Ateliers « Référentiel IoT»

Le présent document constitue le bilan tiré par les services de l'Arcep des ateliers portant sur l'élaboration d'un référentiel de comparaison des objets connectés, qui se sont tenus les 11 et 14 décembre 2017.

Synthèse

Dans la continuité du livre blanc sur l'Internet des objets (IoT) publié en novembre 2016, les services de l'Arcep ont souhaité réfléchir aux actions qui permettront aux utilisateurs d'objets connectés de mieux comprendre les différences entre les solutions disponibles afin de pouvoir déterminer plus facilement l'offre la plus adaptée à leurs besoins. A cette fin, l'une des options identifiées consistait en la définition d'un référentiel de comparaison des solutions IoT, qui n'aurait pas vocation à être contraignant mais pourrait être librement utilisé par les fournisseurs d'IoT. Les services de l'Arcep ont ainsi organisé deux ateliers regroupant d'une part les utilisateurs, d'autre part les fournisseurs de solutions IoT afin de recueillir leur avis et de discuter de la pertinence des six axes de comparaison pré-identifiés : connectivité, protection des données personnelles, sécurité, consommation énergétique, pérennité, ouverture/interopérabilité.

A l'issue de ces ateliers, les services de l'Arcep considèrent que les discussions ont permis de confirmer le bien-fondé des axes de comparaisons proposés, qui reflètent bien les préoccupations des utilisateurs et les différences entre les technologies disponibles. Toutefois, l'élaboration d'un référentiel de comparaison quantitatif sur cette base et la définition des métriques associées paraissent difficilement atteignables à court terme, au vu de la diversité des cas d'usage auxquels les offres s'adressent, de la difficulté à mesurer certains axes (comme l'interopérabilité par exemple), ou du fait que certaines solutions IoT peuvent être définies sur mesure pour répondre au besoin spécifique d'un utilisateur particulier.

Par conséquent, les services de l'Arcep se fixent comme objectif d'élaborer un guide méthodologique d'accompagnement des utilisateurs de solutions IoT, qui visera à les aider à se poser les bonnes questions pour comparer qualitativement les offres disponibles et déterminer celle la plus adaptée à leurs besoins.

Introduction

L'Autorité de régulation des communications électronique et des postes (Arcep) cherche à accompagner et faciliter l'émergence de l'Internet des objets (aussi appelé *Internet of Things,* ou IoT), en identifiant et le cas échéant en levant les éventuelles barrières réglementaires qui empêcheraient son auto-organisation. A cette fin, l'Arcep a publié en novembre 2016 un livre blanc sur l'IoT, basé sur un cycle d'auditions et d'ateliers préparatoires, qui identifiait cinq principaux enjeux :

- Assurer une connectivité multiple, mobile, fiable
- Veiller à la disponibilité des ressources rares (fréquences, identifiants)
- Garder un jeu ouvert à tous
- Contribuer à bâtir la confiance autour des données
- Poursuivre le dialogue avec les acteurs de l'IoT.

Parmi les orientations définies par le livre blanc, figure l'élaboration d'un référentiel commun de comparaison visant à permettre aux utilisateurs d'objets connectés de mieux comprendre les différences entre les solutions IoT disponibles et de déterminer l'offre la plus adaptée à leurs besoins. A cette fin, les services de l'Arcep ont organisé en décembre 2017 deux ateliers consacrés à la réflexion autour d'un référentiel de comparaison des solutions IoT, qui se sont tenus en décembre 2017 et ont regroupé les participants suivants :

- Durant l'atelier « utilisateurs » : CNIL, Renault-Nissan, GRTGaz, Transdev, MedAppCare.
- Durant l'atelier « fournisseurs » : CNIL, Sigfox, Bouygues Télécom, Objenious, Verizon, Nokia, FIEEC, Arteria, SAP, Orange, AFNUM, Matooma, Qualcomm.

