



QUI A PARLÉ D'OBJETS CONNECTÉS INTEROPÉRABLES ?

La connectivité des objets est dominée par des technologies propriétaires, développées souvent hors normalisation technique ou juridique, posant des problématiques non triviales, notamment de sécurisation.



Avocat à la Cour d'appel de Paris, Frédéric Forster dirige le pôle Télécoms du cabinet Lexing Alain Bensoussan Avocats depuis 2006. Il était précédemment directeur juridique du groupe SFR. Il est également vice-président du réseau international d'avocats Lexing.

Les objets connectés constituent le maillon faible de nombreux systèmes informatiques, qu'ils soient personnels ou professionnels, privés ou publics. C'est le cas des connexions réalisées entre ces objets et les systèmes auxquels ils sont raccordés, lorsqu'elles utilisent la voie radio qui est très, voire trop, fréquemment basée sur des protocoles propres à chaque fabricant d'objets. Ainsi, pour un type de connexion radio donné (par exemple, le WiFi), il existe quasiment autant de protocoles de transmissions que de fabricants, rendant l'interopérabilité des objets interfabricants très complexe à organiser. Cette situation a conduit à une estimation étonnante selon laquelle un peu plus de la moitié seulement de la valeur dégagee

par les objets connectés serait exploitable, et cela, en raison de leur trop faible interopérabilité mutuelle et de l'écosystème d'utilisation. C'est pourquoi des réflexions sont menées afin de mettre en place des outils normatifs qui placent cette interopérabilité au-dessus de celle des objets eux-mêmes, et cela, grâce à des API (*application programming interfaces*) positionnées sur une plate-forme transversale, à laquelle les objets se connecteraient indépendamment de la technologie que chacun d'eux utilise. Ainsi, plutôt que de normer les interfaces pour la communauté des objets, l'idée est donc de ne pas en gommer les spécificités technologiques mais de les contraindre à se connecter à une plate-forme qui supprime ces hétérogénéités pour réintroduire une couche protocolaire minimale et commune, notamment au plan sécuritaire. Tel est le projet mis en avant par les huit principaux organismes de normalisation dans le secteur des TIC que sont Arib (Japon), Atis (Amérique du Nord), CCSA (Chine), Etsi (Europe), Tia (Amérique du Nord), TSDSI (Inde), TTA (Corée du Sud) et TTC (Japon).

Casser la fragmentation habituelle des technologies

Ce projet, intitulé OneM2M, a pour ambition de fournir un cadre technique commun aux acteurs de l'internet des objets, par une norme reconnue mondialement afin de casser la fragmentation habituelle des technologies. Ce projet n'est pas le seul puisque des industriels ont pris des initiatives de même nature. Citons,

par exemple, Qualcomm avec son projet open source ALLJoyn, qui aurait réussi à rassembler une centaine d'interlocuteurs comme LG, Sony, Canon ou Microsoft. Mais outre l'interopérabilité, les industriels se sont davantage penchés sur les applications offertes par les objets, leur ergonomie et les usages (réels ou supposés) que sur la sécurité. L'actualité montre que les piratages exploitent les failles de sécurité que laisse ouvertes la croissance exponentielle des objets connectés à laquelle s'ajoute la non-croissance, tout aussi exponentielle, de leur sécurisation. Ainsi, l'absence de norme induit la possibilité non seulement que des tiers accèdent à des données, notamment à caractère personnel, qui auraient dû rester protégées et secrètes, mais aussi que ces informations soient détournées des finalités pour lesquelles elles ont été collectées. Elles alimenteraient alors des bases de données occultes, autorisant toutes les dérives imaginables. Selon le Gartner, 80 % des objets connectés présentent de telles failles, ce qui, à quelques mois de la prise d'effet des dispositions du Règlement européen sur la protection des données personnelles, est évidemment hautement problématique. Il faut donc sécuriser les infrastructures auxquelles ces objets sont raccordés, par exemple, par des antivirus, firewalls, politiques de mots de passe robustes et tests réguliers d'intrusion. ■



« L'idée n'est pas de gommer le caractère technologique des objets mais de les contraindre à se connecter à une plate-forme qui supprime ces hétérogénéités pour réintroduire une couche protocolaire commune »