

UIT Internet Reports, *The Internet of Things*, 2005
<http://www.itu.int/osg/spu/publications/internetofthings/index.html>

UNESCO & Conseil de l'Europe, *Ethique et droits de l'homme dans la société de l'information*, Actes de la Conférence de la région Europe, Strasbourg, septembre 2007.

UNESCO, *Ethical Implications of Emerging Technologies* (Rundle & Conley), 2007
<http://unesdoc.unesco.org/images/0014/001499/149992E.pdf>

ÉTUDES ET RAPPORTS DE RECHERCHE

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

CDT, *Privacy Best Practices for Deployment of RFID Technology*, Center for Democracy and Technology, 2006.
<http://www.cdt.org/privacy/20060501rfid-best-practices.php>

CHIRICO Filomena et al., *Network neutrality in the UE*, DP 2007-030, Tilburg Law and Economics Center, Tilburg University (NL), septembre 2007.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1018326

Commission européenne, *Internet of Things in 2020, roadmap for the future*, D.G INFSO in co-operation with the Working Group RFID of the ETP EpoSS, mai 2008.
<http://www.smart-systems-integration.org/public/internet-of-things>

Commission européenne, JRC-IPTS, *RFID Technologies : Emerging Issues, Challenges and Policy Options*, 2007
<http://www.stop-project.eu/portals/1/publications/eur22770en.pdf>

FIDIS (Future of Identity in the Network Society), NoE UE-FP6, livrable WP12 *A Holistic Privacy Framework for RFID Applications*.
http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp12-del12.3.A_Holistic_Privacy_Framework_for_RFID_Applications_v2.pdf

FIDIS, *Identity in a Networked World*, août 2006.
<http://www.fidis.net/resources/networked-world/>

FING, *Confiance et sécurité sur les réseaux*, Document de synthèse (A. Belleil et D. Kaplan), 2004.
http://www.fing.org/jsp/fiche_document.jsp?STNAV=&RUBNAV=&CODE=1119947447000&LANGUE=0&RH=IDENTITE

IPTS, Institute for Prospective Technological Studies, *The Future of The Information Society in Europe : Contributions to the Debate*, 2006.
<http://ipts.jrc.ec.europa.eu/publications/pub.cfm?prs=1453>

IPTS, *RFID Technologies : Emerging Issues, Challenges and Policy Options*, JRC Scientific and Technical Reports, 2007.
<http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=1476>

ISOC, *Preserving the User Centric Internet*, Internet Society Discussion Paper, 2008.

www.isoc.org/pubpolpillar/docs/usercentric_en_2008.pdf

ISOC, *Trust and the Future of Internet*, 2008

<http://www.isoc.org/isoc/mission/initiative/docs/trust-report-2008.pdf>

Politecnico di Milano, *RFID tra presente e futuro*. Collana Quaderni AIP. April 2005.

http://www.valuepartnersgroup.com/vp_pubbl_pdf/PDF_Comicati/Notizie/2005/invito_osservatorio_rfid.pdf

VOX INTERNET, *Gouvernance d'Internet : l'État de fait et l'Etat de droit*, MSH éditions, 2005

http://www.voxinternet.org/IMG/pdf/_RAPPORT_VF.pdf

ZITTRAIN Jonathan L., PALFREY John G. Jr., "Acces Denied : The Practice and Policy of Global Internet Filtering", *Oxford Internet Institute, Research Report n°14*, Juin 2007.

ARTICLES ET COMMUNICATIONS SCIENTIFIQUES

ARVIDSSON Adam, BRAUWENS Michel & PEITERSEN Nicolai, "The Crisis of Value and the Ethical Economy", *Journal of Futures Studies*, mai 2008.

http://www.p2pfoundation.net/Crisis_of_Value_and_the_Ethical_Economy

BASSET Caroline, HARTMANN Maren, O'RIORDAN Kate, "After Convergence : what connects?", *FibreCulture*, n°13, septembre 2008.

BENKLER Yochai, *From Consumers to Users : Shifting the Deeper Structures of Regulation, Toward Sustainable Commons and User Access*, 2000.

www.law.indiana.edu/fclj/pubs/v52/no3/benkler1.pdf

BERLEUR Jacques : "15 years of ways of Internet governance: Towards a new agenda for action", in *Social Dimensions of Information and Communication Technology Policy*, Avgerou, Chrisanthi; Smith, Matthew L.; Besselaar, Peter van den (Eds.) Proceedings of the Eighth International Conference on Human Choice and Computers (HCC8), IFIP TC 9, Pretoria, South Africa, September 25-26, 2008, Series: IFIP (International Federation for Information Processing), Vol. 282, 2008, VIII.

BROUSSEAU Eric, "Multilevel Governance of the Digital Space : Does a 'second rank' Institutional Framework exist?", in *Internet and Digital Economics*, E. Brousseau & N. Curien, eds., Cambridge University Press, 2006.

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=920228

BURKERT Herbert, « Changing Patterns, Supplementary Approaches to Improving Data Protection, A European Perspective », présentation à la conférence CIAJ 2005 *Annual Conference on Technology, Privacy and Justice*, Toronto, 29-30 septembre 2005.

CARR Nicholas, "IT doesn't matter", *The Harvard Business Review*, mai 2003.

<http://www.nicholasgarr.com/articles/matter.html>

CASELL Justine, BICKMORE Timothy, "External Manifestations of Trustworthiness in the Interface", in *Communications of the ACM*, 43(12). 50-56, 2000.

<http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.37.9208>

CLARK David D., BLUMENTHAL Marjory S., « Rethinking the design of the Internet : The end-to-end arguments vs the brave new world », 25th Telecom Policy Research Conference, 2000.

<http://www.tprc.org/abstracts00/rethinking.pdf>

CLEAN SLATE Project, workshop *The Future of TCP: Train-wreck or Evolution?*, Stanford University, avril 2008.

<http://yuba.stanford.edu/trainwreck/>

CORSTEN Daniel, GRUEN Thomas, "Stock-Outs mean Walkouts", *The Harvard Business Review*, mai 2004.

DAVIS Fred D., "Perceived usefulness, perceived ease of use, and user acceptance", *MIS Quarterly*, 319-340, 1989.

IRIE (International Review of Information Ethics), *Ethical Challenges of Ubiquitous Computing*, vol. 8, décembre 2007
<http://www.i-r-i-e.net/inhalt/008/008-full.pdf>

JUELS Ari, "RFID Security and Privacy: a Research Survey", *IEEE Journal on Selected Areas in Communication*, 2006.
http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf

LE CROSNIER Hervé, « A l'ère de l'informatique en nuage », *Le Monde diplomatique*, août 2008.
http://www.monde-diplomatique.fr/2008/08/LE_CROSNIER/16174

LELONG Benoît et al., « La fabrication des normes », *Réseaux*, vol. 18, n°102, Hermès Science, 2000

MAYER-SCHONEBERG Viktor, "Useful Void, The Art of Forgetting in the Age of Ubiquitous Computing", *Harvard University - John Kennedy School of Government Faculty Research Working Papers Series*, avril 2007.
http://www.vmsweb.net/attachments/pdf/Useful_Void.pdf

MERRILL Duane, "Mashups: The new breed of Web app.", octobre 2006.
<http://www.ibm.com/developerworks/xml/library/x-mashups.html>

RUBINSTEIN Ira et al., "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches", *The University of Chicago Law Review*, février 2008
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1116728

RUNDLE Mary, "Beyond Internet Governance : The Emerging International Framework for Governing the Networked World", *Research publication n° 2005-16, Berkman Center for Internet and Society*, Harvard Law School, Automne 2005.
http://cyber.law.harvard.edu/publications/2005/Beyond_Internet_Governance

SANTUCCI Gerald, "Policy & technology drivers in the Internet of Things", *Internet of Things International Conference for Industry and Academia*, Zurich, 27 mars 2008
<http://www.the-internet-of-things.org/prg/slides/santucci.pdf>

SYREY Bénédicte, « La notion de "privacy" au cœur des pratiques de consommation », intervention lors des 6èmes *Journées Normandes de Recherche sur la Consommation : Société et consommations*, 19-20 mars 2007.
http://www.argonautes.fr/uploads/uploads/documents/BenedicteSy_Rey.doc

VAN DER TOG & al., « Electromagnetic Interference From Radio Frequency Identification Inducing Potentially Hazardous Incidents in Critical Care Medical Equipment », *JAMA.*, 2008. 24(299): 2884-2890.

VUORINEN Jukka, "Ethical codes in the digital world: comparisons of the proprietary, the open/free and the cracker system", *Ethics and Information Technology*, Springer, 2007.

WU Tim, DYSON Esther, FROOMKIN Michael, GROSS David, "On the Future of Internet Governance", *American Society of International Law*, n°101, juin 2007.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=992805

ZITTRAIN Jonathan, "The Generative Internet", *The Harvard Law Review*, n°119, Juin 2006
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=847124

OUVRAGES

ALBERGANTI Michel, *Sous l'oeil des puces, La RFID et la démocratie*, Actes Sud, 2007.

BELL Genevieve, DOURISH Paul, *Yesterday's tomorrows : notes on ubiquitous computing's dominant vision*, Springer-Verlag, London, avril 2006.

DRIEUX Philippe, *Le miroir des neurones*, Odile Jacob, 2008

FINKENZELLER Klaus, *RFID handbook, fundamentals and applications in contactless smart card and identification*, Willey, 2nd Edition, 2003.

GANASCIA Jean-Gabriel, *Communication et connaissance, Supports et médiations à l'âge de l'information*, CNRS Editions, 2006.

GARFUNKEL S., ROSENBERG B., *RFID, applications, security, and privacy*. Addison-Wesley, 2005.

GOUJON Philippe et al., *The Information Society : Innovation, Legitimacy, Ethics and Democracy*, Springer, 2007.

GREENFIELD Adam, *Everyware : the dawning age of ubiquitous computing*, New Riders Publishing, 2006.

ITEANU Olivier, *L'identité numérique en question*, Eyrolles, 2008.

LAFONTAINE Céline, *L'empire cybernétique - Des machines à penser à la pensée machine*, Seuil, 2004.

LESSIG Lawrence, *L'avenir des idées*, PUL, 2005.

LESSIG Lawrence, *Code version 2.0*, Basic Books, 2006.

LIBAERT Thierry, *La transparence en trompe-l'œil*, Descartes et Cie, 2003.

YAN Lu, ZHANG Yan, YANG Laurence T., NING Huansheng, *The Internet of Things. From RFID to the Next-Generation Pervasive Networked Systems*, New York: Auerbach Publication, 2008.

ZITTRAIN Jonathan, *The Future of Internet and How to stop it*, Yale University Press, 2008.