

L'Internet des objets : les limites d'un concept essentiellement *marketing*

Avec pour ambition de faire dialoguer les objets, entre eux et avec les hommes, et pour perspective un monde de connexion encore plus dense que celui de l'Internet actuel, l'Internet des objets concentre moult défis technologiques, scientifiques, sociétaux, réglementaires et politiques. Il promet d'être le moteur de profondes transformations dans la vie des entreprises, des individus et des institutions.

L'Europe doit s'affirmer dès à présent dans les débats et travaux sur sa genèse, si elle ne veut pas se voir imposer de solutions venues d'ailleurs, et elle se doit de construire un Internet des objets acceptable et gouvernable, qui lui soit profitable.

La France, qui a largement contribué à la médiatisation de ce concept, a un rôle clé à jouer en matière de recherche dans ce domaine et d'émulation des acteurs européens autour de son initiative en faveur de l'application de l'Internet des objets à la grande distribution.

Par **Olivier ROUXEL***

Dès le début du « buzz » à l'origine de sa popularité, l'Internet des objets (IoT) (1) a été associé aux technologies RFID (2). Les puces RFID constituent en effet un des moyens les plus intuitifs pour rendre communicant un objet et pouvoir ainsi l'identifier à distance et sans visibilité et ce,

* Chargé de mission à la Direction générale de la Compétitivité, de l'Industrie et des Services (DGCIS), ministère du Redressement productif.

(1) IoT : *Internet of Things*.

(2) RFID : *Identification radio-fréquence* (étiquettes électroniques RF).

(3) 2006, Bruxelles ; 2007, Berlin, Lisbonne ; 2008, Nice.

à moindre coût : il suffit simplement d'y apposer une étiquette électronique ou d'incorporer celle-ci lors de la fabrication de l'objet considéré.

Les différentes conférences (3) organisées par des États membres de l'Union européenne (sous leurs présidences respectives du Conseil de l'Union) ainsi que par la Commission européenne elle-même, entre 2006 et 2008, l'ont bien montré : les seules réalisations concrètes se rapprochant du concept d'IoT reposent quasi exclusivement sur l'usage des puces RFID, notamment dans les processus logistiques. Ce constat s'applique également aux projets d'IoT qui sont conduits ailleurs dans le monde (en Russie,

au Japon, etc.) (4) et qui sont pour l'essentiel des projets RFID.

Pourtant, ce « concept » de l'Internet des objets est extrêmement riche en termes de technologies mises en œuvre et de secteurs d'utilisation, d'enjeux de R&D, d'enjeux industriels et sociétaux, réglementaires, etc. Cependant, sans frontières précises en raison, d'une part, de nombreux recouvrements avec des thématiques adhérentes (M2M, *smart grid*, villes intelligentes, services sur téléphones mobiles et NFC, Intranet des marchandises, Internet du Futur, etc.) et, d'autre part, des représentations que s'en font les acteurs, aussi diverses qu'ils le sont eux-mêmes, ce concept reste peu lisible : certains disent même qu'il ne s'agit pour l'heure que d'une « vision » (5).

QU'ENTEND-ON PAR L'« INTERNET DES OBJETS » ?

Ouvrant une nouvelle phase de développement de la société de l'information, l'avènement de l'Internet des objets (IoT) devrait modifier en profondeur l'économie numérique mondiale. L'IoT fait référence à un réseau qui interconnecterait l'ensemble des objets en leur donnant la capacité de communiquer entre eux, directement ou par l'intermédiaire d'Internet, pour échanger des informations (sur leur identité, leurs caractéristiques physiques, leur environnement), pour réagir à des commandes, etc.

Au fil des ans, les définitions proposées par les acteurs concernés se sont avérées plus ou moins complètes et partiales, chacun appréhendant l'IoT selon son propre environnement (même celle promue à l'Union Internationale des Télécommunications (UIT) en 2012 par la Commission européenne (6) ne faisait pas consensus). Simplicité rimant souvent avec efficacité, la définition proposée (en forme de clin d'œil) par Rafi Haladjian (7) mérite plus qu'un simple sourire : « L'Internet des objets, ce sont des objets reliés à Internet ». Sa généricité a en effet l'avantage d'embrasser les nombreux visages de l'IoT.