L'ébauche de référentiel proposée porte sur les trois couches qu'on distingue généralement, à savoir l'objet connecté (le terminal), le réseau (la connectivité), et la plate-forme (le stockage et le traitement des données). Il est composé de 6 axes, qui sont détaillés dans le support de présentation :

- La connectivité (couverture des émetteurs, débit, taux de livraison, risque de brouillage, facilité de déploiement…)
- La protection des données personnelles, qui vise d'une part à informer l'utilisateur sur le traitement de ses données personnelles, d'autre part à déterminer la capacité d'une solution IoT à traiter des données plus ou moins sensibles
- Le niveau de sécurité (niveau de chiffrement des données…)
- La consommation énergétique et la capacité de résilience en cas de rupture de l'alimentation énergétique

- La pérennité (durée minimale de maintenance, capacité à basculer vers d'autres technologies équivalentes, degré de dépendance vis-à-vis d'une entreprise en particulier…)
- L'ouverture (accessibilité d'un système à l'ensemble des acteurs, au-delà de son propriétaire) et l'interopérabilité (compatibilité entre les objets et entre les applications).

Il convient tout d'abord de bien cerner les limites de la démarche envisagée, qui ont été rappelées par plusieurs participants :

- Il n'est pas possible de chercher à établir un classement absolu des différentes solutions IoT : en effet, chacune possède ses propres caractéristiques techniques qui la rendent plus ou moins pertinente en fonction du cas d'usage recherché. Par conséquent, le référentiel devra être suffisamment adaptatif pour que l'utilisateur puisse choisir l'offre la plus pertinente en fonction de son usage spécifique.
- Le rôle de l'Arcep n'est pas d'influer sur le choix des technologies, qui doit être arbitré par le marché.
- Un référentiel de comparaison ne devra pas constituer une lourdeur administrative supplémentaire qui conduirait à brider l'innovation.

Les services de l'Arcep sont bien conscients de ces limites, mais notent également une demande générale de clarification, de la part des utilisateurs notamment, sur les technologies IoT et les solutions disponibles.

Connectivité et qualité de service

Le premier axe proposé par les services de l'Arcep pour faciliter la comparaison entre des offres IoT est la connectivité. On constate actuellement une profusion de technologies de connectivité, filaire ou sans fil, utilisant les bandes libres ou les bandes sous licence.

Les discussions ont permis de faire émerger trois indicateurs principaux sur ce plan qui intéressent les utilisateurs : la couverture (en intérieur ou en extérieur), le débit et le risque de brouillage.

La couverture et le débit sont des indicateurs classiques, qui peuvent être assez bien quantifiés et peuvent faire l'objet d'une garantie de la part du fournisseur, via un *Service Level Agreement* (SLA).

L'évaluation du risque de brouillage est un indicateur particulièrement important pour les utilisateurs, car les nouveaux appareils sous bande libres peuvent non seulement s'avérer inopérants si les bandes sont saturées, mais aussi conduire à troubler le fonctionnement des anciens appareils en place, posant ainsi un problème de rétrocompatibilité avec les technologies existantes. Plusieurs utilisateurs craignent

que l'augmentation exponentielle annoncée de la quantité d'objets connectés ne conduise à saturer les bandes, et ce quelle que soit la technologie employée. La quantification *ex ante* du risque de brouillage dans les bandes libres paraît cependant difficile, ne serait-ce que parce que ce risque est variable dans l'espace et dans le temps. En première approche, on peut toutefois distinguer, de manière binaire, d'une part les solutions utilisant les bandes libres, d'autre part les solutions utilisant les bandes sous licence. Ces dernières sont a priori plus coûteuses mais présentent un risque de brouillage plus limité et contrôlé.

D'autres indicateurs potentiels ont également été identifiés et discutés :

- Le nombre d'antennes du réseau, qui a l'avantage d'être basique, simple et facilement compréhensible. Il peut cependant être incomplet voire trompeur, dans la mesure où certains types de réseau ont besoin de beaucoup moins d'antennes pour avoir la même qualité de couverture, du fait de l'utilisation de bandes de fréquence différentes qui portent plus ou moins loin.
- Le taux de livraison des messages, qui peut être difficile à mesurer dans la mesure où il dépend beaucoup de la localisation (en intérieur, dans une cage métallique…).
- La compatibilité des technologies à l'étranger. L'utilisation de bandes de fréquence différentes pour une technologie donnée entre pays ou continents peut en effet être un critère de choix important, en particulier pour les objets de plus petite taille (bracelets connectés…) qui ne peuvent pas toujours détecter le continent où ils sont présents et utiliser la bande de fréquence appropriée aussi facilement que les plus gros objets.
- La sobriété d'exposition aux ondes électromagnétiques, qui peut constituer un critère de choix pour certains utilisateurs (en général les particuliers) et dans certains domaines (comme la santé).
- La possibilité de mettre en place des répéteurs pour améliorer la couverture, qui n'est pas autorisée pour toutes les technologies.
- La possibilité de faire du *roaming* via plusieurs opérateurs.

