Internet des objets : les usages face à la problématique sécuritaire (3)

Il faut rencontrer les acteurs français des objets connectés, concepteurs des 'devices' qui équipent l'Internet des objets, pour constater la vitalité de ce secteur porteur d'innovations… **Réunis par Freescale à Paris** lors de son séminaire *Designing with Freescale*, ils affichent pourtant une souffrance qui prend sa source dans le décalage entre l'innovation technologique qu'ils portent , les contraintes d'un marché soumis parfois au dictat de quelques gros opérateurs, et la réalité d'un domaine au riche potentiel mais qui peine à exploser.

A la question des usages, chacun y va de son expérience et de son métier. L'automobile, la santé, la cité numérique (principalement la gestion de la distribution de l'électricité, du gaz et de l'eau), la sécurité (vidéo surveillance, etc.), l'électronique grand public, les objets connectés envahiraient presque notre quotidien, si certains freins ne venaient tempérer leur marche en avant.

Des devices à la tracto-pelle

Combien sont-ils, tout d'abord, ces devices. Selon les analystes, les chiffres de 40, 50, voire dernièrement 120 milliards (pour la fin de la décennie), circulent ! Et sont en permanence ré-évalués à la hausse. Seuls les fabricants de composants pourraient nous fournir des chiffres précis, mais ils gardent jalousement cette information stratégique.

D'ailleurs les chiffres réels seraient peu intéressants, puisque dans la catégorie IoT (Internet of Things) prennent place les produits RFID – en particulier les étiquettes qui embarquent des données et une antenne – qui embarquent bien peu d'intelligence. Comme les experts que nous avons rencontrés l'ont rappelé, **supprimez le RFID et le ballon des dizaines de milliards d'objets connectés va rapidement se dégonfler**, tout en restant important au demeurant, et surtout en constante inflation.

Usages… tout reste à découvrir

En réalité, deux usages émergents du IoT dominent : la **collecte des données** et le **déclenchement**. Le premier consiste tout simplement à mesurer – en général des débits dont les sources peuvent être d'une très grande diversité (fluides, énergie, passages, températures, actions, etc.) – et à transmettre l'information. Le second est centré sur le pilotage des composants électroniques, comme par exemple l'ouverture ou la fermeture d'un volet roulant, d'un chauffage, d'un équipement de sécurité dans une automobile, etc.

Émerge également une tendance de fond, le Cloud Computing. Celui-ci apporte une même réponse à deux questions : où doit être la donnée et où doit-elle être traitée ? L'Internet des objets affiche en effet de grands besoins d'infrastructures. Un phénomène qui ne peut que s'accélérer car la prolifération des objets connectés s'accompagne d'une forte intégration et d'une baisse des coûts qui facilitent la création en masse de ces mêmes objets. En revanche, la sophistication qui en

découle ne peut plus être traitée au niveau du device. D'où le recours au cloud dont les infrastructures supportent la consolidation, l'analyse et les traitements complexes.

Automatiser la prise de décision

En terme d'usages, la multiplication des sources d'information, des capteurs, mais également des outils analytiques va permettre d'élever le niveau d'accompagnement à la prise de décision. Et c'est bien là qu'est la finalité technologique de la plupart des acteurs du marché : **permettre aux équipements de prendre seuls la bonne décision**, avec la compréhension de nos attentes ou de nos usages.

Un exemple – étonnant pour les uns, inquiétant pour les autres – est apporté par le 'smart meter', le compteur électrique intelligent. L'observation de notre consommation électrique peut apporter un nombre incroyable d'informations sur nos usages. Par exemple sur notre consommation de l'Internet, de la télévision, etc. Des chercheurs ont démontré que, moyennant l'exploitation d'outils analytiques puissants, ces informations peuvent aller jusqu'à l'identification des programmes TV consommés…

La sécurité en question

L'Internet des objets soulève nombre de questionnements. Mais le plus important porte certainement sur la **sécurité**. Beaucoup de produits connectés, dont certains que nous utilisons au quotidien, affichent un réel **manque de maturité**, et donc en corollaire de sécurité. Ce qui est mis en cause ici n'est pas le 'safety' – la qualité des devices ne se prête qu'à peu de risques, celui qu'un tableau électrique ne s'enflamme est quasi nul par exemple –, qui est reconnu de longue date par les industriels. Il n'en est pas de même pour le 'security', qui avec l'IoT prend sa source plutôt dans la connectivité et la communication.

Le phénomène est accentué par le passage de protocoles propriétaires à des protocoles communs, donc connus et largement partagés, qui facilitent l'introduction de failles de cyber sécurité. Le constat est sans appel, dans l'IoT, la disponibilité et l'intégrité des données, les infrastructures critiques, et jusque dans la distribution, les systèmes ne sont pas sûrs… Pire encore, dans les systèmes industriels, les spécialistes de la sécurité pointent le manque de prise de conscience des failles connues depuis longtemps !

Le frein sécuritaire

Si chacun reconnait que la partie sécurité doit être prise en compte dans le processus de développement d'un nouveau produit, elle n'est pas garantie car il y aura toujours des failles. La conséquence de ce constat est triple : la sécurité est un frein dans les processus de création de solutions de IoT, qui alourdit et limite les avantages attendus du 'time to market' ; soumis à des règles et restrictions plus nombreuses que dans d'autres régions du monde, les entreprises françaises qui innovent sur ce marché peinent à lancer et commercialiser leurs produits ; et la préoccupation sécuritaire handicape la facilité d'usage…

En complément :

Internet des objets : faire face à la prolifération des objets connectés (1)

Internet des objets : l'industrie face au manque de standardisation (2)

Voir aussi

Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes