

CONSULTATION PUBLIQUE

Du 19 juillet au 16 septembre 2016

PROJET DE LIVRE BLANC – PREPARER LA REVOLUTION DE L'INTERNET DES OBJETS

Document n°1 – Une cartographie des enjeux

19 juillet 2016



Préambule : modalités pratiques de consultation publique

La présente consultation publique est ouverte jusqu'au 16 septembre 2016 à 18h00. L'avis des acteurs du secteur est sollicité sur l'ensemble du document mis en consultation par l'Autorité et ses partenaires. Seules les contributions arrivées avant l'échéance seront prises en compte.

Les réponses doivent être transmises à l'Arcep de préférence par courrier électronique en précisant l'objet « Réponse à la consultation publique « Document N°1 du livre blanc sur l'internet des objets » » à l'adresse suivante : iot@arcep.fr.

Elles peuvent également être transmises :

Par courrier à l'adresse suivante :

Autorité de régulation des communications électroniques et des postes
à l'attention de Monsieur Benoit LOUTREL, Directeur général
7, square Max Hymans
75730 Paris Cedex 15

Sur le site internet de l'Arcep dédié à l'internet des objets : <http://www.arcep.fr/iot/>

L'Arcep, l'ANFR, l'ANSSI, la CNIL, la DGALN, la DGE et France Stratégie, dans un souci de transparence, publieront l'intégralité des réponses qui leur auront été transmises, à l'exclusion des parties couvertes par le secret des affaires. Dès lors que leur réponse contiendrait de tels éléments, les contributeurs sont invités à transmettre leur réponse en deux versions:

une version confidentielle, dans laquelle les passages couverts par le secret des affaires sont identifiés entre crochets et surlignés en gris : «une part de marché de [25]» ;

une version publiable, dans laquelle les passages couverts par le secret des affaires auront été remplacés par «...» : «une part de marché de «...»%».

Les contributeurs sont invités à limiter autant que possible les passages couverts par le secret des affaires. L'Autorité et ses partenaires pourront déclasser d'office des éléments d'information qui par leur nature ne relèvent pas du secret des affaires.

LIVRE BLANC – PREPARER LA REVOLUTION DE L'INTERNET DES OBJETS

Document n°1 – Une cartographie des enjeux

Introduction

L'internet des objets (ou IoT pour *internet of things*) est au centre de l'attention des consommateurs et des entreprises. Et pour cause, la promesse d'un monde peuplé d'objets connectés offre d'innombrables opportunités par les possibilités offertes, en tant qu'utilisateur comme en tant que fournisseur de service.

De nombreuses études annoncent une explosion du volume d'objets connectés dans le monde d'ici 2020. Ainsi, l'IDATE¹ anticipe 80 milliards d'appareils connectés d'ici 2020, CISCO² en envisage 50 milliards tandis que Gartner³ en prévoit 26 milliards. Bien qu'une forte vigilance reste nécessaire à la lecture de ces chiffres, tant les définitions de périmètre varient, ceux-ci confortent néanmoins une tendance au déploiement massif des objets connectés.

La notion même d'internet des objets, qui est sujette à interprétation, mérite d'être précisée. Dans le cadre de ce rapport, une acception large du terme internet des objets sera retenue, correspondant à un ensemble d'objets physiques connectés qui communiquent *via* de multiples technologies avec diverses plateformes de traitement de données, en lien avec les vagues du *cloud* et du *big data*.

Les données et leurs utilisations sont en effet au centre de l'internet des objets. Celles-ci, extraites des divers terminaux et capteurs, permettent d'informer les utilisateurs en temps réel de l'évolution de leur environnement. Au-delà de la simple mise à disposition d'informations, l'agrégation de la multiplicité de ces données provenant de sources hétérogènes permet de quantifier l'environnement connecté pour dégager des tendances, enrichir les usages ou en envisager de nouveaux. L'utilisateur – individu ou entreprise – dispose grâce à l'internet des objets de la possibilité d'agir en temps réel sur son environnement – de manière manuelle ou automatisée – pour optimiser des processus (par exemple, optimisation de flux routiers ou de chaînes logistiques en temps réels).

Les pouvoirs publics entendent faciliter l'adoption de l'internet des objets et lever les éventuelles barrières pour que les entreprises françaises et européennes fassent partie de l'écosystème en cours de constitution au niveau mondial. L'émergence de l'internet des objets amène à considérer une multitude de problématiques et nécessite une coordination entre diverses institutions. L'Arcep a ainsi tenu à s'associer aux partenaires publics les plus concernés par l'internet des objets : l'Agence nationale des fréquences (ANFR), l'Agence nationale de la sécurité des systèmes d'information (ANSSI), la Commission nationale de l'informatique et des libertés (CNIL), la Direction Générale de l'Aménagement, logement et nature (DGALN), la Direction Générale des Entreprises (DGE) et France Stratégie. En effet, si l'on décline les différents volets de l'internet des objets, il apparaît que la connectivité et les réseaux reposent sur la gestion de ressources rares tandis que naissent des enjeux de sécurité, propres aux différents types d'objets, aux réseaux qui les portent et à leur destination, des enjeux de confiance, propres aux nouveaux types de données collectées impactant plusieurs

¹ *Internet of Things - A key pillar of digital transformation*, Idate research, Octobre 2015

² *The Internet of Things - Vertical Solutions*, Cisco, Février 2015

³ <http://www.journaldunet.com/ebusiness/le-net/previsions-gartner-objets-connectes-1213.shtml>

catégories d'utilisateurs, ainsi que des enjeux de développement des entreprises françaises et européennes.

Déjà des applications concrètes de l'internet des objets

Les applications de l'internet des objets se traduisent par de nombreux usages concrets - nouveaux ou améliorés - impactant significativement le quotidien des individus, des entreprises et des collectivités. Les bénéfices potentiels attendus facilitent son adoption par cette diversité d'utilisateurs. Plusieurs filières, ou marchés porteurs, ressortent, notamment :

- Les territoires dits « intelligents » sont au cœur des projets des collectivités et devraient permettre d'optimiser la gestion des infrastructures communicantes (transport, énergie, eau, etc.) pour amener un meilleur service aux administrés et respectant les objectifs de développement durable au sein des territoires ;
- Grâce à l'internet des objets, les logements et lieux de travail deviennent plus confortables, plus faciles à gérer et moins coûteux à l'usage. Le bâtiment connecté, incluant la maison connectée, offre notamment des possibilités de contrôle des consommations énergétiques, d'intégration des systèmes de sécurité et de confort accrus ;
- L'industrie du futur (l'utilisation de l'internet des objets au service des moyens de production) connaît un développement progressif. La relève d'information en constitue la première étape. La rétroaction et la commande à distance sont des phases plus complexes à mettre en œuvre dans certains domaines d'activité ;
- Le véhicule connecté, pour lequel de premières applications ont déjà vu le jour, a lui aussi franchi une première étape de lecture des informations grâce à l'intégration de l'électronique embarquée de longue date. Les acteurs de la filière automobile cherchent aujourd'hui à développer de nouveaux modèles économiques pour tirer parti de ces nouvelles possibilités tandis qu'affleurent les questions liées aux responsabilités ;
- La santé connectée, incluant le segment « bien-être », fait partie des applications auxquelles le grand public est le plus sensibilisé, notamment grâce aux *wearables*. Les aspects liés à la protection des données personnelles focalisent l'attention, du fait de la collecte d'informations personnelles particulièrement intimes - voire de santé - et nouvelles par des acteurs privés et des enjeux que représente leur exploitation, notamment par certains services. Les apports technologiques sur l'organisation des soins et sur le degré d'implication des professionnels de santé est également un sujet d'attention. Les mutations permises par l'évolution des technologies souvent plus rapides que les évolutions sociales et réglementaires rendent ce secteur plus difficile à appréhender et plus complexe ;
- L'entreprise agricole utilise d'ores et déjà l'internet des objets dans son processus de production. À travers des capteurs d'état du végétal, des animaux ou du milieu, des capteurs embarqués sur les machines agricoles, des outils d'aide à la décision ou de guidage des engins, les agriculteurs utilisent de plus en plus d'outils connectés dans leur travail quotidien.

Un levier pour l'économie française et un rôle à jouer pour les pouvoirs publics

Au-delà des filières identifiées ci-dessus, l'internet des objets détient un potentiel d'application très large, à même d'affecter positivement l'ensemble des secteurs de l'économie. En ce sens, l'internet des objets peut être considéré *per se* comme une nouvelle filière, transversale, elle-même génératrice de revenus et d'emplois.

La France apparaît particulièrement dynamique sur l'ensemble de cet écosystème en cours de création. Forts du constat de ce démarrage réussi, les pouvoirs publics souhaitent accélérer la disponibilité de ces services au bénéfice des entreprises et des citoyens et faciliter la poursuite du développement des entreprises nationales à l'échelle européenne et mondiale.

L'Arcep a fait de l'internet des objets l'un des chantiers prioritaires de sa revue stratégique⁴. L'objectif pour l'Autorité est de favoriser l'auto-organisation de l'écosystème en identifiant et en anticipant les éventuelles décisions structurantes qui devraient être prises. Elle a initié en ce sens une démarche partagée avec d'autres institutions concernées par l'émergence de cette nouvelle filière. Il s'agit avant tout de connaître, de comprendre et de faciliter le mouvement autour de l'internet des objets.

Cette démarche s'est traduite par la tenue d'une trentaine d'auditions⁵, puis par l'organisation d'ateliers⁶ portant sur différentes filières à potentiel précitées. L'Arcep et ses partenaires institutionnels ont ainsi recueilli les problématiques des acteurs de l'écosystème et dressé le présent état des lieux

Conjointement, l'Arcep publie ses propres orientations visant à accompagner l'émergence de l'internet des objets.

Parallèlement, des travaux autour de l'internet des objets ont été amorcés par diverses institutions, en particulier par la Commission européenne et l'Organe des régulateurs européens des communications électroniques (ORECE) et par le Groupe européen pour la politique du spectre (RSPG). Le présent document s'inscrit pleinement dans le calendrier des travaux européens et l'Arcep vise ici à nourrir cette démarche autour d'un sujet par nature transnational.

⁴ Conclusions de la revue stratégique de l'Arcep, Arcep, Janvier 2016 - <http://www.arcep.fr/larceppivote/larcep-presente-les-conclusions-de-sa-revue-strategique/>

⁵ La liste des auditions est donnée en annexe n°1

⁶ La liste des participants aux ateliers est donnée en annexe n°2

1 L'écosystème de l'internet des objets

L'internet des objets pourra autant permettre à des éléments de la maison de communiquer des informations à l'attention de l'utilisateur qu'aux véhicules de communiquer entre eux ainsi qu'avec les territoires intelligents qu'ils traverseront. C'est également grâce aux solutions de l'internet des objets que certains individus pourront contrôler leurs données de santé ou que les industriels optimiseront leurs processus opérationnels. Les auditions ont ainsi montré la grande diversité de l'écosystème de l'internet des objets dont les cas d'usage tout aussi variés dessinent un éventail très large d'exigences en termes de technologies (bas débit, haut débit) et sécurité (données et intégrité des réseaux), de couverture et de modèles d'affaires.