De manière transverse, plusieurs difficultés liées à l'évaluation de la connectivité d'une solution IoT ont été mises en évidence :

- L'évaluation de la couche « connectivité » d'une solution IoT indépendamment des couches « terminal » et « plateforme » peut s'avérer difficile : dans certains cas, une vision globale de l'ensemble des trois couches est nécessaire (par exemple pour la voiture connectée).
- Le champ des technologies à comparer étant très vaste, il pourrait être nécessaire de réduire le nombre de technologies prises en compte pour améliorer la lisibilité pour l'utilisateur (ce qui poserait cependant un problème d'égalité de traitement entre toutes les technologies).

Protection des données personnelles

Les objets connectés, de par leur nature même, recueillent de très nombreuses données qui sont souvent des données personnelles. Selon la CNIL, elles peuvent même révéler des informations très intimes, par leur accumulation notamment, même si elles peuvent sembler à première vue anodines lorsqu'elles sont prises individuellement. Le constructeur doit mener un travail pour qualifier ces données, et le cas échéant être en mesure de justifier la nécessité de leur collecte.

Dans ce contexte, l'enjeu de cet axe est double :

- d'une part, informer clairement l'utilisateur sur le traitement de ses données personnelles ;
- d'autre part, déterminer la capacité d'une solution IoT à traiter des données personnelles plus ou moins sensibles.

Les ateliers ont permis de s'interroger sur la nécessité et la pertinence d'inclure cette dimension dans le référentiel.

Certains arguments ont été avancés pour retirer cette dimension :

- La problématique de la protection des données personnelles n'étant pas spécifique à l'IoT, certains considèrent qu'elle n'a pas vocation à faire l'objet d'un traitement spécifique dans le référentiel proposé.
- Les solutions IoT devront obligatoirement respecter les textes européens qui imposent déjà des contraintes en matière de protection des données personnelles (RGPD notamment).
- La protection des données personnelles (respectivement la sécurité informatique) étant dans le champ de compétences de la CNIL (respectivement de l'ANSSI), certains considèrent qu'elles n'ont pas vocation à figurer dans un référentiel de l'Arcep.

À l'inverse, d'autres arguments militent pour son maintien :

- L'enjeu du référentiel pourrait être non pas de s'assurer du respect des textes législatifs et réglementaires européens et nationaux (supposé acquis), mais de permettre de distinguer les solutions IoT qui iraient au-delà des exigences minimales, par exemple en ne récoltant aucune donnée personnelle. Le référentiel pourrait aussi permettre de distinguer les objets connectés selon leur capacité à fonctionner en cas de refus par l'utilisateur de la collecte de ses données personnelles.
- La démarche du référentiel est de rassembler dans un lieu unique les différents éléments permettant de comparer les solutions IoT, y compris les éléments relatifs à la protection des données personnelles et à la sécurité, même si ceux-ci restent bien évidemment de la compétence de la CNIL et

de l'ANSSI. C'est pourquoi la démarche des services de l'Arcep se fait en coopération avec ces administrations. Cette démarche peut également aider à vulgariser le sujet auprès du grand public, afin que celui-ci se l'approprie plus facilement, comprenne pourquoi les données sont récupérées et puisse donner son consentement de manière éclairée.

Au total, les services de l'Arcep jugent préférable de ne pas écarter cette dimension du référentiel à ce stade de la réflexion.

Sécurité

Les failles de sécurité posent de véritables défis pour la maîtrise des données, qu'elles soient personnelles ou professionnelles. L'enjeu de cet axe du référentiel est de comparer la capacité des objets connectés à répondre aux exigences de sécurité des utilisateurs, par exemple grâce à la présence de protocoles de chiffrement des données, d'authentification, ou de certification via des labels.

