# IoT : 2016, l'année du décollage

**Spécial Bilan 2016**. L'année qui s'achève restera comme celle de la confirmation pour le marché de l'IoT. Là où le RFID a bégayé pendant des années, handicapé par ses contraintes propres comme l'installation de portiques dédiés, ce qu'on appelle désormais l'Internet des objets – en réalité un cocktail de technologies assez variées – semble, lui, trouver rapidement sa vitesse de croisière. En milieu d'année, le cabinet d'études IDC relevait ainsi ses prévisions, anticipant désormais 145 milliards de dépenses dans l'IoT sur la seule année 2016. Et une croissance des investissements des entreprises en équipements, logiciels, services et connectivité au cours des 4 années qui viennent.

Plusieurs facteurs concourent à ce décollage. Un changement de l'offre d'abord. Avec, en particulier, l'émergence de réseaux alternatifs dits non cellulaires. Des réseaux généralement très bas débits et à longue portée (LPWA) dédiés aux objets connectés et déployés par des acteurs comme Sigfox ou par ceux réunis autour de la LoRa Alliance. Si leurs performances sont très limitées en termes de débit, ces réseaux présentent de multiples avantages pour les industriels. D'abord, ils sont mis en œuvre par des opérateurs qui fournissent le réseau radio et l'infrastructure de collecte des messages. Un souci en moins pour l'entreprise. En outre, le prix d'accès à ces réseaux est bien inférieur à celui des réseaux cellulaires (GPRS, 3G et 4G). Autre point clé, la consommation électrique bien plus faible. Loin d'être un détail puisqu'il devient possible de créer un objet connecté capable de fonctionner pendant des années sans entretien et sans source électrique extérieure. Selon le cabinet ABI Research, les connexions sur les réseaux LPWA dépasseront de 12 % celles sur les réseaux cellulaires classiques en 2021. Un indicateur du boom attendu des applications IoT sur ces infrastructures.

## 1 $ par an et par objet

Autre élément clef concomitant : la baisse du coût des capteurs. Star française sur ce marché en plein boom – avec une levée de fonds record de 150 millions d'euros en fin d'année – Sigfox envisage de dépasser les 100 millions d'objets connectés sur son réseau, en partie grâce à la baisse du coût des capteurs. « *On arrive à 1 dollar par an par objet, un prix satisfaisant pour nos clients. Le frein vient du coût des composants qui dépendent eux-mêmes des volumes. Avec des petits volumes, un module atteint les 10 dollars, ce qui est trop cher pour une diffusion massive des objets. A travers nos partenariats, nous avons pu descendre de 10 à 2 dollars. Et on ne désespère pas de diviser encore par deux ou quatre ce tarif dans les années à venir* », expliquait récemment dans nos colonnes Ludovic Le Moan, le patron de Sigfox. Le discours est identique du côté de la LoRa Alliance, portée en France par les opérateurs Orange et Bouygues Télécom (au travers de sa filiale IoT Objenious).

**[A lire aussi, notre dossier : La stratégie IoT des grands acteurs IT]**

Cet alignement des planètes technologiques a réveillé l'appétit des industriels. Lors du récent salon Smart Industries, qui se tenait à Paris début décembre, des fleurons de l'économie française comme Airbus, Michelin, Safran ou la SNCF exposaient leurs projets. S'y ajoutent les initiatives des constructeurs automobiles, en pleine révolution de la voiture connectée. Car, maintenant que les tarifs sont compatibles avec des déploiements à l'échelle industrielle, les scénarios d'usage se multiplient. « *Avec l'IoT, on étend le champ des possibles sur toute la chaîne de valeur en matière de*

*traçabilité*, expliquait ainsi Nicolas Monturet, architecte SI chez Airbus, lors de Smart Industries. *Mais on peut aussi amener de nouveaux usages, modifier l'expérience des passagers*. » Autrement dit, les usages sont à la fois internes et externes, à destination des clients finaux des entreprises. Selon une étude de l'éditeur SAS Institute auprès de 75 dirigeants de grandes entreprises en Europe, les scénarios d'utilisation vont du client connecté (cité dans 20 % des cas), à l'autodiagnostic (17 %) en passant par le suivi des ressources (16 %) ou l'optimisation de la chaîne logistique (14 %). « *Le domaine de la maintenance prédictive est d'ailleurs aujourd'hui identifié par de nombreux clients comme un facteur d'économie amené par l'IoT. Aux côtés de la logistique ou encore de la sécurité routière* », dit Stéphane Allaire, Pdg d'Objenious, la filiale IoT de Bouygues Telecom.