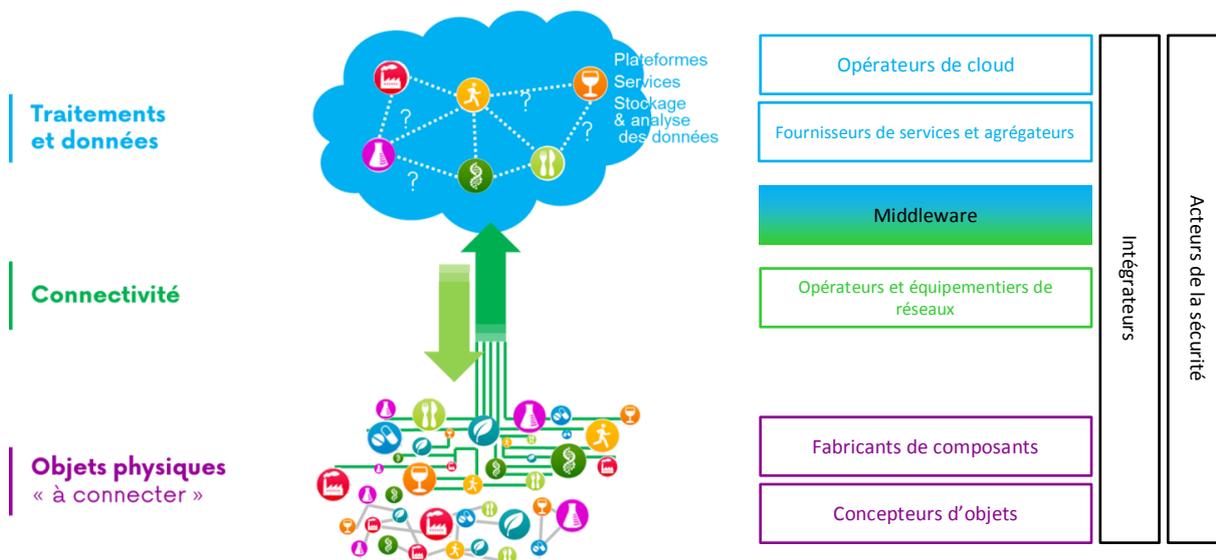
Une spécificité de l'internet des objets est qu'il mobilise aussi bien des problématiques « grand public » que des enjeux propres au monde de l'entreprise, de l'industrie et des services. Les modèles d'affaires développés et envisagés, et les chaînes de valeur qui en découlent, sont ainsi autant B2B et B2B2C que B2C, ce qui a des conséquences importantes sur la structuration de l'écosystème et sur la captation de la valeur dans les applications liées à différents secteurs économiques.

1.1 Un écosystème large, entre objets, communications et traitement de données

L'internet des objets se situe à la confluence des secteurs de l'informatique et des communications électroniques, où tout objet communique, peut être interrogé, envoie de l'information et interagit. L'Union Internationale des Télécommunications (UIT) définit ainsi en 2012 l'internet des objets comme une « *infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution* ».

De manière plus pragmatique, l'internet des objets correspond à un ensemble d'objets connectés, de communications et d'internet, qui se conjugue avec les vagues du *cloud* et du *big data* :

- Les objets physiques possèdent des technologies embarquées de capteurs, d'intelligence et de connectivité, leur permettant de communiquer avec d'autres objets ;
- Les réseaux de communications électroniques permettent de transporter les données issues des objets ;
- L'informatique, plus ou moins distribuée, apporte les outils pour le stockage, la corrélation et l'analyse de ces données. C'est d'ailleurs souvent dans ce *cloud* que se trouvent les processus décisionnels à même de rétroagir sur les objets physiques.



Différents volets à considérer dans l'internet des objets

La nébuleuse de l'internet des objets est constituée d'une multitude d'acteurs, issus de secteurs différents et fonctionnant ensemble afin de constituer ce nouveau pan d'activité économique :

- Les concepteurs et fabricants d'objets à connecter ;
- Les fabricants des composants de modules, qui apportent la connectivité aux objets via des composants matériels et logiciels embarqués. On trouve parmi ces acteurs les électroniciens, les fondeurs de semi-conducteurs, les fabricants de capteurs ou encore les développeurs de logiciels embarqués assurant la connectivité ;
- Les opérateurs et équipementiers de réseaux permettant de connecter les objets et les services du cloud. On retrouve sur ce segment les acteurs historiques des communications électroniques, à savoir les opérateurs, qui disposent déjà de réseaux qu'ils adaptent pour de nouveaux usages dédiés à l'internet des objets, ainsi que leurs équipementiers traditionnels. Ce segment inclut également des acteurs moins impliqués traditionnellement dans les communications électroniques, comme les gestionnaires de réseaux d'énergie qui mettent à disposition leurs infrastructures de réseaux pour y déployer de nouvelles technologies de communications, ou encore des entreprises nées avec l'internet des objets qui développent leurs propres réseaux dédiés ;
- Les opérateurs de cloud assurant principalement le stockage et le traitement des données brutes. Sur ce segment, les acteurs historiques de l'Internet et des serveurs sont concurrencés par de nouveaux acteurs déployant leurs propres infrastructures informatiques ;
- Les fournisseurs d'interfaces logicielles, ou de *middleware*, permettant de faire communiquer les différents objets. On retrouve sur ce segment des éditeurs traditionnels de logiciels ;
- Les intégrateurs qui orchestrent l'ensemble des briques précédentes en assemblant d'abord les différentes couches physiques – objets et capteurs – pour concevoir le produit final, puis peuvent le relier via les réseaux au *cloud*, d'où il est géré et où ses données sont stockées et analysées pour être ensuite exploitées en vue de futurs services. On retrouve sur ce segment les intégrateurs classiques du monde informatique ;

- Les fournisseurs de services et agrégateurs de données qui exploitent les données des utilisateurs générées par les objets pour répondre à leurs besoins. Les éditeurs classiques de plateformes numériques se sont positionnés sur ce segment ;
- En parallèle, les acteurs de la sécurité, présents à tous les niveaux de la chaîne, depuis la conception de l'objet jusqu'aux services. Dans le meilleur des cas, ces acteurs issus du monde de la sécurité informatique travaillent en étroite collaboration avec tous les acteurs de la chaîne de valeur. Certains sont par ailleurs absorbés par les acteurs de l'internet des objets.

L'ensemble des acteurs mentionnés ci-dessus proposent des offres que les utilisateurs intègrent dans leurs quotidiens. On observe trois grandes catégories d'utilisateurs : les entreprises, les collectivités locales et les particuliers.

Le cycle d'auditions a montré un écosystème où les acteurs essaient encore de se positionner au sein du marché ; certains explorent des intégrations ou des partenariats dans les différentes briques constituant l'internet des objets.

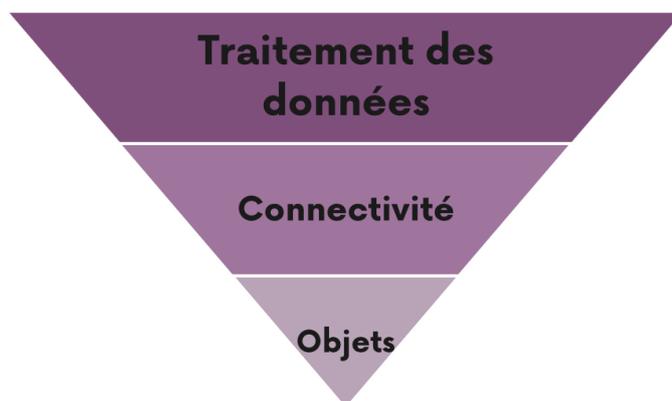
Cette volonté de couvrir l'ensemble de la chaîne de valeur peut s'expliquer par la recherche :

- de différenciation entre concurrents afin de convaincre les utilisateurs dans l'adoption de leurs solutions ;
- d'une part plus importante du marché, en proposant des offres maîtrisées de bout en bout ;
- d'un positionnement sur le segment où se trouve la plus grande partie de la valeur.

1.2 La valeur de l'internet des objets tirée par les données

La valeur de l'internet des objets s'articule autour des trois grands volets définis précédemment : objets, connectivité et traitements & données.

La connectivité, c'est-à-dire les réseaux et leurs équipements, semble être la couche la plus avancée de l'internet des objets. La connectivité est d'ores et déjà présente dans le quotidien des utilisateurs qui disposent d'une interface pour interagir avec l'internet des objets, *via* leurs smartphones et tablettes ; en France, 58% de la population utilise un smartphone⁷. Cette connectivité s'organise autour d'une multitude de réseaux qui permettent de couvrir le territoire à des échelles locales et nationales. L'émergence d'une grande diversité de réseaux et de cas d'usage rend le volet de la connectivité concurrentiel. Néanmoins, deux autres niveaux de concurrence restent à venir : entre les acteurs et entre les standards.



Quant à elle, la couche des objets est encore en mutation. D'un côté, les évolutions technologiques de ces dernières années ont rendu les capteurs plus performants et accessibles à des prix réduits. À

⁷ Source : CREDOC, Enquêtes sur les « Conditions de vie et les Aspirations »

titre d'exemple, le prix des capteurs a été divisé par deux en 10 ans⁸ ; il devrait continuer à baisser. D'un autre côté, des solutions techniques restent à développer pour répondre à des besoins plus complexes, exigeant souvent des débits ou une qualité de service supérieurs, comme le véhicule connecté ou certains usages industriels critiques.

Enfin, dans le domaine du traitement des données, qui devrait porter l'intelligence associée à l'internet des objets, tout reste à organiser pour les acteurs du marché, dont le positionnement n'est pas encore stabilisé. Le cycle d'auditions mené par l'Arcep et ses partenaires a fait ressortir un consensus assez large selon lequel la majorité de la valeur de l'internet des objets, au sens des revenus, devrait revenir au dernier volet de l'internet des objets, à savoir le traitement des données conduisant à la production de services. En effet, l'innovation pourrait se concentrer sur ces couches hautes où beaucoup reste encore à créer : nouveaux services pour les industriels, les collectivités territoriales mais aussi pour le grand public. En termes de revenus, même si la répartition de la valeur ne semble pas encore claire, ce sont également les activités liées aux données qui devraient en attirer une part importante à moyen terme. L'étude menée par A.T. Kearney⁹ conforte cette expectative et situe les futurs revenus de l'internet des objets sur les couches hautes. En particulier, d'après cette même étude, près de 56 milliards d'euros devraient revenir d'ici 2025 aux activités liées au traitement des données (services, agrégation des données et intégration des systèmes), incluant notamment les acteurs du cloud et les intégrateurs, quand les revenus associés à la connectivité pèseraient pour 15 milliards d'euros et ceux associés à la couche objets, au sens des composants, pour 10 milliards d'euros.

Cette répartition des revenus générés par l'internet des objets place la donnée au centre de l'économie de l'internet des objets. La valorisation de la donnée pourra s'effectuer à deux niveaux : d'abord, auprès de chaque utilisateur pour une collecte et une exploitation propres des données – notamment pour les entreprises –, ensuite *via* une exploitation massive des données qui permettra, en agrégeant celles de plusieurs utilisateurs, de proposer des solutions intelligentes. En effet, les données seront d'autant plus valorisées si elles sont contextualisées et mises en relation au sein d'un environnement permettant dans un premier temps de les faire communiquer avec d'autres données issues des différents objets d'un même utilisateur, et, dans un second temps, de les faire communiquer avec des données similaires relatives à d'autres utilisateurs.

Face à ces perspectives, on distingue deux modèles économiques autour de la donnée : la vente des données ou la monétisation des données avec la vente d'un service. Dans le premier cas, la vente des données pourra se faire auprès d'acteurs économiques, utilisateurs ou non. Certains acteurs pourraient être intéressés par la collecte des données brutes, qu'ils analyseraient eux-mêmes par la suite ; d'autres pourraient être demandeurs de données déjà exploitées. Un exemple pourrait être celui des compagnies d'assurance, qui souhaitent acquérir et utiliser des données afin de mieux cibler leurs offres et calculer les risques afférents. Un autre exemple pourrait être celui de la récupération des données par les fournisseurs de solutions de l'internet des objets afin de proposer à l'utilisateur des services gratuits, accompagnés par exemple d'une publicité ciblée, ou bien de proposer un modèle *freemium* où les premières fonctionnalités seraient gratuites et celles plus avancées seraient payantes. Dans le deuxième cas, l'économie de l'internet des objets pourra se faire *via* des services vendus directement. Dans ce cas, les données seront directement valorisées auprès de l'utilisateur final.

⁸ D'après le rapport « Internet des objets, les *business models* remis en cause ? », Oliver Wyman (2015)

⁹ *The Internet of Things : A new path to European prosperity*, A.T. Kearney

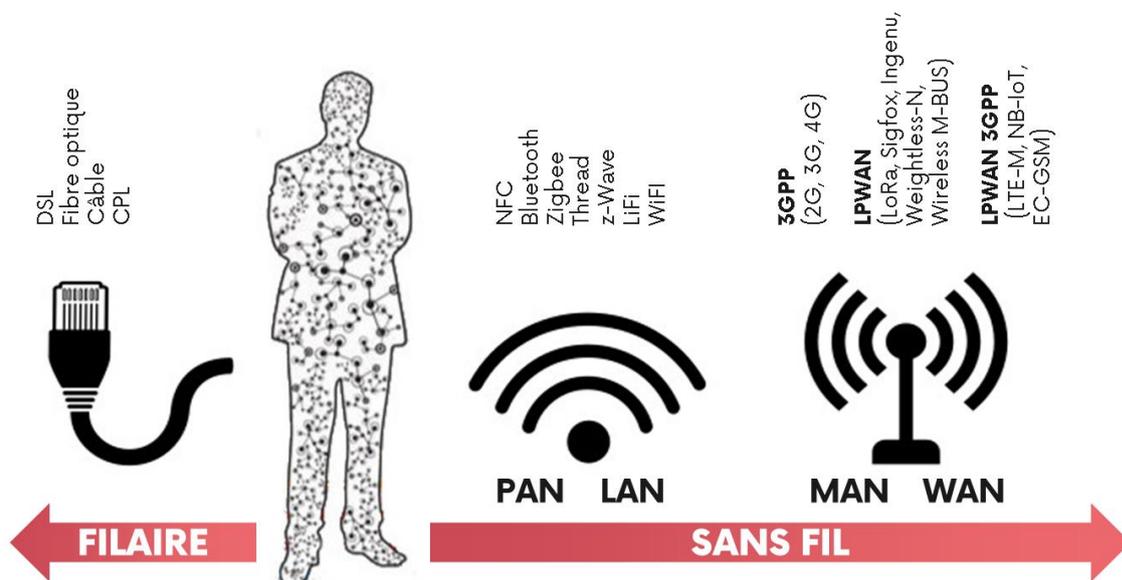
2 Les infrastructures de connectivité

Le développement de l'internet des objets s'appuie sur l'accès à des réseaux d'objets de natures hétérogènes. Toute la variété des technologies de communication est mise à contribution pour répondre aux multiples usages attachés à ces objets. On peut relever en particulier le besoin accru en mobilité et en couverture pour des objets peu consommateurs en énergie, qui a favorisé le développement de nouvelles technologies de connectivité, qui permettent à leur tour de nouveaux usages.

2.1 Un foisonnement de technologies

Si certains objets fixes peuvent être connectés par des réseaux filaires, la croissance de l'internet des objets devrait majoritairement être portée par l'utilisation de technologies sans fil et mobiles. Les technologies de connectivité sans fil sont nombreuses et variées, et l'usage de l'une ou l'autre est souvent avant tout décidé par la portée du réseau envisagé. Certains cas d'usage nécessitent également l'association de technologies sans fil et filaires pour relier les équipements à des réseaux privés étendus ou à Internet.

Un point saillant des développements technologiques actuels autour de l'internet des objets a trait au bouleversement de la dichotomie classique entre, d'une part, des technologies à courte portée opérant en bande « libre », souvent foisonnantes et déployées par l'utilisateur lui-même et, d'autre part, des technologies à grande portée opérant en bande de fréquence soumise à autorisation préalable (« sous licence »), déployées par un nombre réduit d'opérateurs. Le développement de réseaux à bas débit et longue portée, en bandes libres, entraîne ainsi un foisonnement d'initiatives et de développements.



Un foisonnement de technologies pour répondre à une multitude de besoins de connectivité

2.1.1 Des réseaux non opérés à portée locale ou ultra locale

Pour les usages sans fil à courte distance, de type PAN (*Personal Area Network*) ou LAN (*Local Area Network*), les technologies Wi-Fi, Bluetooth, notamment sa déclinaison Low Energy, Zigbee¹⁰, Thread¹¹, z-Wave¹² et NFC, fonctionnant en bandes « libres »¹³, se démarquent particulièrement. D'autres technologies pourraient également apparaître, comme le Li-fi, utilisant des fréquences très hautes, dans la gamme de la lumière visible.

La plupart de ces réseaux locaux, notamment chez les particuliers, sont non opérés. C'est généralement l'utilisateur qui fait l'acquisition des équipements réseau (routeurs reliés à une *box* internet par exemple) et devient responsable de la configuration et du bon fonctionnement du réseau local. Ces réseaux permettent une mobilité très limitée, quoique parfaitement adaptée à un usage domestique ou individuel.

En revanche, les technologies susmentionnées, principalement orientées LAN et PAN, n'offrent pas de connectivité étendue à l'échelle nationale ou internationale, par opposition aux réseaux MAN (*Metropolitan Area Network*) ou WAN (*Wide Area Network*). Ces différentes catégories de réseau, en recouvrement géographique partiel mais répondant à des besoins différents, offrent des possibilités d'articulation et de complémentarité.

2.1.2 Des réseaux opérés au déploiement étendu

Parmi les technologies sans fil déployées sur de grandes distances, de type MAN) ou WAN, on peut retenir principalement :

- Les réseaux cellulaires classiques (3GPP¹⁴) : 2G, 3G, 4G, dont la plupart sont déployés sur des fréquences sous autorisation exclusive ;
- Les réseaux de type LPWAN (*Low Power Wide Area Network*) : LoRa¹⁵, Sigfox¹⁶, Qowisio¹⁷, Ingenu¹⁸, Weightless-N¹⁹, Wireless M-BUS²⁰ ;
- Les solutions de type LPWAN *via* réseaux cellulaires (3GPP) en cours de normalisation : LTE-M²¹, NB-IoT²², EC-GSM²³.

Pour assurer la mise en œuvre et l'exploitation de ces réseaux à grande échelle, le recours à un opérateur²⁴ est le plus souvent nécessaire. On parle alors de réseaux opérés²⁵, dont font notamment

¹⁰ <http://www.zigbee.org/>

¹¹ <https://www.threadgroup.org/>

¹² <http://z-wavealliance.org/>

¹³ La définition de « bande libre » est explicitée en partie 3.1

¹⁴ <http://www.3gpp.org/>

¹⁵ <https://www.lora-alliance.org/>

¹⁶ <http://www.sigfox.com/fr>

¹⁷ <https://www.qowisio.com/>

¹⁸ <http://www.ingenu.com/>

¹⁹ <http://www.weightless.org/about/weightlessn>

²⁰ <http://www.m-bus.com/info/mbuse.php>

²¹ <http://www.gsma.com/connectedliving/long-term-evolution-machine-type-communication-lte-mtc-cat-m1/>

²² <http://www.gsma.com/connectedliving/narrow-band-internet-of-things-nb-iot/>

²³ <http://www.gsma.com/connectedliving/extended-coverage-gsm-internet-of-things-ec-gsm-iot/>

partie les réseaux mobiles cellulaires historiques, presque exclusivement déployés avec des technologies 3GPP (2G, 3G et 4G).

À cet égard, certains besoins nouveaux de l'internet des objets, plutôt antagonistes à la course aux performances qui a longtemps animé le développement des réseaux mobiles, ont entraîné l'émergence de nouvelles technologies de connectivité mobile. Celles-ci permettent d'atteindre des coûts de terminaux très bas et de très faibles consommations énergétiques et sont souvent regroupées sous le terme LPWAN (Low Power Wide Area Network). Plusieurs technologies se distinguent au niveau mondial dans ce domaine et on peut citer Sigfox, LoRaWAN, Qowisio, Ingenu, Weightless-N ou encore Wireless M-BUS. Ce sont essentiellement les deux premières qui connaissent un développement significatif en France, tout en ayant par ailleurs des origines françaises :

- Sigfox propose un modèle verticalement intégré. L'opérateur assure une couverture internationale en s'appuyant sur des déploiements propres ou sur des partenariats avec des opérateurs locaux (nationaux). La technologie pour le développement de modules de connectivité est librement accessible mais la certification des terminaux et le passage exclusif par le *cloud* de Sigfox sont imposés²⁶ ;
- LoRaWAN est un protocole de communication développé coopérativement par de nombreux acteurs au sein de la LoRa Alliance, dont font notamment partie en France Bouygues Telecom, Orange, Actility, Qowisio. Ce modèle, ouvert à la coexistence de plusieurs opérateurs membres de l'alliance sur une même zone géographique, amène naturellement au développement d'un standard interopérable, permettant aux terminaux LoRa de fonctionner sur les divers réseaux – privés comme ouverts au public – déployés internationalement. Néanmoins, si le protocole reste ouvert, le nombre de fournisseurs de composants de décodage reste très limité.

En ce qui concerne les technologies cellulaires, les opérateurs et équipementiers de téléphonie mobile, rassemblés au sein du projet partenarial de développement de standards 3GPP, collaborent à l'adaptation des normes de réseaux et équipements déjà déployés, notamment 4G LTE, en vue de satisfaire les besoins à faible débit et très faible consommation énergétique. Ces travaux devraient faire émerger prochainement plusieurs solutions : le Narrow Band IoT (ou NB-IoT), l'EC-GSM et le LTE-M. Celles-ci posséderont l'avantage pour les opérateurs de téléphonie mobile de s'appuyer sur les équipements déjà déployés et ne nécessiteraient, le plus souvent, que des mises à jours logicielles.

Les acteurs du 3GPP travaillent par ailleurs à la standardisation de la 5G qui cherche à prendre en compte, dès sa création, tous les besoins de l'internet des objets (densité, consommation énergétique, asynchronisme, coût des terminaux...).

²⁴ Aux termes du 15° de l'article L. 32 du CPCE, « on entend par opérateur toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques ».

²⁵ On entend dans ce document « réseau opéré » comme un synonyme de « réseau de communications électroniques ouvert au public ».

²⁶ <http://makers.sigfox.com/>

2.1.3 Réseau mobile professionnel

Enfin, les entreprises ont également la possibilité de déployer un réseau indépendant réservé à leurs propres usages de l'internet des objets. C'est ce qu'ont décidé de faire un certain nombre d'entreprises de services urbains telles que Veolia, Suez Environnement ou GrDF, qui exploitent leurs propres réseaux afin d'en maîtriser davantage la qualité et la sécurité, ou parce qu'elles utilisent leur propre technologie (qui peut être fondée sur un standard existant).

2.1.4 Des réseaux filaires

De nombreux objets fixes sont connectés aux réseaux filaires des opérateurs traditionnels. Le réseau de cuivre, la fibre optique et le câble coaxial sont couramment utilisés, en particulier pour tous les usages nécessitant de forts besoins en débit (caméras de vidéosurveillance, supports publicitaires vidéo, etc.) ou des latences faibles et maîtrisées (machines-outils, téléchirurgie, etc.).

Au titre des usages innovants qui pourraient apparaître, notamment avec l'essor des multiples projets de ville intelligente ou de mobilier urbain, l'Arcep a ouvert dans sa consultation publique en cours²⁷ la question de la réutilisation des déploiements en fibre optique en dehors des immeubles bâtis au bénéfice de l'IoT.

Les technologies de courant porteur en ligne (CPL) peuvent également être utilisées à travers les réseaux des fournisseurs d'énergie, mais sont plutôt réservées aux courtes distances ou pour des usages moins exigeants en termes de débit (commande de lampadaires, relève de compteurs, etc.).

2.2 La connectivité des objets élargit la gamme des besoins par rapport aux réseaux

Les besoins des réseaux en termes de couverture et de qualité sont renouvelés par le déploiement massif d'objets connectés. En effet, l'économie de l'internet des objets, pour ce qui concerne les besoins nécessitant des réseaux à large couverture, ne se développera qu'à la condition que les réseaux soient disponibles sur une large partie des territoires, *a minima* à l'échelle européenne.

Par ailleurs, les opérateurs sont tenus d'assurer la résilience - c'est à dire la capacité d'un système à surmonter une crise déclenchée par un incident critique - de leur propre réseau pour répondre aux besoins de leurs utilisateurs, qui peuvent souhaiter assurer la résilience de leur système de connectivité à travers une redondance inter-technologies (*multi-sourcing*) ou une haute disponibilité intra-technologie (*multi-roaming*).

2.2.1 Un besoin accru de mobilité et de couverture

Les acteurs ont saisi l'enjeu d'une couverture étendue, continentale, nécessaire à la création d'un marché suffisamment vaste, afin de générer des économies d'échelle et permettre la baisse des prix des terminaux et de la connectivité. Par ailleurs, cette couverture transnationale sera un impératif pour certains usages, tels que le véhicule connecté ou le suivi de marchandises.

²⁷

[http://www.arcep.fr/index.php?id=8571&no_cache=1&tx_gsactualite_pi1\[uid\]=1874&tx_gsactualite_pi1\[annee\]=&tx_gsactualite_pi1\[theme\]=&tx_gsactualite_pi1\[motscl\]=&tx_gsactualite_pi1\[backID\]=26&cHash=2a6abd1f8efe62c7f9cfd0d64291632d](http://www.arcep.fr/index.php?id=8571&no_cache=1&tx_gsactualite_pi1[uid]=1874&tx_gsactualite_pi1[annee]=&tx_gsactualite_pi1[theme]=&tx_gsactualite_pi1[motscl]=&tx_gsactualite_pi1[backID]=26&cHash=2a6abd1f8efe62c7f9cfd0d64291632d)

Les réseaux cellulaires traditionnels ont depuis longtemps mis en place des accords pour permettre l'itinérance des cartes SIM dans le monde entier. À l'échelle européenne, ces accords sont encadrés par des obligations découlant du droit de l'Union européenne, qui incluent des dispositions à la fois techniques et économiques. L'Union européenne a marqué son attachement à la création d'un marché européen des communications électroniques par la publication le 25 novembre 2015 d'un nouveau règlement portant notamment sur le *roaming*²⁸. Ce règlement fixe les conditions de l'accès de gros aux réseaux publics de communications mobiles aux fins de la fourniture de services d'itinérance. Il a pour objectif de supprimer l'écart entre les prix nationaux et les prix d'itinérance au sein de l'Union par un encadrement des tarifs de prestation d'itinérance sur les marchés de gros et de détail.

L'Organe des régulateurs européens des communications électroniques (ORECE), dont l'Arcep exercera la présidence en 2017²⁹, a publié le 12 février 2016 un rapport intitulé *Enabling the internet of things*³⁰, dans lequel il conclut, en interprétant le règlement sur l'itinérance, que les cas d'usage de l'internet des objets sur les réseaux mobiles de communications électroniques entrent généralement dans le périmètre de ce règlement et sont également soumis à ce titre à l'obligation d'accès et à l'encadrement tarifaire. S'agissant, en revanche, de l'itinérance permanente, l'ORECE considère qu'il s'agit d'une approche au cas par cas. Elle conclut que le règlement ne devrait pas s'appliquer dans le cas d'un séjour prolongé d'un appareil connecté sur le réseau d'un opérateur étranger, sans voyager³¹. L'ORECE identifie à ce titre un enjeu à poursuivre dans de futurs travaux afin de délimiter plus nettement les cas d'itinérance permanente et transitoire.

2.2.2 Certaines applications nécessitent une haute disponibilité

L'Arcep a constaté une demande, principalement d'acteurs économiques privés ou publics, pour des services mobiles à haute disponibilité, prévoyant une bascule d'un réseau mobile à un autre en cas de besoin (*multi-roaming*), qui est imparfaitement satisfaite par les opérateurs français à ce jour.

Les solutions actuellement mises en œuvre pour répondre à cette demande passent souvent par des mécanismes de contournement, s'appuyant sur des accords d'itinérance internationaux : elles transitent *via* les réseaux d'opérateurs étrangers ayant accès à des accords d'itinérance avec plusieurs opérateurs français.

Une offre nationale intégrant une bascule de sécurisation entre réseaux mobiles requiert la mise en œuvre d'un partage de réseaux mobiles national entre opérateurs français. Ce type de solution est déjà en œuvre pour les appels d'urgence. Les utilisateurs naturels d'une telle offre pourraient être, au-delà d'acteurs économiques privés, certains services publics critiques ou des applications de communication entre machines qui nécessiteraient une sécurisation particulière.

²⁸ Règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) no 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union.

²⁹ et la vice-présidence en 2016 et 2018

³⁰ http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things

³¹ Traduction libre du rapport de l'ORECE *Enabling the Internet of Things* (2016) : "IoT connected devices used on permanent roaming and not travelling at all"

Si l'Arcep a souligné³² que la généralisation de telles offres à tout le marché devrait *a priori* être exclue, elle a indiqué que la fourniture de services mobiles à haute disponibilité pouvait être pertinente pour répondre à des besoins particuliers. Elle a ainsi invité les opérateurs intéressés à se rapprocher d'elle.

2.2.3 Les nouveaux réseaux LPWAN permettent par ailleurs d'envisager des possibilités complémentaires de redondance

Ni les utilisateurs ni les fabricants d'objets connectés ne sont tenus de respecter des obligations de résilience³³ : ils sont considérés comme de simples acheteurs d'une connectivité auprès d'un opérateur de communications électroniques sur les réseaux opérés. Toutefois, certains objets, sites ou applications critiques emploient des mécanismes de redondance (*multi-sourcing*) depuis de nombreuses années, en particulier sur le marché entreprises. Les solutions de double connectivité, avec ou sans bascule automatique d'un réseau vers l'autre en cas de coupure, avec des garanties de sécurité plus ou moins importantes (double raccordement physique ou logique), ont permis de répondre aux besoins de redondance en combinant des réseaux d'opérateurs différents et/ou des technologies différentes (fibre, cuivre, câble, cellulaire, satellite, Wi-Fi, autre). La naissance des nouvelles technologies réseaux LPWAN (comme LoRa ou SigFox) vient ajouter des possibilités complémentaires de redondance de l'accès.

En effet, les services de connectivité LPWAN sont produits à faible coût, autonomes en énergie et offrent de bonnes performances de couverture *indoor*. En particulier, leur très faible consommation énergétique, autorisant une alimentation sur batterie, permet de surmonter les cas de coupure électrique. Ces performances font de la connexion de secours l'un des marchés privilégiés des services de connectivité LPWAN : un objet peut être connecté grâce à un réseau fixe ou mobile « haut débit » en tant que connexion principale et basculer sur une connexion LPWAN de secours afin de prendre le relais en cas de défaillance. À titre d'exemple, Securitas Direct a ainsi choisi de relier 1,2 millions d'alarmes au réseau de Sigfox en Espagne et en France. Toutefois, les faibles débits associés au LPWAN les cantonnent, en ce qui concerne les liaisons de secours, à certains types de solution ou à un usage nécessitant de véhiculer uniquement certains flux critiques et peu consommateurs de données.

³² [Arcep, Lignes directrices sur le partage de réseaux mobiles](#), mai 2016 (section 3.3.2.a)

³³ Il faut cependant noter que, conformément à l'article L. 34-9 du CPCE, les équipements terminaux destinés à être connectés à un réseau ouvert au public doivent faire l'objet d'une évaluation de leur conformité aux exigences essentielles. Ces dernières peuvent notamment porter sur la protection des réseaux.

Les principaux enjeux

Les auditions ont démontré l'existence d'un foisonnement de technologies – filaires et sans fil – qui s'avère nécessaire, et qu'il faudra favoriser, pour répondre à la multitude des besoins d'usages et de connectivité de l'internet des objets. Les réseaux sans fil à courte distance sont généralement gérés par l'utilisateur alors que ceux à plus longue portée (dont 3GPP et LPWAN font partie) requièrent généralement le concours d'un opérateur.

Un autre enjeu, cette fois-ci au niveau européen, sera celui des conditions d'itinérance permanente pour les objets puisqu'une partie des objets connectés ont vocation à être utilisés en dehors de leur pays de production.

Enfin, l'enjeu de résilience est au cœur des technologies de l'internet des objets. En effet, les opérateurs sont tenus d'assurer la résilience de leur propre réseau tandis que l'utilisateur peut souhaiter assurer la résilience de son système de connectivité à travers une redondance inter-technologies (*multi-sourcing*) ou une haute disponibilité intra-technologie (*multi-roaming*). Le besoin en haute disponibilité est imparfaitement satisfait à ce jour et la question de l'itinérance nationale (sous conditions restreintes) pourrait être envisagée pour y répondre. Les performances des nouvelles technologies de réseaux LPWAN (forte couverture, faible consommation énergétique, coût de connectivité faible) en ont fait des candidats idéals pour ajouter des possibilités complémentaires de redondance de l'accès.

3 Les ressources rares nécessaires au développement de l'internet des objets

La fourniture de solutions de connectivité identifiées précédemment mobilise souvent deux types de ressources : des fréquences et des adresses. Ces ressources, considérées comme rares, le sont d'autant plus que la croissance envisagée pour le nombre d'objets connectés est extrêmement importante.

3.1 Des régimes d'autorisation d'utilisation de fréquences différents pour répondre à des contraintes diverses

Les bandes de fréquences utilisables pour l'internet des objets incluent :

- Des fréquences dont l'utilisation se base sur un régime d'autorisation générale sous réserve du respect des conditions techniques. Il s'agit des fréquences dites « libres », utilisées par exemple pour des réseaux LPWAN par Sigfox, Qowiso et les acteurs de l'Alliance LoRa ;
- Des fréquences dont l'utilisation est soumise à autorisation individuelle, dont :
 - Des fréquences utilisées pour la mise en œuvre de réseaux mobiles ouverts au public (2G, voire 3G ou 4G puis 5G) ;
 - Des fréquences pour la mise en œuvre de réseaux mobiles professionnels (réseaux dits PMR ou *professional mobile radio*) ;
 - Des fréquences du service fixe (boucle locale radio, faisceaux hertziens) ;
 - Des fréquences des services par satellite.

Pour les fréquences « libres », aucune autorisation individuelle préalable n'est nécessaire et leur utilisation n'est pas soumise au paiement de redevances. En revanche, l'utilisateur ne bénéficie d'aucune garantie de protection contre les brouillages et doit respecter certaines contraintes techniques. Un certain nombre de ces bandes de fréquences, dont les conditions techniques d'utilisation sont fixées par l'Arcep, sont utilisées par les dispositifs de faible puissance, comme les appareils utilisant le Wi-Fi, mais également par l'internet des objets, notamment les bandes : 13,56 MHz, 169 MHz, 433 MHz, 863 – 870 MHz, 2400 – 2483,5 MHz, 5150 – 5350 MHz et 5470 – 5725 MHz³⁴.