De quels objets parle-t-on ? D'objets réellement communicants (avec une liaison de communication établie dans le temps), ou d'objets renvoyant un simple identifiant (à la manière des RFID) ? Des objets avec ou sans capteur(s) ?

Des objets reliés à Internet. Oui, mais de quelle manière ? Avec ou sans fil ? De façon permanente, ou non ?

Des objets identifiés. Oui, mais de quelle façon ? *Via* un identifiant IoT unique ? *Via* leur adresse IP ? Ou leur adresse MAC ?...

Quelles sont les technologies à l'œuvre ? Le concept sous-entend la sollicitation simultanée ou non de nombreuses technologies : des technologies d'identification, des technologies de communication, des capteurs miniatures et des réseaux de capteurs, des tech-

nologies de récupération d'énergie (*Energy Harvesting*), etc.

Cette définition simplissime a l'avantage de fonctionner quel que soit le point de vue où l'on se place : à la maison (pour l'Internet des objets « personnel », souvent omis), au niveau d'une entreprise, d'un secteur d'activité, d'une ville, au niveau d'un pays ou, plus largement, d'une région géographique mondiale et, enfin, globalement.

Elle englobe aussi toutes les conceptions parfois opposées de l'Internet des objets, allant des partisans du tout RFID à ceux du « tout, sauf la RFID », de ceux du M2M (8) à ceux des réseaux capillaires, de ceux des entités autonomes en énergie à ceux des objets sur secteur, de ceux du coût le plus faible possible à ceux d'un coût à la hauteur de la valeur ajoutée du produit, etc.

Comme le montrent le lapin Nabaztag ou la balance connectée de Withings, l'IoT ne concerne pas uniquement des objets qui seraient RFID, peu chers et porteurs d'enjeux en matière d'autonomie énergétique : en effet, les produits précités ne sont pas « pucés » RFID (Nabaztag peut « sniffer » des puces RFID, mais il n'est pas identifié par ce biais), ils n'ont aucun problème d'énergie et ne sont pas spécialement bon marché. Pourtant, ces objets, qui sont connectés à Internet et qui interagissent avec leur environnement, relèvent bien, de fait, de l'IoT.

Le thème de l'IoT nécessite d'être abordé sans précipitation et avec un minimum de recul, pour éviter de tomber dans certains travers comme l'ont fait, volontairement ou pas, de grands groupes et des institutions multilatérales ? En effet, n'est-il pas plus porteur, d'un point de vue *marketing*, de coller au « buzz » en parlant d'IoT, plutôt que de M2M ?

(4) Présentation du projet CASAGRAS2 (FP7 EC), IoT-Week, juin 2011.

(5) Nice Conference on the Internet of Things (2008): Auto-ID Lab, Université de St-Gallen, Zürich, Suisse.

(6) Définition de l'IoT soutenue par la Communauté européenne : « *Internet of Things (IoT) is a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual things have identities, physical attributes and virtual personalities and use intelligent interfaces and are seamlessly integrated into the information network* ». (L'Internet des objets (IoT) est un réseau mondial dynamique d'infrastructure doté de capacités d'auto-configuration fondées sur des protocoles standard et interopérables de communication pour lesquels les objets, tant physiques que virtuels, ont une identité, des attributs physiques et une personnalité virtuelle, qui utilisent des interfaces intelligentes et qui sont intégrés sans solution de continuité au réseau (mondial) d'information [traduction de la Rédaction]).

(7) « Serial entrepreneur », fondateur notamment des sociétés Violet et Sen.se.

(8) M2M : *Machine-to-Machine*, c'est un marché connaissant une croissance à 2 chiffres depuis plus de 5 ans.

