Lettre d'information N°111 – Mars 2023

L'Internet des objets au service de l'intelligence des immeubles

L'un des plus grands avantages que nous avons aujourd'hui est notre capacité à communiquer aisément les uns avec les autres. L'Internet des objets (ou *internet of things* – IoT) permet également aux machines, aux ordinateurs et aux appareils mobiles de communiquer entre eux, sans notre intervention… ou presque.

D'un point de vue technique, l'IoT est l'identification numérique normalisée (adresse IP, site http…) d'un objet physique grâce à un système de communication sans fil comme le Bluetooth, le Wifi, le RFID, la 5G ou tout autre réseau non-filaire.

Çà semble intéressant, pourtant les objets connectés peinent à s'imposer dans le quotidien des Français malgré l'augmentation de l'offre et la révolution des usages qu'ils promettent. Souvent perçus comme des gadgets dispensables, ils pâtissent aussi d'un coût élevé et de craintes liées à la sécurité des données personnelles. Autant de défis pour les acteurs d'un marché pourtant promis à un bel avenir depuis des années.

En fait depuis 2010, les experts et prospectivistes du monde entier ne cessent d'annoncer son essor imminent, à grands renforts de chiffres tous plus spectaculaires les uns que les autres. En 2015, le cabinet GfK prédisait que deux milliards d'objets connectés seraient vendus en France d'ici à 2020, soit... au moins trente par personne !

Décalage entre les attentes et la réalité

La démesure de ces promesses tranche avec la situation actuelle du marché. On est loin des chiffres avancés. Ainsi en 2018, derniers chiffres connus, les objets connectés orientés grand public ont représenté un marché de 1,1 milliard d'euros en France.

Pourtant, convaincus comme Sylvain ROLLAND *(lire en note 1)* que l'IoT est "*the next big thing*", les constructeurs et équipementiers du monde entier s'y sont mis. De plus en plus d'objets connectés apparaissent sur le marché et retiennent l'intérêt quand ils ne déclenchent pas une vague d'enthousiasme au moment de leur sortie. Certains objets connectés ont même été des stars du récent salon CES de Las Vegas, la grand-messe mondiale de l'électronique, qui vient de s'achever à Las Vegas *(lire en note 2).*

Souvent vus comme des "gadgets" par le grand public

Pour réaliser son immense potentiel, le secteur - encore adolescent - de l'internet des objets, qui se compose en réalité d'une multitude de sous-secteurs (communication 5G, domotique, sécurité des personnes, santé, smart city, automobile, systèmes intelligents pour les entreprises et les immeubles...), doit régler quelques problèmes qui freinent aujourd'hui son développement.

A commencer par la question de la valeur d'usage. Pour séduire les foules, il faut que le produit réponde à un réel besoin sinon seuls les geeks seront tentés. Le taux d'équipement du smartphone a dépassé la barre des 75% *(lire en note 3)* car de plus en plus de personnes veulent être connectées en permanence à leur messagerie, se géolocaliser dans la rue ou accéder aux réseaux sociaux partout. Or, le grand public ne considère toujours pas les objets connectés comme indispensables.

Posséder un assistant vocal à la maison pour entendre la météo, un store qui descend tout seul au premier rayon de soleil, une montre connectée enregistreuse d'activités ou un réfrigérateur qui envoie une alerte la veille de la date de péremption des yahourts reste perçu comme relevant du gadget.

Souvent perçus comme trop chers pour le service rendu

Qui est prêt à payer plus de 300 euros une montre connectée pour compter ses pas alors qu'un podomètre électronique en vaut moins de 30 ? Ou bien plus de 1.000 euros pour un lave-linge connecté alors que le prix moyen d'une grande marque est aux alentours de 500 pour un modèle … qui lave très bien et économiquement le linge.

Pour les spécialistes et experts du secteur, ce n'est qu'un problème passager car, de leur point de vue, le marché des objets connectés est dans la même situation que celle du téléphone mobile dans les années 1990, ou celle du smartphone il y a quinze ans. Ce n'est qu'une question de temps pour Jens HEITHECKER, directeur exécutif de l'IFA *(lire en note 4) :* "*Le marché se développe lentement. Mais combien de personnes ont dit dans les années 1990 : je n'aurais jamais besoin d'un téléphone mobile ?".*

Le problème de la sécurité

Autre frein à l'adoption massive des objets connectés : la sécurité et la confidentialité des données. Laisser des objets recueillir et analyser en permanence des informations extrêmement personnelles

nécessite un rapport de confiance entre l'utilisateur et l'entreprise qui collecte celles-ci. Ainsi, les traqueurs d'activités des smartphones ou des montres associées gèrent un nombre important de données sensibles relatives à la mobilité et à la santé des personnes, tandis que les objets de la maison intelligente détiennent des informations sur leur mode de vie.