Les fréquences dont l'utilisation est soumise à autorisation individuelle font l'objet d'une coordination, dans l'objectif de fournir à l'utilisateur une protection contre les brouillages. L'usage de ces fréquences est, sauf cas exceptionnel, soumis au paiement de redevances. Les technologies d'accès GSM, UMTS et LTE, utilisées par les réseaux mobiles ouverts au public, permettent déjà des applications pour l'internet des objets qui seront encore facilitées par l'émergence de nouvelles normes 3GPP mentionnées précédemment. Les bandes attribuées aux opérateurs mobiles en France métropolitaine³⁵ sont : 700 MHz, 800 MHz, 900 MHz, 1800 MHz, 2100 MHz et 2600 MHz.

³⁴ Le cadre réglementaire fixant les conditions d'utilisation des fréquences radioélectriques par des dispositifs à courte portée est fixé par la décision n° 2014-1263 de l'Arcep en date du 6 novembre 2014 d'utilisation des fréquences: http://www.arcep.fr/uploads/tx_gsavis/14-1263.pdf

³⁵ Le tableau de répartition des fréquences attribuées aux 4 opérateurs mobiles en métropole est disponible sur le site web de l'Arcep en suivant ce lien : http://www.arcep.fr/fileadmin/reprise/dossiers/mobile/Repartition_des_frequences_-_decembre_2015.pdf

Le choix de l'utilisation d'une bande de fréquences plutôt qu'une autre dépend, en plus du régime d'autorisation de la bande et donc de la simplicité d'accès à la ressource, des exigences opérationnelles :

- Communication ininterrompue ou utilisation intermittente ;
- Communications en temps réel (par exemple, pour des applications de contrôle/commande) ou communications retardées (par exemple, pour de la collecte d'informations) ;
- Utilisation de bande passante (hauts ou faibles débits de données) ;
- Couverture (usages de proximité ou avec couverture étendue, à l'intérieur ou à l'extérieur des bâtiments) ;
- Consommation énergétique.

Ainsi, en fonction de leur modèle d'affaire ou des usages anticipés, les acteurs auront tendance à se tourner soit vers des bandes libres, soit vers des bandes attribuées à titre exclusif (notamment en s'appuyant sur les réseaux des opérateurs mobiles grand public).

De plus, les auditions ont mis en avant que l'usage de fréquences « libres » présente pour certains acteurs un moyen de tester des modèles économiques à moindre coût, en comparaison de l'usage de bandes soumises à autorisations individuelles. En effet, l'usage des bandes libres permet l'innovation sans permission, sous réserve de respecter des conditions techniques plus ou moins contraignantes et sans protection contre les brouillages. Les auditions ont également été l'occasion pour les acteurs en manque d'information d'interroger l'Arcep sur le cadre juridique relatif à l'expérimentation dans les bandes soumises à autorisations individuelles.

À cet égard, l'Arcep souligne qu'elle délivre déjà, sur le fondement de l'article L. 42-1 du code des postes et des communications électroniques (CPCE), des autorisations individuelles d'utilisation de fréquences afin de mener des expérimentations. En outre, des dispositions visant à renforcer le cadre réglementaire sur l'expérimentation est prévu dans le projet de loi pour une République numérique. L'Arcep pourrait, sous certaines conditions, définir un cadre expérimental visant à accompagner un opérateur donné dans le développement d'une technologie ou d'un service innovants, du point de vue technique ou commercial. A cette fin, l'Arcep, lorsqu'elle attribue à titre individuel des ressources en fréquences et de numérotation « *à des fins expérimentales* », pourrait lever pour une durée maximale de deux ans, pour l'exercice de l'activité nécessitant les ressources, certaines des obligations attachées à l'attribution de ces ressources ou afférentes à l'exercice d'une activité d'opérateur ou d'exploitant de réseau indépendant.

3.2 Une disponibilité des fréquences à anticiper pour le moyen terme

À court terme, les fréquences disponibles ne semblent pas être un frein au déploiement de l'internet des objets et de multiples options sont déjà disponibles comme l'a démontré le récent atelier de la CEPT³⁶.

Les perspectives de croissance, qui annoncent un internet des objets reliant, d'ici 2020, plus de 50 milliards d'objets³⁷, imposent néanmoins une démarche d'anticipation. La CEPT a ainsi engagé plusieurs actions concrètes, pour développer les gammes de fréquences mobilisables. L'Arcep contribue à la préparation de la position française sous l'égide de l'ANFR qui intervient dans cette

³⁶ <http://www.cept.org/ecc/cept-workshop-on-machine-to-machine-communications-m2m/>

³⁷ Source : Cisco

enceinte. D'une part, elle cherche à identifier des orientations d'harmonisation à court terme dans la bande 800 – 900 MHz pour des utilisations sous autorisations générales. D'autre part, elle évalue la compatibilité des conditions techniques d'usage des bandes des opérateurs mobiles avec l'Internet des objets.

3.2.1 Dans les bandes soumises à une autorisation générale, dites bandes « libres »

Dans un premier temps, en ce qui concerne l'utilisation des bandes de fréquences « libres », l'Arcep a mené fin 2014 une consultation publique³⁸ visant notamment à approfondir sa vision prospective sur les usages et les besoins à venir dans ces bandes, en particulier dans le contexte du développement de l'internet des objets. Les enseignements de cette consultation publique rejoignent ceux des auditions et confirment, dans certains contextes, certaines limites de l'utilisation des fréquences libres. Une croissance importante des applications et des usages sur une certaine bande de fréquences peut contraindre le fonctionnement d'une application ou le service rendu à l'utilisateur final. En conséquence, il importe de répondre aux demandes d'accès aux fréquences soulevées par les nouvelles applications et formulées par l'industrie afin de permettre le cas échéant d'adresser des usages plus complexes ou plus consommateurs de données, et d'accompagner l'augmentation prévisible de la densité d'objets connectés. Le processus de coopération entre l'ETSI et la CEPT présente un atout pour l'Europe dans ce contexte.

Par ailleurs, il ressort des auditions que la qualité d'utilisation de ces bandes peut être perturbée par des brouillages, notamment dus au non-respect des normes harmonisées ou des conditions d'utilisation des fréquences en vigueur par certains équipements. En outre, les règles d'utilisation conçues pour des usages définis pourraient nécessiter des adaptations aux nouveaux besoins de l'internet des objets. En effet, les conditions techniques d'utilisation des bandes de fréquences libres peuvent être relativement restrictives afin de permettre l'utilisation non coordonnée de très nombreux systèmes. Elles peuvent parfois être limitées à une application spécifique afin de réduire les risques de brouillage. En revanche, l'augmentation exponentielle de la densité d'objet prévue par toutes les études pourrait *in fine* justifier l'identification de nouvelles ressources harmonisées en tenant compte de nouveaux scénarios de déploiements et conditions d'utilisation, par exemple de l'augmentation des niveaux de puissance et des taux d'utilisation, pour accompagner la croissance du secteur. Les acteurs ont ainsi profité des auditions pour confirmer le besoin d'assouplissement des conditions de la bande 863 - 870 MHz et d'ouverture d'une partie des bandes 870 - 876 MHz et 915 - 921 MHz. Ces évolutions potentielles avaient été formulées dans le rapport ministériel *Une gestion dynamique du spectre pour l'innovation et la croissance* de mars 2014. A la suite de la remise de ce rapport, la secrétaire d'Etat chargée du Numérique a confié à l'ANFR la responsabilité d'étudier « *afin de contribuer au développement des objets connectés, les conditions techniques et réglementaires qui permettraient le développement des appareils de faible puissance dans les bandes 870 876 MHz, 915 921 MHz et 862 870 MHz* ». Cette mission a été reprise dans le Contrat d'objectifs et de performance pour la période 2015 2017 de l'ANFR³⁹. Les travaux ont commencé en 2015 et une consultation publique est ouverte du 3 juin au 18 juillet 2016.

L'harmonisation des fréquences au niveau mondial est une condition importante, notamment pour les acteurs qui visent un déploiement international. En effet, la croissance des industriels français et européens sur la scène internationale dépend en partie de leur capacité à réaliser des économies

³⁸ La synthèse de la consultation publique est disponible ici : http://arcep.fr/fileadmin/uploads/tx_gspublication/Synthese_-_Consultation_bandes_libres.pdf

³⁹ http://www.anfr.fr/fileadmin/mediatheque/documents/Publications/COP_ANFR_VF_2015-11-23.pdf

d'échelles afin d'offrir des solutions technologiques à bas coût en s'appuyant sur des systèmes utilisant les mêmes fréquences.

À ce sujet, les bandes de fréquences 863 – 870 MHz, 870 – 876 MHz et 915 – 921 MHz ont été identifiées au niveau européen pour plusieurs applications de faible puissance (RFID, *smart metering*, *smart grid*, *smart cities*, *home automation*, alarmes, aide à l'audition). Des travaux sont actuellement menés par les pouvoirs publics français pour assouplir les conditions de la bande 862 – 870 MHz et pour ouvrir les bandes 870 – 876 MHz et 915 – 921 MHz pour l'internet des objets. Ils s'inscrivent dans une logique d'harmonisation européenne et autant que possible internationale. L'Arcep et l'Agence nationale des fréquences (ANFR) ont lancé le 3 juin 2016 une consultation publique⁴⁰ visant à recueillir les observations des parties prenantes sur les nouvelles opportunités pour l'utilisation des bandes 862 - 870 MHz, 870 - 876 MHz et 915 - 921 MHz. Elle vise à l'ouverture de nouvelles bandes de fréquences et à étudier les conditions techniques et réglementaires qui permettraient le développement de dispositifs de faible puissance dans ces bandes, afin d'orienter les travaux nationaux et européens en cours pour faciliter le développement de l'internet des objets.

3.2.2 Dans les bandes soumises à autorisation individuelle

Les auditions n'ont pas fait ressortir de demande spécifique en vue de l'attribution de bandes soumises à autorisation individuelle, ce qui peut s'expliquer par le fait que les acteurs sont avant tout en attente de l'arrivée des standards EC-GSM, LTE-M et NB-IoT, qui devraient fonctionner dans les bandes aujourd'hui attribuées, et à terme de la 5G qui fait d'ores et déjà l'objet de travaux visant la mise à disposition de nouvelles bandes de fréquences ou l'adaptation des conditions techniques dans les bandes actuellement harmonisées pour les réseaux mobiles.

En complément, des réflexions sont en cours aux niveaux européen et national pour examiner et adapter si nécessaire le cadre technique et réglementaire, en vue *in fine* de permettre aux opérateurs d'utiliser l'ensemble des bandes affectées aux réseaux cellulaires pour du M2M. En effet, les dispositions harmonisées pour l'utilisation des bandes 700 MHz, 800 MHz, 2,1 GHz, 2,6 GHz et 3,5 GHz reposent sur le principe de « masques de puissance », sans faire référence à certaines technologies particulières. En revanche, dans les bandes 900 MHz et 1800 MHz, les dispositions d'harmonisation sont liées aux conditions spécifiques de coexistence entre systèmes GSM, UMTS, LTE et WiMAX. La CEPT a engagé des travaux visant à évaluer la compatibilité de ces cadres réglementaires avec les solutions envisagées pour l'Internet des objets dans ces bandes. Elle prévoit de publier des résultats en mars 2017.

3.3 Multiplicité des modes d'adressage

Plusieurs systèmes d'adressage sont utilisés pour identifier les objets connectés dans les réseaux :

- Identifiants ouverts : numéros de téléphone mobiles, identifiants de cartes SIM, adresses IP (dans leurs variantes IPv4 ou IPv6), adresses MAC, identifiants OID (Object IDentifiers) de l'UIT;
- Identifiants propriétaires : formats non standardisés.

Le principal enjeu est d'éviter la pénurie d'identifiants ouverts face à un volume d'objets connectés toujours croissant. Il peut être également nécessaire de définir une meilleure articulation entre

⁴⁰ La consultation publique est ouverte jusqu'au 18 juillet 2016 et est disponible ici : http://www.arcep.fr/uploads/tx_gspublication/consult-arcep-anfr-iot-frequences-030616.pdf

l'échelle mondiale du marché des objets connectés et la gestion nationale de certaines ressources de numérotation. Par ailleurs, les problématiques liées aux modes d'adressage rejoignent celles liées à la fluidité et à l'interopérabilité, étudiées au chapitre suivant.

3.3.1 Réseaux cellulaires

S'agissant des réseaux mobiles : les normes 3GPP (GSM / UMTS / LTE) prévoient qu'à chaque ligne mobile soit affecté un numéro de téléphone mobile MS-ISDN compatible avec le standard E. 164 de l'UIT⁴¹. Ces numéros MS-ISDN sont également utilisés pour identifier les objets connectés dans le système d'information de l'opérateur de réseau mobile. Cependant, l'objet communique généralement avec l'application métier par le biais de protocoles de communications informatiques tels que l'IP, situé sur une couche réseau supérieure⁴².

Toutefois, les protocoles de communication voix et SMS, utilisant le numéro MS-ISDN comme identifiant d'adressage, sont utilisés dans le cadre de certaines applications spécifiques, ou pour « réveiller » les machines (qui opèrent la plupart du temps en mode veille pour optimiser leur autonomie) afin d'initier un échange de données. Cela est notamment le cas pour les actions de télé-relève commandées par un système central.

Ces numéros MS-ISDN sont attribués par l'Arcep aux opérateurs, qui les affectent ensuite aux abonnés. En 2012, afin d'éviter une pénurie des numéros mobiles, l'Arcep a décidé de la création d'une tranche spéciale de numéros mobiles étendus à 14 chiffres en métropole, commençant par « 0700 », pour permettre aux lignes mobiles dédiées aux communications de machine à machine (M2M)⁴³ de ne plus peser sur le stock de numéros mobiles à 10 chiffres. Ces communications sont ainsi exclues de l'utilisation des numéros mobiles à 10 chiffres depuis le 1^{er} janvier 2016 (des dérogations pour une utilisation jusqu'au 30 juin 2017 ayant pu être sollicitées auprès de l'Arcep)⁴⁴. Il convient également de noter qu'en application du plan national de numérotation⁴⁵, ces numéros doivent être affectés à des utilisateurs domiciliés sur le territoire français, et n'ont donc pas vocation à être utilisés de manière permanente en dehors du territoire national. Toutefois, certains opérateurs internationaux rencontrés lors des auditions ont émis le souhait que ces conditions soient assouplies afin de permettre un accès simplifié au marché mondial avec les ressources de leur pays d'origine.

En outre, chaque carte SIM est également identifiée par un code « IMSI » dont le format est défini par la recommandation E. 212 de l'UIT⁴⁶. L'IMSI est composé de trois parties :

- MCC : représente le pays de destination : il est attribué aux pays par l'UIT (208 pour la France métropolitaine) ;

⁴¹ Plan de numérotation des télécommunications publiques internationales défini par l'UIT. L'UIT est l'institution spécialisée des Nations Unies pour les technologies de l'information et de la communication - <https://www.itu.int/rec/T-REC-E.164-201011-l/fr>

⁴² Au sens du modèle OSI.

⁴³ Décision n° 2012-0855 de l'Arcep en date du 17 juillet 2012

⁴⁴ Décision n° 05-1085 de l'Arcep en date du 15 novembre 2005, telle que modifiée par la décision n° 2015-1295 du 22 octobre 2015

⁴⁵ Décisions n° 05-1084 et 05-1085 de l'Arcep en date du 15 décembre 2005.

⁴⁶ Plan d'identification international pour les réseaux publics et les abonnements défini par l'UIT - <https://www.itu.int/rec/T-REC-E.212/fr>

- MNC : représente le réseau mobile de destination : il est attribué aux opérateurs par l'Arcep⁴⁷. 100 MNC sont disponibles par MCC ;
- MSIN : représente l'abonné : affecté au client par l'opérateur (numéro interne au réseau, non public, différent du numéro de téléphone de l'abonné).

Compte tenu de leur fonction d'identification du réseau mobile et de leur rareté, les codes MNC sont uniquement attribués aux opérateurs qui, au regard de leurs infrastructures et de leurs contrats, sont en mesure de les exploiter. En pratique, il s'agit à ce jour des opérateurs de réseaux mobiles (MNO) et des opérateurs de réseaux mobiles virtuels (MVNO).

3.3.2 Réseaux LPWAN

S'agissant des réseaux LPWAN, il n'existe à ce jour aucun plan de numérotation standardisé et unifié. Ces réseaux utilisent des identifiants privés, aux formats propriétaires, pour identifier les capteurs.

3.3.3 Adressage IP

Enfin, pour être directement accessible sur le réseau Internet, chaque objet doit se faire attribuer une adresse IP publique. Au niveau mondial, la gestion des adresses IP est assurée par l'*Internet Corporation for Assigned Names and Numbers*. L'ICANN partage les adresses IP en blocs, entre les différents registres régionaux (le RIPE NCC (Réseaux IP Européens - *Network Coordination Centre*) pour l'Europe et le Moyen Orient), lesquels se chargent de les attribuer localement. La version 4 du protocole IP a été définie en 1981. Le 14 septembre 2012, le RIPE NCC a annoncé le début de la distribution des adresses issues du dernier bloc d'adresses IPv4 dont il dispose, alertant ainsi contre un risque de pénurie et appelant à la nécessaire migration vers le nouveau système d'adressage IPv6.

La version 6 du protocole IP, qui a été finalisée en 1998 par l'IETF permettra d'identifier directement l'ensemble des objets connectés à l'Internet à travers le monde sans risque de pénurie, grâce à l'utilisation d'adresses plus longues permettant un espace d'adressage quasi illimité. A ce titre, la secrétaire d'Etat chargée du numérique, Axelle Lemaire, a saisi l'Arcep sur l'état de déploiement du protocole IPv6. En effet, longtemps pionnière dans le déploiement de l'IPv6, la France a depuis quelques années perdu sa position de meneur en la matière.

⁴⁷ La liste de codes MNC attribués par l'Arcep est disponible à l'adresse suivante : <https://extranet.arcep.fr/portail/LinkClick.aspx?fileticket=etHdgos5yN4%3d&tabid=217&portalid=0&mid=850>

Les principaux enjeux

Il ressort des auditions deux enjeux associant les ressources rares au déploiement de l'internet des objets. Le premier est propre aux fréquences, le second aux questions d'identification des objets.

Concernant les fréquences, deux problématiques ont été identifiées :

- La disponibilité des ressources pour l'ensemble des acteurs, y compris les fréquences libres, est impérative pour le déploiement de l'offre. L'enjeu autour de la disponibilité des fréquences est étroitement lié à l'harmonisation européenne et internationale des ressources requise pour un déploiement au niveau mondial des acteurs de l'internet des objets. Des travaux sont d'ores et déjà engagés, notamment par l'Arcep et l'ANFR dans les bandes 862-870, 870-876 et 915-921 MHz ;
- Les conditions d'utilisation de certaines bandes libres pourraient être adaptées aux nouveaux besoins de l'internet des objets, toutefois en imposant des conditions à même de minimiser les brouillages dans ces bandes. Ce sujet relève également des travaux susmentionnés engagés par l'Arcep et l'ANFR.

Concernant l'identification des objets, deux enjeux ont été identifiés :

- La gestion de la rareté de ces ressources constitue un enjeu concernant plusieurs systèmes d'adressage utilisés pour identifier les objets dans les réseaux. Concernant les réseaux cellulaires, une tranche de numéro à 14 chiffres a été mise à disposition spécifiquement pour le M2M. De même, certains opérateurs souhaiteraient aujourd'hui accéder à une itinérance permanente au niveau mondial avec les ressources en numérotation nationales de leur pays d'origine. En revanche, concernant les réseaux LPWAN, il n'y a pas d'enjeu car ils utilisent à ce jour des identifiants privés.
- La transition de l'IPv4 à l'IPv6 est un enjeu dont les pouvoirs publics se sont déjà saisis car il adresse dans un premier temps la question de rareté des identifiants, et favorise ensuite une interopérabilité au niveau des couches basses (cf. partie suivante). Ainsi, dans son rapport rendu en Gouvernement sur le déploiement du protocole IPv6, l'Arcep évalue les risques liés à la pénurie d'adresses IPv4 et d'un déploiement tardif du protocole IPv6, notamment pour l'IoT. De même, l'article 20 bis A du projet de loi pour une République numérique prévoit qu'à compter du 1er janvier 2018, tout nouvel équipement terminal, au sens de l'article L. 32 du CPCE, destiné à la vente ou à la location sur le territoire français doit être compatible avec la norme IPV6.

4 L'ouverture au sein de l'internet des objets

Pour que les objets connectés fassent réseau, et répondent à la promesse que porte l'expression « internet des objets », il sera nécessaire que des formes plus ou moins larges d'interopérabilité existent entre les objets, qui peuvent se mettre en place à différents niveaux.

Les auditions ont permis de distinguer deux grands niveaux d'interopérabilité :

- l'interopérabilité au niveau des couches basses, c'est-à-dire de l'acheminement de l'information ;
- l'interopérabilité au niveau de couches hautes correspondant au dialogue applicatif, pour le traitement des données.

4.1 L'enjeu de l'ouverture et de l'interopérabilité

Les implications du degré d'ouverture des systèmes ont déjà fait l'objet d'analyses économiques dans le cadre de marchés présentant une innovation forte et des économies de réseau importantes. L'Autorité de la concurrence estimait ainsi, dans son rapport intitulé « Analyse économique des systèmes ouverts et fermés »⁴⁸, publié en 2014, que les avantages et les inconvénients d'un système ouvert⁴⁹, par rapport à un système fermé, devaient être appréciés au cas par cas. D'abord, elle a relevé que l'ouverture comme la fermeture d'un système pouvait être favorables à la concurrence : quand la première vise à promouvoir la concurrence au sein d'un système, la seconde encourage la concurrence entre systèmes. Ensuite, elle a souligné que l'ouverture favorisait la compatibilité entre systèmes, ce qui augmente le bien-être des utilisateurs et maximise les effets de réseau ; elle a également noté que la fermeture, au contraire, permettait d'encourager l'innovation en évitant la standardisation. Ces analyses peuvent s'appliquer à l'internet des objets.

Le développement de l'internet des objets s'appuie sur l'accès au réseau d'objets non connectés jusqu'alors. Pour ce faire, toute la variété des technologies de communication⁵⁰ est mise à contribution, au bénéfice d'utilisateurs aux besoins variés. Cette diversité de solutions de connectivité démontre une innovation forte et s'accompagne de l'émergence de nombreux acteurs, mais pourrait être remise en cause avec la maturité du marché. Le développement du marché pose ainsi la question de son juste degré d'ouverture, qui peut se poser à différents niveaux (objets/capteurs, données, connectivité, adresses et protocoles, etc.). En l'espèce, l'ouverture peut se mesurer à l'aune des possibilités d'interopérabilité et des conditions de fluidité en général.

La question de l'interopérabilité est celle de la compatibilité entre les objets et entre les applications. L'interopérabilité se traduit par deux effets économiques. D'une part, l'interopérabilité favorise la fluidité du marché, condition nécessaire au plein exercice de la concurrence, puisqu'elle laisse aux utilisateurs le choix des solutions de l'internet des objets sans contrainte de changement de technologies donc de fournisseurs. D'autre part, elle permet, à niveau de concurrence donné, de maximiser les effets de réseau. En effet, en rendant les objets compatibles, elle permet aux utilisateurs d'enrichir la gamme et le volume d'objets connectables à leurs propres objets. Cela

⁴⁸ Rapport publié conjointement en décembre 2014 par l'Autorité de la concurrence française et la Competition and Markets Authority britannique

⁴⁹ Un système, défini par Hazlett et al (2011) comme « un ensemble de deux composants ou plus, associés à une interface leur permettant de fonctionner ensemble » est qualifié d' « ouvert » lorsque l'interface est accessible à l'ensemble des acteurs, au-delà de son propriétaire.