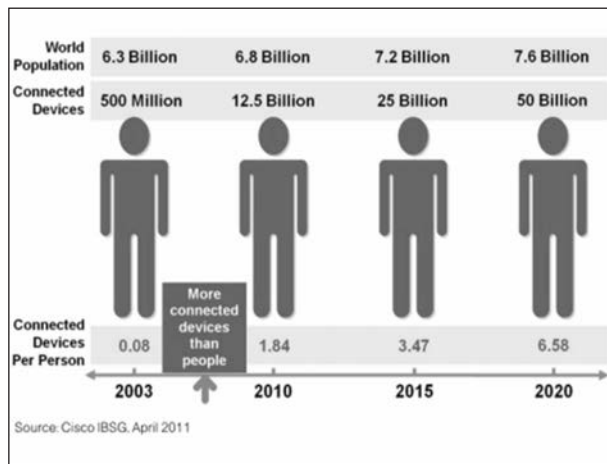


Figure 2. Evolution comparée du nombre d'objets connectés et de la population mondiale.

coûts et une meilleure compréhension, par les acteurs, du retour sur investissement (ROI) et du partage des coûts dans la chaîne de valeur.

En parallèle, et comme pour la RFID, les « anti » se sont mobilisés, dénonçant les menaces pour la vie privée d'une nouvelle ère de type Big Brother, parfois de façon objective, mais souvent sans nuance (y compris au Parlement européen). De même, la Commission européenne (12), tout en reconnaissant les bénéfices potentiels pour les citoyens et pour l'économie au sens large (et donc pour la compétitivité de l'Europe), place systématiquement le thème de la protection de la vie privée et des données personnelles au rang de sujet prioritaire en matière d'IoT, car cette protection fait, pour la Commission, partie intégrante des fondamentaux de l'Union européenne.

– Enfin, au niveau « *marketing* et communication », nombreux sont les acteurs qui ont fait le choix de donner un vernis IoT à leur stratégie, à leur *road-map* de R&D ou à leur gamme de produits (Cela vaut aussi bien pour les industriels que pour les académiques et les laboratoires de recherche). Le recours à la notion d'IoT devient ainsi systématique, comme on peut le faire, par ailleurs, aux Cloud, Big Data et autres Green...

DES ENJEUX IMPORTANTS

Enjeux technologiques et enjeux en matière de R&D

La concrétisation de l'IoT et son déploiement au plan mondial passent par la contribution simultanée (ou non) de nombreuses technologies au niveau non seulement de son architecture, mais aussi des services proposés, qu'il reste à imaginer : RFID, NFC sur mobile, Bluetooth, Zigbee, Wifi, Internet, nanotech-

nologies, réseaux de capteurs, systèmes à très faible consommation d'énergie, sans oublier les *middlewares* et les logiciels applicatifs, ou encore l'adaptation nécessaire des équipements des réseaux, etc. Par exemple, une rupture technologique dans le domaine de l'autonomie énergétique pourrait véritablement libérer les usages.

Le passage à l'échelle mondiale en matière d'objets connectés et de volumétrie des informations échangées impactera l'architecture et la capacité des réseaux actuels : de nouveaux identifiants seront nécessaires pour pouvoir admettre un potentiel de 50 milliards, voire même de 50 000 milliards d'objets (à comparer aux 6 milliards de téléphones mobiles recensés aujourd'hui), et l'énorme quantité d'informations échangées. Les réflexions se focalisent depuis plusieurs années déjà sur l'*Internet Protocol Version* (IPv6).

Un précurseur... et des concurrents

D'importants travaux sont menés actuellement au niveau mondial sur les briques susceptibles de constituer l'IoT : aux États-Unis, au travers du réseau et des *Electronic Product Codes* (EPC) (13), et en Asie, au travers du concept d'application ubiquitaires et des *uCode*, au Japon, et des *mCode*, en Corée.

De nombreux accords de coopération, d'échanges et de partenariat sont noués de part et d'autre des océans, en particulier entre l'Europe, le Japon, la Corée, la Chine et les États-Unis d'Amérique.

Promu par EPC/GS1 (14) au-delà des chaînes d'approvisionnement de la grande distribution, pour laquelle il a été développé, le réseau d'EPC Global est trop souvent vu comme « La brique unique du futur IoT ». Ce raccourci hâtif amène à assimiler les problématiques soulevées par l'*Object Naming Service* (ONS) (15) aux problématiques propres à l'IoT.

Centralisée autour d'un serveur racine ONS unique géré depuis 2004 par la société américaine VeriSign (également gestionnaire du serveur principal du *Domain Names System* – DNS), l'architecture de ce service crée *de facto* un lien entre ONS et DNS qui permet aux États-Unis à la fois de superviser de façon unilatérale le système des noms de domaines coor-

(12) Communication de la Commission du 18 juin 2009 : «Internet of Things - An action plan for Europe».

(13) EPC (*Electronic Product Code*) : nom donné à son système de codification RFID par EPC Global Inc (un consortium privé implanté aux États-Unis et contrôlé à parité par GS1 et par GS1-USA).

(14) GS1 : présente dans plus de 100 pays, cette « organisation » promeut des standards de codes-barres pour différents secteurs, dont la grande distribution. GS1 France est une entreprise.

(15) ONS (*Object Naming Service*) : annuaire renvoyant vers les pages Web des entreprises du réseau et permettant, grâce au service de recherche (*Discovery Service*) qui le complète, de retrouver les informations associées à un produit.

donné par l'ICANN (16) et de jouer un rôle incontournable dans la mise en œuvre du réseau EPC.

Cette situation est jugée inacceptable non seulement par les acteurs européens – industriels et institutionnels – mais aussi mondiaux (l'UIT, par exemple) en raison des problèmes qu'elle soulève en matière de souveraineté des États et d'intelligence économique.

Dans ce contexte, GS1 France a mis en œuvre en 2008, au niveau de la « région » France, un serveur racine ONS qui constitue une première réponse à la problématique de la racine unique : ses adhérents pourront ainsi consulter « localement » les informations sur leurs produits sans avoir nécessairement à recourir à l'annuaire ONS américain.

Il reste à vérifier l'interconnexion de cet ONS avec le serveur américain et (surtout) à définir le nouveau modèle de gouvernance applicable. EPC Global, qui espérait imposer sa racine unique, apparaît très peu moteur dans ces domaines, tout comme les institutionnels américains intervenus à la conférence de Nice, fin 2008, qui plaçaient clairement la balle dans le camp des Européens.

Cette racine ONS « en France » ne peut en l'état être considérée comme la racine européenne de l'ONS, ni même comme celle du futur IoT. Mais l'initiative est intéressante, et GS1 France a mis son ONS à la disposition de la communauté « GS1 in Europe ». De plus, Orange Business Services, son opérateur technique, se dit « ouvert aux discussions avec les acteurs des autres États membres ».

En Asie, le Japon a développé le système uID (*ubiquitous ID*), qui est très semblable à l'ONS : ce système recourt à des uCodes, mais ceux-ci sont indépendants du support (codes-barres, *tags* RFIDs, *tags* infrarouges, etc.), ils sont destinés à l'identification non seulement d'objets, qu'ils soient physiques ou immatériels (logiciels, musique, etc.), mais aussi de lieux – un système qui, toutefois, ne s'applique pas aux personnes.

Alors que l'ONS a été initialement conçu pour les chaînes logistiques, l'uID vise les applications ubiquitaires dans lesquelles l'Internet mobile joue un rôle clé. De nombreux réseaux ou applications uID sont d'ores et déjà déployés au Japon, et des expérimentations à grande échelle sont en cours dans huit villes japonaises, sous le concept d'« U-Cities ».

Des initiatives similaires sont menées par plusieurs pays asiatiques, notamment la Corée et la Chine. Il existe des *Ubiquitous ID Centers* à Taïwan, en Chine, au Japon et en Corée, chacun de ces pays s'étant doté de son propre système de résolution et de ses propres identifiants.

D'autres acteurs prendront probablement part à la construction de cet IoT, comme l'Alliance IPSO (*IP*

for Smart Objects) créée fin 2008 à l'initiative d'une trentaine d'entreprises (notamment CISCO, SUN Microsystems, SAP, ATMEL, EDF R&D, etc.) pour promouvoir les technologies d'Internet dans les futurs réseaux d'objets intelligents ; certains de ces acteurs étant des géants comme Microsoft, Google et Apple, qui ne cachent plus leur intérêt pour l'IoT et pourraient lancer leurs propres systèmes d'identification et de résolution, et d'autres étant des structures plus petites, comme l'ont montré les sociétés françaises Violet, pionnière des objets communicants, et, plus récemment, Sen.se.