Une difficulté majeure, quand on cherche à évaluer le degré de sécurité d'une solution IoT, réside dans la nécessité d'évaluer la protection de bout en bout : en effet, il suffit qu'un maillon de la chaîne de connexion soit vulnérable pour que la sécurité de l'ensemble soit compromise. Par exemple, le terminal peut présenter des failles de sécurité majeures, qui compromettent la protection des données récupérées par l'objet connecté. La plateforme a également un rôle important, car c'est à son niveau que la donnée collectée sera mise en relation avec l'identité du client. La sécurité dépend aussi des précautions que prend l'utilisateur final avec les données : il suffit par exemple que l'utilisateur stocke ses données en clair pour que la sécurité de la solution IoT dans son ensemble soit fragilisée.

Il faut signaler que des labels de sécurité existent ou sont en cours de définition dans différents pays européens. De manière générale, plusieurs participants signalent leur souhait que des labels équivalents délivrés dans d'autres pays d'Europe devraient avoir la même valeur que ceux délivrés en France, afin de faciliter les déploiements transfrontaliers. Des travaux visant à définir des labels communs au niveau européen sont en cours avec l'ENISA, ce qui pourrait résoudre cette difficulté.

En outre, vu la consommation d'énergie des mécanismes de chiffrement, certains objets autonomes à faible consommation d'énergie ne sont pas capables de proposer des solutions de sécurité satisfaisantes. Une analyse de risque, au cas par cas, est alors nécessaire.

Le développement de compétences en interne en matière de sécurité, plutôt que le recours à des sous-traitants, est jugé inévitable par certains participants pour assurer un niveau de sécurité satisfaisant.

Consommation énergétique

La consommation énergétique peut être un critère de comparaison important, surtout lorsque l'objet connecté est situé dans une zone difficile d'accès, ou quand le coût de changement des piles ou des batteries devient trop élevé. Le référentiel pourrait donc inclure cette dimension, via par exemple les sous-critères suivants :

- La consommation d'énergie en conditions d'utilisation standard ;
- Pour les objets non raccordés au réseau électrique, l'autonomie ;
- La résilience de l'objet en cas de coupure de courant (présence d'une batterie intégrée, capacité à garder les données en mémoire).

Cet axe est jugé pertinent par les utilisateurs. Toutefois, plusieurs difficultés pour le mesurer sont apparues :

- Tout d'abord, la consommation énergétique dépend beaucoup de la manière dont l'utilisateur utilise l'objet. Par exemple, un capteur de géolocalisation peut être réglé pour faire remonter des informations toutes les semaines, tous les jours, toutes les minutes... Les usages sont tellement vastes que la définition des cas d'usage risque d'être très difficile (contrairement à d'autres produits comme les réfrigérateurs ou les aspirateurs, qui sont des objets très similaires, avec des cas d'usage bien connus, et pour lesquels des indicateurs ont pu plus facilement être définis).
- Pour un cas d'usage donné, une même solution IoT peut se décomposer en plusieurs variantes avec des architectures techniques différentes (au niveau des modules par exemple), et donc des consommations énergétiques différentes. Ces variantes peuvent être construites de manière *ad hoc*, en fonction des besoins spécifiques des clients.
- Certains participants estiment difficile de déterminer le périmètre à prendre en compte pour calculer la consommation énergétique : par exemple, dans le cas de réseaux cellulaires IoT (comme le NB-IoT), il faudra décider si toute l'architecture LTE sous-jacente est à prendre en compte ou pas.

Une possibilité alternative serait de raisonner non pas à partir de la consommation énergétique, mais plutôt de l'efficacité énergétique, à savoir la consommation énergétique de la solution IoT rapportée à sa consommation énergétique optimale. Cette approche peut servir à évaluer l'évolution relative de la consommation de l'objet en fonction de son âge.

Pérennité

Le déploiement des objets connectés pourrait être entravé par le risque d'obsolescence ou de désuétude des technologies à long terme. Le référentiel pourrait faciliter la comparaison des objets connectés suivant cet axe, en indiquant par exemple :

- la capacité de la solution IoT à basculer vers d'autres technologies équivalentes, sans surcoût pour l'utilisateur ;
- le degré de dépendance vis-à-vis d'une entreprise en particulier (opérateur mobile, entreprise déployant le réseau…).