⁵⁰ Voir la partie « II. Les technologies de connectivité »

permet d'enrichir les offres et de faire émerger de nouveaux usages. Ainsi, l'interopérabilité est *a priori* de nature à améliorer le bien-être des utilisateurs.

Néanmoins, l'interopérabilité, en ce qu'elle peut créer des contraintes et des interdépendances pour les fabricants (qui peuvent néanmoins varier selon le niveau où se joue l'interopérabilité), peut limiter les facultés de différenciation et d'innovation. Alors que le marché est encore émergent, forcer l'interopérabilité risquerait de freiner, voire d'empêcher, l'innovation : cela limiterait les possibilités de monétisation pour les acteurs innovants qui seraient moins en mesure de retenir leurs clients. Dans le contexte spécifique de l'internet des objets, imposer une interopérabilité totale et générale pourrait également avoir un impact physique sur les objets, alors qu'il existe déjà d'importantes contraintes technologiques pour les fabricants, telles que la taille, la mémoire, l'autonomie et la consommation.

À très court terme, l'interopérabilité ne semble pas le premier enjeu pour les fabricants ; les solutions technologique ne sont pas encore matures, les usages restent souvent locaux, géographiquement ou au sein d'une entité unique, et relèvent plutôt de la télémessure, en particulier dans le contexte industriel. Les nombreux fabricants ont ainsi tendance à développer leurs objets indépendamment les uns des autres, conduisant à une multitude d'offres en silo. Pour les utilisateurs, l'interopérabilité n'est pas une priorité à court terme, en particulier pour les industriels et les collectivités territoriales qui testent encore à petite échelle les solutions qui leur sont proposées et ont une certaine capacité à y incorporer par la suite une étape d'intégration, avant d'envisager un déploiement massif.

En revanche, les acteurs de l'internet des objets ont conscience qu'à moyen terme, tout objet connecté sera valorisé en fonction de sa capacité à communiquer avec un écosystème. Par exemple, dans le cas de la maison connectée, il conviendra d'éviter aux particuliers de faire face à une multitude de modalités de connectivité en leur proposant des objets parlant la même langue pour leur éviter des coûts d'apprentissage et des dépenses supplémentaires pour le contrôle de leurs équipements. Dans le cas des véhicules connectés, il sera crucial que les véhicules communiquent entre eux et avec les territoires connectés qu'ils seront amenés à traverser. Le manque d'interopérabilité pourra alors se révéler être un frein au déploiement de l'internet des objets.

4.2 Une course au standard au niveau des couches basses

Au niveau des couches basses, on peut identifier deux sujets d'interopérabilité : sur les protocoles de communication d'une part, et sur l'adressage des objets d'autre part.

L'heure n'est pas encore à l'interopérabilité en termes de protocoles de communication : la recherche de très bas coûts pour les modules de connectivité impose une simplicité qui ne permet que difficilement, pour le moment, de connectivité multi protocoles. Toutefois, certains acteurs s'organisent pour promouvoir des standards à l'échelle mondiale.

Ainsi, les acteurs de la LoRa Alliance visent, en respectant le standard commun LoRa, une forme d'interopérabilité entre les réseaux des opérateurs adhérents. De leur côté, les membres de la Wi-Fi Alliance, déjà active à l'échelle mondiale, proposent le standard HaLow pour répondre aux besoins de l'internet des objets contraints par une faible consommation énergétique. De même, les membres de la ZigBee Alliance développent un standard commun sur le protocole de communication et ont créé un partenariat avec le consortium Thread afin d'assurer une forme d'interopérabilité allant jusqu'aux couches hautes.

Sigfox, quant à lui, contrôle seul le déploiement de son standard propriétaire et gère l'alliance SNO (*Sigfox Network Operators*) qui octroie des accords de déploiement localement exclusifs à ses

opérateurs membres. L'interopérabilité s'entend dans ce cas uniquement comme un moyen d'augmenter la couverture de la technologie de Sigfox.

Les exploitants de réseaux mobiles, pour leur part, s'appuieront sur les standards 3GPP, qui permettent une forte interopérabilité puisque les terminaux seront nativement compatibles avec les réseaux de tous les opérateurs respectant ces standards.

L'identification des objets pose également des questions d'interopérabilité. En effet, comme cela a été vu précédemment, les modalités d'adressage retenues par les différents fabricants pour les objets sont multiples (numéros de téléphone mobiles, identifiants de cartes SIM, adresses IP dans leurs variantes IPv4 ou IPv6, et formats propriétaires non standardisés). En l'occurrence, le déploiement de l'IPv6, en ce qu'il ne présentera pas les problèmes de pénurie observés avec l'IPv4, pourrait être favorable à un accroissement de l'interopérabilité. En effet, ce protocole pourrait servir de langage universel dans la mesure où, dans de nombreux cas, la communication ne se fait pas directement entre objets mais *via* des éléments de réseau intermédiaires assurant une traduction entre les réseaux et protocoles hétérogènes.

4.3 Une autre course aux standards au niveau des couches hautes

Si l'interopérabilité paraît difficile à organiser au niveau des couches basses, certains acteurs semblent se positionner sur les couches hautes pour structurer le marché au niveau applicatif, en gommant l'hétérogénéité des couches physiques. Ces pratiques s'opèrent selon deux modalités, *via* une gouvernance collective ou autour d'un acteur unique.

Dans le premier cas, un standard est porté par une alliance. Ainsi, le consortium AllSeen, par exemple, (comprenant entre autres des acteurs comme Qualcomm, Microsoft, LG et Panasonic) travaille à développer des standards communs de communication *via* la technologie AllJoyn. Cette technologie présente de plus la caractéristique d'être mise à disposition en *open source*.

Dans le deuxième cas, un acteur se saisit du rôle de passerelle entre les objets. Cet acteur peut occuper une place plus ou moins incontournable auprès des fabricants d'objets. Le rôle de la passerelle peut être peu intrusif, lorsque celle-ci joue simplement un rôle de traducteur. C'est le cas par exemple de la plateforme IFTTT « *If This Then That* » qui a établi de nombreux partenariats afin de permettre l'interopérabilité entre les objets via le partage d'APIs, par exemple avec Netatmo pour le *Smart Home*. Son rôle peut au contraire être très étendu, comme dans le cas d'Apple qui a développé le protocole HomeKit ou de Google qui a développé le protocole Weave : ces deux protocoles s'intègrent directement dans les objets de la maison. Dans ce dernier cas, le rôle de l'intermédiaire peut de surcroît être accru lorsque les données doivent nécessairement transiter par sa plateforme.

4.4 Des enjeux de fluidité

Le passage d'une solution technologique à une autre, ou d'un fournisseur à un autre, fait généralement l'objet de coûts de changement, qui peuvent réduire les incitations à la migration et avoir des impacts sur la fluidité et les incitations concurrentielles sur le marché.

Les auditions ont permis d'identifier, à ce stade, trois grandes catégories de coûts de changement potentiels dans le contexte de l'internet des objets.

D'abord, de tels coûts pourraient être supportés lors du changement de fournisseur de connectivité. Il peut s'agir du coût de remplacement complet de l'objet, lorsque les technologies ne sont pas interopérables, ou du coût de changement de carte SIM dans le cas de technologies cellulaires,

interopérables. En effet, le changement d'opérateur sur ces technologies impose un changement physique de cette carte SIM, ce qui engage des coûts de changement importants pour l'utilisateur. Toutefois, il se développe des technologies permettant la reprogrammation des cartes SIM « *over the air* » qui offrent la possibilité de modifier à distance, sans intervention physique sur la flotte de terminaux, le contenu de la carte SIM pour remplacer notamment les clés de sécurité et l'IMSI d'un opérateur par ceux d'un autre. Cette solution semble permettre de limiter, en partie, le verrouillage des utilisateurs vis-à-vis de leurs fournisseurs de connectivités, dans le cas de réseaux cellulaires. Leur bon développement, dans des conditions efficaces et ouvertes à tous les fournisseurs de connectivité cellulaire, constitue un enjeu d'actualité.

Ensuite, des coûts de changement pourraient être dus au manque de transparence sur le marché, compte tenu de la faible comparabilité des informations disponibles, en termes de couverture et de qualité de service, concernant les différents réseaux déployés. L'hétérogénéité observée, par exemple, au niveau de la définition des indicateurs peut nuire à la lisibilité des performances de chaque fournisseur et limite la volonté des utilisateurs à changer de fournisseur.

Enfin, les modalités de portabilité des données ou des contenus pourraient également engendrer des coûts de changement pour les utilisateurs, si le changement de système implique la perte, totale ou partielle, ou du moins la modification, des données des utilisateurs. Les évolutions probables ou à venir du cadre juridique national et européen⁵¹ devraient faciliter la portabilité des données personnelles fournies par les utilisateurs en leur permettant de pouvoir les récupérer dans un format structuré, couramment utilisé et lisible par machine.

Les principaux enjeux

L'émergence de l'internet des objets s'accompagne de l'éclosion d'une multitude de technologies. De nombreux écosystèmes cloisonnés structurent actuellement l'internet des objets, malgré quelques initiatives allant vers plus de standardisation.

Dans ce contexte, l'analyse de l'ouverture se fait en deux temps. Dans un premier temps, alors que le marché est émergent, l'innovation prime, et stimule la concurrence, souvent entre standards. Dans un deuxième temps, lorsque le marché sera plus mature, l'enjeu d'ouverture, à travers celui de l'interopérabilité, deviendra plus prégnant pour s'assurer du bien-être des utilisateurs.

A ce stade du déploiement de l'internet des objets, l'ouverture semble s'organiser naturellement, évitant de brider l'innovation. Néanmoins, l'absence d'ouverture pourra constituer un enjeu si elle conduit au verrouillage des utilisateurs.

⁵¹ Article 21 du projet de loi pour une République numérique et article 20 du règlement 2016/679 du 27 avril 2016 dit « règlement général sur la protection des données », qui entrera en application en mai 2018.

5 La confiance au cœur de l'internet des objets

L'internet des objets est au cœur d'un modèle économique basé sur la production, la mise à disposition et l'exploitation de données. Les auditions ont confirmé le rôle que jouent ces données dans le développement des écosystèmes de l'internet des objets : si la confiance des consommateurs et des entreprises producteurs de données n'est pas établie, l'adoption de l'internet des objets sera limitée.

Cette confiance se décline selon plusieurs aspects, qui seront détaillés par la suite, dont en particulier :

1. La confiance dans l'exactitude, la fiabilité et l'intégrité des données échangées ;
2. La confiance dans la protection des données et dans les traitements qui en sont fait de manière souvent centralisée ;
3. La confiance dans la sécurité, la résilience et la performance des objets connectés et leurs réseaux supports*.

5.1 Le rôle important des données

Les applications qui s'appuient sur la collecte et le traitement de données représentent une opportunité formidable pour le futur, qu'il s'agisse aussi bien de sauver des vies grâce à des dispositifs d'e-santé alertant automatiquement les services d'urgence ou encore d'optimiser en temps réel la gestion du trafic routier ou de l'énergie à l'échelle d'une ville.

Les données représentent la matière première de l'écosystème. Qu'il s'agisse de données à caractère personnel⁵², de données provenant d'une entreprise ou émanant d'une collectivité, la confiance représente un enjeu majeur qui déterminera l'adoption de l'internet des objets par les utilisateurs.