PERSPECTIVES ET PROPOSITIONS

L'initiative de GS1 France ouvre la voie à un futur réseau EPC composé de plusieurs serveurs racines ONS régionaux interconnectés à la racine américaine, dont le cœur, européen, serait ainsi maîtrisé par l'Europe. La situation nouvelle bénéficie aux acteurs français (GS1 France, OBS). Au-delà du nombre des ONS européens, qui dépendra de l'attitude des grands opérateurs de téléphonie (qui ne veulent pas être en reste), la solution EPC se heurte, dans le domaine de la grande distribution, aux alternatives régionales, et son adoption rapide en Asie n'est pas acquise (voir le uCode japonais), en dépit du rôle joué par de grands donneurs d'ordres qui devraient y contribuer.

En dehors de la distribution, des besoins parfois très différents ou encore un refus du système de redevances d'EPC/GS1 pourraient amener les grands secteurs industriels (notamment l'automobile et l'aéronautique) à développer leurs propres standards d'étiquettes électroniques, ou à mettre en œuvre des standards existants autour d'ONS sectoriels dédiés et ce, sans rechercher d'interopérabilité ni d'interconnexion avec des acteurs se situant en dehors de leur propre écosystème.

Par ailleurs, il faudrait obtenir un engagement clair des acteurs américains (dont EPC Global et l'ICANN) à contribuer aux tests menés par les Européens sous la conduite de GS1 France, dans ce nouveau contexte où la racine américaine de l'Intranet des marchandises n'est plus unique au monde.

Le concept d'IoT est, quant à lui, global et ouvert aux citoyens. Il est profondément transversal en termes d'usage, et est bien plus qu'une simple transposition des standards et du réseau EPC.

La coexistence de plusieurs sous-systèmes contribuant à l'IoT est une perspective envisageable, chacun d'eux utilisant son propre schéma d'identification. L'interopérabilité d'ensemble devrait alors être assurée grâce à un moyen permettant d'unifier ces schémas d'identification tout en conservant les règles d'enregistrement propres à chacun, comme par

(16) *Internet Corporation for Assigned Names and Numbers* (ICANN) : organisation de droit privé à but non lucratif chargée d'attribuer les identificateurs de protocole et de gérer les noms de domaines de premier niveau.

exemple le système des *Objects Identifiers* (OID) (17), qui fournit une référence unique internationale à chaque schéma. Ainsi, la Corée a demandé à l'UIT un OID pour son mCode. Le Japon et EPC pourraient en faire de même.

Avec un intérêt grandissant des grandes entreprises et des organisations internationales pour l'IoT, une bataille de pouvoir s'annonce entre communautés d'intérêts, surtout entre les fournisseurs de technologies, qui voient en lui un marché ultra-prometteur.

Les réflexions sur l'IoT ne doivent pas se dérouler sous le contrôle d'acteurs dominants. La place de certaines entités dans le débat devrait être systématiquement rappelée, en termes tant de « structure » que de légitimité. Alors que les manifestations sur le sujet se multiplient à l'initiative d'acteurs publics ou privés français ou européens, mais sans qu'une réelle avancée ait été à ce jour constatée, il apparaît maintenant urgent d'étudier les alternatives potentielles en matière d'architecture, de codage et de technologies connexes présentes ailleurs dans le monde (notamment en Asie), et d'analyser les possibilités d'interconnexion de ces systèmes avec le réseau EPC.

Dans la perspective d'un IoT multiple où coexisteraient des solutions globales aux côtés d'applications plus régionales, sectorielles voire personnelles, la question de l'unification des identifiants et des passerelles entre ces différents systèmes est clairement posée.

Les limitations des architectures actuelles doivent être identifiées et des solutions envisagées dans le contexte du passage à l'échelle liée à l'IoT (infrastructures réseau, systèmes d'identification). Une des réponses possibles serait la migration vers IPv6.