Or, les entreprises qui collectent, analysent, stockent, gèrent voire monétisent ces montagnes de données sont très rarement connues des Clients et certaines d'entre elles reconnaissent que de nombreux objets connectés présentent des failles de sécurité, parfois majeures.

A tel point que la Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes a jugé utile d'éditer une fiche *(lire en note 5)* sur les risques auxquels les objets connectés exposent les consommateurs. Principalement centrés sur deux types de risque :

- l'utilisation commerciale des données personnelles et les atteintes à la vie privée sans consentement : une des conséquences de ce monde de réseaux et de communication est que nous laissons de plus en plus de traces numériques. Au-delà des progrès technologiques, il s'agit désormais de parvenir à garantir l'anonymat des données collectées par ces appareils et le droit à « l'oubli numérique » de leurs utilisateurs ;
- le piratage : dès lors que se connecter à internet devient une fonction intégrante d'objets du quotidien, les concepteurs de ces équipements doivent faire face aux risques des cybers-attaques et leurs utilisateurs doivent en être clairement informés et prendre conscience de leurs conséquences.

Le problème de la compatibilité.

Il n'existe actuellement aucune norme de compatibilité internationale au niveau macro pour l'internet des objets. Cela peut rendre difficile la communication de certaines machines entre elles, surtout si elles proviennent de fabricants différents. Bien sûr, les opérateurs IoT opèrent en coopération avec les constructeurs d'objets dans un état d'esprit de responsabilité partagée en matière de sécurité. Malheureusement, pendant que l'IoT continue de croître, les normes officielles ne suivent pas toujours aussi vite.

Toutefois, la famille de normes ISO/IEC 27000 est un socle solide *(lire en note 6).* Ainsi l'ISO/IEC 27001 est la norme la plus connue au monde pour les systèmes de management de la sécurité de l'information (SMSI) et leurs exigences. D'autres bonnes pratiques en matière de protection des données et de cyber-résilience sont couvertes par plus d'une douzaine de normes de cette famille 27000. Ensemble, associées au Règlement Général sur la Protection des Données (RGPD) applicable dans l'Union depuis 2018, elles permettent aux entreprises et organisations de tous les secteurs et de toutes les tailles de gérer la sécurité des actifs non physiques tels que les informations financières, la propriété intellectuelle, les données des personnes et les informations confiées par elles à des tiers.

Le besoin de fiabilité

Qu'elles soient conceptrices ou utilisatrices d'objets connectés, plus encore que pour le grand public (hormis les applications santé), l'enjeu de la fiabilité est primordial pour les entreprises.

Et c'est notamment dans les immeubles intelligents (smart buildings) qui désignent des infrastructures connectées proposant une gestion technique automatisée et optimisée, pour une réduction drastique des coûts d'occupation, une expérience utilisateur privilégiée et une performance énergétique

optimisée que se situent les vrais champs d'expérience de l'innovation et les relais de croissance du marché.

Une solution d'avenir dans l'immobilier

Plus encore que la maison individuelle, les bâtiments connectés sont une solution d'avenir non seulement pour les logements collectifs mais également pour les entreprises, collectivités et administrations pour leurs immeubles tertiaires ou industriels, ou les usines. Rendre intelligent un bâtiment consiste à l'équiper de centaines de mini-systèmes de détection capables de :

- surveiller des consommations d'énergies et fuites éventuelles des réseaux ;
- contrôler la température, la qualité de l'air et le taux d'humidité pour le confort des utilisateurs ;
- mesurer la présence des usagers pour optimiser l'occupation des locaux et assurer leur confort et leur sécurité ;
- ou encore surveiller l'état des équipements pour anticiper et automatiser les opérations techniques de maintenance ;
- etc…

Toutes ces données (ou data), collectées par une plateforme experte *(lire en note 7)* seront ensuite mises au service de prises de décision efficientes pour une gestion durable, économe et réactive de vos biens immobilièrs.

De la domotique à l'immotique : l'intelligence artificielle déjà aux commandes

L'efficience d'un smart building équipé d'un environnement IoT dépend en grande partie de la puissance de calcul et de l'expertise logicielle de la plateforme qui centralise et analyse les données afin d'automatiser le pilotage des équipements connectés. Dans le domaine résidentiel, la domotique permet l'automatisation d'une habitation en matière de sécurité et de confort.