## Vendre un service, non plus un produit

Enjeu de transformation des produits en service, enjeu de montée dans la chaîne de valeur (comme ce concepteur de bacs plastiques pour médicaments qui, via l'ajout d'un capteur de température, fournit un service de transfert de responsabilité à ses clients) ou enjeu de collaboration à l'échelle d'une chaîne industrielle, les raisons poussant les industriels à s'intéresser au sujet sont diverses. Y compris dans des environnements où on ne les attend pas forcément, comme chez Vallourec, fabricant de tubes en acier sans soudures et de solutions tubulaires spécifiques. « *Le passage à l'IoT va faciliter un accès plus systématique aux données relatives à la vie du produit et nous permettre d'envisager de nouvelles optimisations* », résumait Renaud de Lapeyrière, le directeur du développement du groupe, sur le salon Smart Industries.

**[A lire aussi, notre dossier : IoT et automobile : les constructeurs pied au plancher]**

Chez Safran, l'attrait pour l'IoT résulte avant tout d'une adaptation à un changement de modèle économique. Plutôt que de commercialiser des équipements à des constructeurs aéronautiques, l'industriel leur vend désormais… des heures de vol. Or, pour y parvenir, la donnée devient un actif stratégique. Car, même si un A380, avion ultra-connecté, génère 800 000 paramètres, soit quelques Go de données par vol, il manque toujours certaines données ici ou là, selon Emmanuel Couturier, chef de programme innovation et business développement chez l'industriel. D'où l'intérêt pour l'IoT, qui permet d'acquérir des paramètres complémentaires, grâce à des réseaux comme LoRa ou Sigfox.

## Démarche d'amélioration continue

Il peut aussi s'agir de fournir un service additionnel à des clients, générant un chiffre d'affaires supplémentaire. C'est par exemple le cas de Michelin, qui a abordé l'IoT via le suivi des paramètres de pneus utilisés sur des installations minières (où les camions doivent fonctionner en permanence pour ne pas arrêter la production), de Colas Rail, pour le suivi de l'état des éclisses (la pièce de métal qui unit mécaniquement deux rails bout à bout, une éclisse défectueuse avait provoqué l'accident de Brétigny-sur-Orge), ou de Bosch. « *Mais recueillir des données permet aussi de mieux connaître le cycle de vie de nos produits et d'entrer dans une démarche d'amélioration continue* », dit Eric Payan, le DSI et Chief Digital Officer de Bosch.

**[A lire aussi, notre dossier : 5 scénarios pour l'Internet des objets en entreprise]**

Reste un nuage noir, un cumulonimbus géant : la sécurité des objets connectés. L'attaque contre le prestataire DNS Dyn, qui a rendu indisponibles quelques grands nom de l'Internet pendant plusieurs heures, a illustré le potentiel de réseaux d'objets connectés zombies, enrôlés pour mener des attaques DDoS (lire notre article « DDoS : la menace de moins en moins fantôme »). Or, de multiples objets disséminés sur le globe comportent des failles de sécurité grossières – comme ces login et mots de passe codés en durs dans des centaines de milliers de caméras -, les mettant à la portée de malwares spécialisés comme Mirai.

## Le DDoS n'est pas l'unique menace

Qui plus est, le DDoS n'est qu'un scénario d'attaque parmi d'autres. La corruption des objets – pour y implanter un malware, pour en réutiliser les clefs d'authentification, pour en corrompre les données… –, l'espionnage des communications, l'usurpation d'identités ou le blocage des connexions légitimes via des interférences sont également à considérer.

« *Dès qu'on aborde des cas d'usage en entreprise, convaincre les clients que le système est sûr et sécurisé est réellement crucial. Imaginons une compagnie travaillant dans la distribution d'eau et installant des compteurs communiquant ; si le système tombe en panne, elle ne peut tout simplement plus facturer ses clients* », illustrait Arnaud Vandererven, le responsable du réseau d'Objenious, lors du salon IoT Planet de Grenoble. La problématique est d'autant moins simple à appréhender que les capteurs déployés doivent ne coûter qu'une poignée d'euros, afficher une durée de vie d'environ 10 ans… et sont bâtis par un grand nombre de sous-traitants. Une chaîne d'intervenants pour laquelle le coût de la sécurisation doit, qui plus est, demeurer modique, faute de quoi c'est tout le modèle économique de l'IoT qui s'effondre. Logique donc de voir la Commission européenne s'intéresser au sujet. En marge d'une législation sur les télécoms, Bruxelles planche sur un corpus de règles qui devraient imposer aux constructeurs d'objets connectés de se conformer à des standards de sécurité et d'en passer par des certifications afin de garantir le respect de la vie privée des utilisateurs.

**L'année 2016 dans le rétroviseur :**

DDoS : la menace de moins en moins fantôme

Comment le ransomware est devenu le gagne-pain des cybercriminels

2016, une année en enfer pour SFR

2016, l'année des vols de données massifs

La longue marche de Microsoft pour imposer Windows 10 au marché

**crédit photo © a-image – shutterstock**