Alors qu'elle dispose d'atouts particulièrement intéressants, l'Europe ne s'est pas encore positionnée comme force de propositions alternatives globales ou complémentaires à l'ONS américain ou à l'uID japonais. À travers la Commission européenne, elle a jusqu'ici essentiellement traité de l'IoT sous l'angle de la gouvernance et des problèmes de protection de la vie privée, ce qui ne permet pas à des acteurs économiques ou industriels européens d'émerger, et peut même s'avérer contreproductif (si cela devait conduire à diviser les Européens).

Aussi, apparaît-il essentiel que l'Europe contribue au plus tôt et de façon ambitieuse à l'émergence d'un Internet des objets européen.

Dans cette optique, la France et l'Europe doivent promouvoir le caractère ouvert, interopérable et non discriminatoire de ce nouvel Internet. Il conviendra en particulier de veiller à l'indépendance des structures de gestion et d'éviter les risques de capture de l'information par des acteurs dominants.

La gouvernance globale de l'Internet des objets pourra ainsi être partagée, neutre et indépendante, en s'appuyant sur des structures européennes autonomes qu'il reste à définir, incluant entreprises, utilisateurs, citoyens et autorités publiques compétentes.

CONCLUSION

Dans le monde de la distribution, la tendance lourde est à l'unification des canaux de distribution à travers l'approche dite *cross-canal*. Cela implique qu'il n'est plus pertinent d'opposer le commerce mobile (m-commerce ou m-shopping) au e-commerce, comme d'opposer le e-commerce au commerce traditionnel, ou encore le social-commerce au e-commerce. Ce sont toutes des composantes à part entière du commerce, qui est désormais une notion protéiforme.

Aujourd'hui, Internet est en train d'évoluer de façon similaire : l'Internet « du futur », l'Internet « nouvelle génération », l'Internet des marchandises, le M2M au sens large, les *smart grids*, l'Internet des objets, etc., sont autant de facettes d'un Internet en perpétuelle évolution.

Le vrai paradigme – celui de l'objet transportant lui-même les informations portant sur son propre cycle de vie/caractéristiques – n'est pas la piste retenue par les acteurs : malgré les enjeux qu'il recèle (nouveaux identifiants, passage à l'échelle, souveraineté des États, intelligence économique, protection des données personnelles, etc.), l'IoT ne procure qu'un niveau de granularité amélioré des informations, mais cela ne constitue pas une rupture.

Pas encore, tout du moins. Et lorsque cette rupture se produira, quelle forme prendra-t-elle ?

Après avoir financé *via* les programmes FP7 et ICP de nombreux projets (18) d'IoT qui se diluent pour la plupart dans des thématiques aussi diverses que la santé, le bâtiment, les transports, etc., et brossent des espaces technologiques hétérogènes comme le *Cloud Computing*, les réseaux de capteurs ou la filière du silicium, la Commission européenne semble prendre conscience des limites de l'exercice : à l'occasion d'une modification de son organisation, elle a mis un terme à son groupe d'experts sur l'IoT en novembre 2012 et considère que la réglementation existante doit suffire à couvrir les problématiques de l'IoT.

Serait-ce un signe des temps ?

(17) OID : système international hiérarchique d'identification principalement utilisé pour référencer des éléments d'information dans des communications électroniques. Le concept est normalisé conjointement par l'UIT-T et par l'ISO/CEI depuis 1985. Chaque entité responsable d'un arc, dans l'arborescence internationale, alloue des sous-arcs en fonction de ses besoins. AFNOR gère l'arc national pour la France, sous lequel beaucoup d'entreprises françaises ont enregistré un OID pour leurs besoins propres (cf. <http://www.oid-info.com>).

(18) À la mi-2011, la Communauté européenne avait consacré plus de 50 millions d'euros à des projets de R&D sur l'IoT (Neelie Kroes, Commissaire européen pour l'agenda numérique, in *IoT-Week*, Barcelone, juin 2011).

À la mi-2012, le Cluster européen de recherche sur l'IoT (IERC) rassemblait 42 projets (Cristina Martinez de la DG Connect, European Commission, 20 juin 2012. http://www.eurosfairer.prd.fr/7pc/documents/1341852459_03_obj_1_4_cristina_martinez.pdf).