Les utilisateurs confirment l'importance de cette dimension dans le choix des solutions IoT. Concernant en particulier le déploiement du réseau, les utilisateurs signalent privilégier globalement les technologies multi-fournisseurs, qui permettent de ne pas être dépendant d'un seul fournisseur, l'idéal étant de pouvoir déployer eux-mêmes leur propre réseau. Concernant les données recueillies, les utilisateurs jugent essentiel de pouvoir conserver ses données au niveau de la couche plateforme pour continuer à les traiter et maintenir son activité en cas de défaillance du prestataire de la solution IoT. Enfin, les utilisateurs signalent qu'obtenir de la part des opérateurs des engagements sur la durée de vie des réseaux peut s'avérer difficile.

À l'inverse, d'autres arguments militent contre le maintien de cet axe dans le référentiel :

- il existe déjà une garantie légale de conformité qui protège les consommateurs contre tous les défauts de conformité existant à la date de livraison du produit, pendant une période de deux ans. Cette garantie est applicable aux contrats conclus entre un consommateur et un vendeur professionnel portant sur la vente de biens mobiliers corporels et de fourniture de biens à fabriquer ;
- dans le cas des industriels, la pérennité de la solution IoT choisie (durée de maintenance de l'objet, des technologies utilisées, de l'environnement matériel et logiciel) fait généralement l'objet d'un engagement contractuel avec le prestataire.

Les services de l'Arcep jugent utile de garder cette dimension dans le référentiel dans la mesure où elle représente une préoccupation forte pour les utilisateurs, même si elle ne pourra pas forcément être quantifiée.

Ouverture et interopérabilité

L'enjeu de cet axe est de quantifier la richesse de l'écosystème auquel l'objet connecté donne accès, en s'intéressant aux notions d'ouverture (qui désigne l'accessibilité d'un système à l'ensemble des acteurs, au-delà de son propriétaire) et d'interopérabilité (qui désigne la compatibilité entre les objets et entre les applications).

Cet axe pourrait être évalué par les critères suivants :

- capacité de l'objet connecté à basculer vers une autre technologie, vers un autre opérateur (ex : cartes SIM virtuelles) ou vers une autre plateforme ;
- capacité de l'objet à communiquer avec d'autres objets hétérogènes (de fonction différente, de marque différente), à accéder à différentes plateformes ;
- degré de portabilité des données ;
- degré d'ouverture des standards utilisés par les technologies de communication et d'adressage.

Les utilisateurs indiquent privilégier globalement les écosystèmes ouverts et les solutions open-source. De leur point de vue, une solution IoT sera d'autant plus appréciée qu'elle présente les caractéristiques suivantes :

- les données stockées au niveau de la couche « plateforme » sont réutilisables si la solution IoT utilisée change ou devient obsolète. En particulier, un changement de capteurs doit être le plus indolore possible, et notamment ne doit pas nécessiter une mise à jour complexe des algorithmes de traitement de données ;
- la solution IoT ne crée pas de dépendance vis-à-vis d'un unique fournisseur (comme ce serait le cas dans un écosystème fermé) ;
- la solution IoT permet à l'utilisateur de garder la main sur les données (celles-ci concentrent en effet de plus de plus de valeur). Les offres en apparence gratuites mais qui récupèrent de nombreuses données peuvent s'avérer en réalité moins intéressantes ;
- la solution IoT permet de croiser des données de natures différentes.

Bien que jugé pertinent, cet axe pourra s'avérer difficile à quantifier précisément.

Conclusion

Les utilisateurs soulignent un manque de connaissance global sur les cas d'utilisation des technologies, et un intérêt pour que puissent être développées des outils pour comparer les solutions IoT, en fonction des différents cas d'usages.

Les services de l'Arcep retiennent de ces ateliers que les questions posées et les axes mentionnés sont pertinents, et reflètent bien les préoccupations des utilisateurs, mais que l'élaboration d'un référentiel sur cette base et la définition des métriques associées restent complexes et lourds à mettre en œuvre. **Les services de l'Arcep envisagent donc dans un premier temps d'élaborer un guide d'accompagnement des utilisateurs d'IoT, afin que ceux-ci puissent se poser les bonnes questions au moment de déterminer la solution la plus adaptée à leurs besoins.**

Un tel guide d'accompagnement pourrait en outre permettre d' « enlever l'anxiété » qui apparaît parfois autour de l'IoT, du fait de la multiplicité des objets et des technologies, alors qu'au fond les questions posées en terme d'obsolescence, de

protection des données ou de compatibilité sont classiques et se retrouvent dans de nombreux autres domaines.