Dans un bâtiment connecté, l'immotique (contraction d'"immeuble" et de « domotique") et la Gestion Technique du Bâtiment (GTB) sont intégrées au sein d'une plateforme unique, qui permet un pilotage global de l'immeuble dans l'ensemble de ses fonctions. Au-delà des protocoles d'automatisation, certaines plateformes intègrent déjà des solutions d'intelligence artificielle (IA), lesquelles permettent des décisions optimales en temps réel, le plus souvent sans intervention humaine.

Dans un tel bâtiment dit intelligent, il devrait être possible de connecter de façon simple et à moindre coût, des capteurs hétérogènes concernant le bien-être des usagers et la sureté des biens et des installations. Les technologies sans fil utilisées permettent une grande simplicité d'installation. L'absence de câblage qui exclue la nécessité de gros travaux est particulièrement intéressante dans le cas de la rénovation ou du changement d'usage d'un bien.

Les capteurs sont souvent discrets, déplaçables et très peu énergivores. Associés à un modèle de communication de type LoRaWan *(lire en note 8),* ils consomment très peu et disposent d'une autonomie de très longue durée liée à un coût de communication extrêmement bas. Ce modèle de communication gagne ainsi chaque jour en popularité dans le secteur du bâtiment parce qu'il permet un déploiement à grande échelle et une couverture réseau étendue et économique.

La gestion des cyber-risques et l'innovation doivent être sur un pied d'égalité.

Les objets connectés produisent de grandes quantités de données. L'ensemble de celles-ci est souvent regroupé sous le terme générique de « Big Data ».

Dès aujourd'hui, les données créées par les objets connectés sont devenues un marché gigantesque et des modèles commerciaux entiers reposent sur des milliers d'interfaces, ce qui pousse les opérateurs à investir de manière significative dans les capacités d'analyse afin de découvrir de nouvelles sources de valeur pour eux-mêmes et leurs clients. Données de reconnaissance faciale, d'accès aux installations du bâtiment ou de système de contrôle industriel… la gouvernance des données semble ne pas suivre le rythme au fil du temps.

Sur certains secteurs économiques, L'IoT est passé de la science-fiction à la réalité plus rapidement que prévu, et est désormais une source d'énormes opportunités pour la création et la capture de valeur, permettant d'innover plus rapidement, de prendre de meilleures décisions et d'offrir des produits et des services attrayants à leurs clients.

Mais dans tous les projets et toutes les applications, cyber-risque et innovation sont inextricablement liés : l'un ne doit pas être subordonné à l'autre.

Conclusion

Comme le dit Grégory ROUSSEAU, vice-Président chez l'éditeur de logiciel de cybersécurité WALLIX *(lire en note 9)* en se projetant dans le futur immédiat : *« fini le bâtiment qui servait uniquement à assurer un environnement de travail confortable aux salariés des entreprises ! En opérant sa transition numérique, il offre aujourd'hui davantage de services aux occupants. S'il va de cette manière gagner en flexibilité et boosté sa valeur globale, il est aussi exposé à certaines failles liées au numérique ».*

L'IoT ne doit pas être considéré comme la solution à tous les problèmes de contrôle et il n'y a pas – à ce jour - de guide de A à Z pour sa mise en œuvre et, comme déjà évoqué, tous les équipements ne seront pas compatibles. Il est donc important de toujours avoir en tête un objectif de résultat clair et tangible, de toujours considérer les systèmes d'automatisation des immeubles de façon holistique et, surtout, de s'assurer que l'équipement que vous comptez utiliser est ouvert, évolutif, sécurisé et qu'il est adapté aux réseaux de connection concernés, existants ou à coonstruire.

Donc, si vous prenez la décision de construire un bâtiment intelligent truffé d'objets connectés, ou d'en rénover un en ce sens, prenez bien soin de vous entourer d'experts pour vous accompagner dans l'écriture de vos besoins et de vous proposer les opérateurs aptes à s'engager à vos côtés dans cette transition numérique, aussi importante et couteuse que peut l'être la transition écologique mais dont les effets combinés avec cette dernière pourront vous apporter des résultats surmultipliés.

Si cette note d'information succincte éveille des attentes ou des questions au sein de votre collectivité, organisation ou de votre entreprise, DCR Consultants se tient à votre disposition pour accompagner votre réflexion vers ce que le marché attend et ce qui pourrait vous être profitable. Cordiales salutations.

Denis CHAMBRIER
Consultant Senior
denischambrier@dcr-consultants.com
Mobile : 06.7777.1883

Note 1 : Sylvain Rolland - La Tribune – Septembre 2015
Note 2 : CES 2023
Note 3 : INSEE 2021
Note 4 : IFA Berlin 2023
Note 5 : DGCCRF fiche pratique objets connectés
Note 6 : ISO 27001
Note 7 : exemple > REQUEA
Note 8 : LoRaWAN
Note 9 : WALLIX