5.1.1 Protection des données personnelles et propriété des données des entreprises

Pour les acteurs commercialisant des objets et capteurs directement à destination du consommateur final, la protection en intégrité et en confidentialité des données liées à l'utilisateur a souvent été présentée comme un enjeu clé pour nouer une relation de confiance avec ce dernier.

Données personnelles : responsabilités vis-à-vis de leur traitement et droit des individus

Du point de vue des données personnelles, la principale problématique posée par les développements récents de l'internet des objets concerne la capacité des individus à disposer d'un contrôle effectif sur les données qui les concernent. Il peut parfois être compliqué d'informer clairement les utilisateurs sur la captation et la destination des données si les objets n'ont pas d'écran.

Au-delà des problématiques liées au caractère sensible de certaines données (par exemple, les données de santé), certains capteurs ou objets connectés produisent des données d'un nouveau genre, à la frontière (floue) de la santé et du bien-être. Liées au corps ou à l'environnement direct des individus, ces données sont susceptibles de révéler leur vie intime, y compris pour les plus anodines d'entre elles *a priori*.

⁵² Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement. Article 2 de la loi « informatique et libertés »

D'une part, les données ainsi collectées ne l'ont jamais été à cette échelle et par ce type d'acteurs. Il n'y a par exemple jamais eu de base de données du nombre de pas quotidiens ou de courbes de poids de milliers de personnes sur plusieurs années détenus par des acteurs privés. Sur ces points, le Règlement européen sur les données reconnaît une acception large des données de santé.

D'autre part, le *big data* offre la capacité de mettre en relation de nombreux types de données, qui pourraient sembler anodines prises de manière indépendante, mais dont la corrélation pourrait permettre de déduire des tendances ou comportements à même de refléter l'intimité des utilisateurs. Il s'agit ici non seulement de protéger des données personnelles en tant que telles, mais également les interconnexions qui sont faites entre différentes bases : cette question est évoquée par la suite.

Propriété et valorisation des données pour les entreprises

Par ailleurs, en dehors des données qu'elles traitent en lien avec des individus, les entreprises peuvent aussi être productrices de données, que celles-ci soient extraites d'objets mis au service de leurs propres moyens de production ou de produits finis *B2B*. La propriété des données (hors données à caractère personnel) - notamment techniques et commerciales - issues des entreprises et le droit d'usage associé ne sont pas encadrés par la loi de la même manière que pour les personnes physiques. La démocratisation de l'internet des objets au sein de toutes les entreprises passera également par la confiance, il est nécessaire de s'assurer que ces dernières, y compris celles qui disposent d'un pouvoir de négociation limité face à leurs fournisseurs IoT, demeurent les propriétaires des données non personnelles qu'elles produisent et disposent de la capacité de les mettre à disposition dans un contexte contractuel et juridique sécurisé.

5.1.2 Destination et usage secondaire des données

Dans un contexte où l'intensité de collecte des données s'intensifie, la nature des données captées et les défis associés varient selon que l'on se situe au plus proche de l'individu, de son corps (*wearable*) et de ce qu'il en fait (*quantified self*), de son environnement direct (domotique) ou au contraire dans des environnements plus éloignés sur lesquels il a *a priori* moins de maîtrise (véhicule connecté, ville intelligente). La capacité de l'utilisateur à être informé des différentes captations dont il est susceptible de faire l'objet est essentiel (type de données collectées, durée de traitement, destinataires,...).

L'agrégation et le traitement de données provenant de sources hétérogènes constitue le cœur de l'internet des objets. Le détournement de la finalité des données collectées représente l'une des préoccupations majeures. Les individus fournissent leurs données dans le cadre d'une finalité précise – ces données n'ont par exemple plus vocation à être conservées dans un format identifiant dès lors qu'elles ne sont plus nécessaires. Or, le foisonnement des données attachées à un utilisateur est susceptible de générer un usage secondaire éloigné de la finalité initiale. Il peut s'agir de déduire des informations intimes de données en apparence anodines (i.e : condition physique sur la base d'une donnée de pas) ou de favoriser les capacités de profilage sur des personnes par recoupement d'informations initialement isolées.

Les questions de transparence sur la finalité de l'usage, sur les méthodes de réutilisation et sur les éventuels transferts de données se posent, de même que la question des méthodes d'anonymisation éventuellement mises en œuvre pour limiter l'exposition des utilisateurs.

5.2 Un enjeu de sécurité complexe encore difficile à appréhender pour les acteurs

Les auditions ont mis en évidence une prise en compte inégale et partielle des questions de sécurité informatique des objets connectés. Les mesures prises pour sécuriser les objets, les réseaux et les moyens de stockage des informations peuvent être insuffisantes au regard des risques auxquels sont exposés les utilisateurs. Ainsi, certains objets se contentent d'un paramétrage par défaut, pouvant permettre à des attaquants d'en prendre le contrôle. Toutefois, l'enjeu de sécurité pourra être différent selon les cas d'usages. Par exemple, le niveau de sécurité exigé ne sera pas le même pour un capteur de température ou pour une pompe à insuline. Par ailleurs, les contraintes liées aux ressources de calculs et d'interface à destination de l'utilisateur ne favorisent pas toujours la sécurisation des objets, ni le déploiement d'éventuelles mises à jour, ni non plus celles liées aux cycles courts de conception des produits.

L'objet connecté doit être considéré comme la partie émergée d'un système d'information complet incluant notamment la collecte, le traitement, le stockage et la restitution des informations issues de ces objets, mais également la gestion et l'administration des objets et du système. Plusieurs facteurs sont à prendre en compte en matière de sécurité informatique pour un objet connecté :

- Sa fonction : capteur d'humidité d'une plantation, objet près du corps, élément d'une « smartgrid », véhicule autonome, automate de contrôle d'un processus industriel, etc. ;
- Sa destination : objet « grand public » ou destiné à un environnement professionnel ;
- Ses capacités : capteur simple ou objet susceptible d'effectuer des traitements ou de recevoir des instructions ;
- Son mode de connexion : directement sur le réseau d'un opérateur de communications électroniques, via un équipement intermédiaire (boîtier de connexion d'un opérateur de type « box », smartphone, équipement urbain), via un réseau spécialisé, éventuellement à bas débit et connecté ou non à un réseau d'opérateur au travers d'une passerelle technique, etc. ;
- Son interaction éventuelle avec d'autres objets connectés ;
- Le type d'information traité : données sensibles, à caractère personnel, médical ;
- Le modèle de possession de l'objet : l'utilisateur peut louer ou posséder l'objet ou être seulement abonné à un service ;
- La réutilisation de briques embarquées de système d'information largement utilisées ou non.

L'ensemble de ces risques doit être analysé de manière systémique et décliné à l'échelle de l'objet : un objet connecté compromis peut à son tour participer à la compromission du réseau dans lequel il est intégré ou à celle de systèmes d'informations tiers. Les risques à prendre en compte sont ceux habituellement traités par les analyses de risque liées à la sécurité des systèmes d'information :

- Risques en matière de *disponibilité* : la compromission intentionnelle ou non d'un objet connecté par un code malveillant peut entraîner son inaccessibilité pour son utilisateur ou son utilisation à des fins malveillantes, par exemple pour intégrer l'objet au sein d'un réseau destiné à provoquer des dénis de services distribués (DdoS) et nuire ainsi à la disponibilité d'autres ressources informatiques ;
- Risques en matière de *confidentialité* : l'information transmise par l'objet connecté peut être interceptée lors de son recueil, de son transport, de son traitement ou de son stockage, des fonctions de l'objet peuvent être détournées de leur usage initial (un micro destiné à répondre à des appels peut, par exemple, permettre d'écouter l'environnement de l'objet) ;

- Risques en matière d'*intégrité* et d'*authenticité* : une compromission informatique peut altérer le fonctionnement de l'objet, modifier ses fonctions, ses conditions de réponses ou les informations transmises.

Ces risques doivent être pris en compte sur toute la durée de vie de l'objet connecté, en fonction de l'évolution de la menace. Ainsi, le maintien en condition de sécurité a autant d'importance que l'intégration de la sécurité informatique dans la conception et le développement initial de l'objet. Les conséquences d'une sécurité informatique insuffisamment prise en compte lors de la conception, du développement ou de l'utilisation d'objets connectés peuvent être graves : perte de vies humaines, atteinte à la vie privée ou aux biens, perte de compétitivité, nuisance dans la vie quotidienne, atteinte à la sécurité ou à la défense nationale. Ces enjeux doivent être considérés au regard de la criticité de l'objet concerné, afin de trouver un équilibre entre nécessité de sécurité et coût de mise en œuvre. A titre d'exemple, les risques encourus concernant un capteur de température ne sont vraisemblablement pas les mêmes que pour un véhicule autonome.

Au-delà des problématiques liées à la sécurité des objets en eux-mêmes, la sécurité des réseaux qui interconnectent ces objets devrait faire l'objet de la plus grande attention. Les obligations en termes de sécurité et de résilience sont encadrées par le droit national et applicables à tout exploitant de réseau de communications électroniques ouvert au public, y compris le cas échéant aux opérateurs de réseaux dédiés à l'internet des objets. En revanche, la sécurité des réseaux non opérés, c'est-à-dire gérés directement par l'utilisateur, pourrait quant à elle constituer le maillon faible dans la chaîne de sécurité, du fait de sa gestion déléguée au niveau de l'utilisateur (hotspot Wi-Fi, Bluetooth, etc.). Dans ce cas, la question de la sécurité des objets continue à se poser, sur les fabricants d'objets connectés et les services associés.

Les principaux enjeux

L'adoption de l'internet des objets est conditionnée à la capacité à assurer la confiance de l'utilisateur, producteur de données.

Les utilisateurs (consommateur, entreprise ou collectivité) doivent pouvoir garder le contrôle sur les données qui les concernent. Il est par ailleurs nécessaire d'assurer la transparence vis-à-vis de l'utilisateur afin d'éviter un usage secondaire inconnu et éloigné de la finalité initiale de la fourniture des données.

La sécurité des objets et des réseaux constitue également un élément essentiel pour assurer la confiance. Le niveau de sécurité requis doit être considéré au regard de la criticité de l'objet concerné et des données qu'il collecte, afin de trouver un équilibre entre nécessité de sécurité et coût de mise en œuvre.

6 La période de transition pour les acteurs de l'internet des objets

L'internet des objets pourra profiter à plusieurs grandes catégories d'utilisateurs :

- les entreprises, qui verront leurs processus métiers modernisés et leurs outils productifs et logistiques optimisés, qui connaîtront mieux le cycle de vie de leurs produits, et dont le modèle économique pourrait être bousculé ;
- les collectivités territoriales, et plus largement les territoires, qui intégreront le numérique dans les missions traditionnelles de la ville, les nouveaux services aux urbains, le développement économique et les modalités de participation citoyenne ;
- les particuliers, qui feront entrer dans leurs quotidiens une multitude d'objets connectés ;
- les différents acteurs de la chaîne de valeur de l'offre de l'internet des objets, en particulier les fabricants d'objets et de modules, équipementiers, opérateurs, fournisseurs d'application qui se saisiront de l'internet des objets pour développer leurs activités et leurs services..

6.1 L'importance d'échanges continus entre pouvoirs publics et acteurs de l'internet des objets

La phase d'auditions a mis en avant la volonté d'une communication soutenue entre les pouvoirs publics et les acteurs participant à l'émergence de l'internet des objets. En ce sens, la démarche initiée par l'Arcep et ses partenaires a reçu un accueil très favorable. Cela concerne en particulier deux aspects :

- le dialogue avec les pouvoirs publics concernant le cadre réglementaire applicables aux nouveaux usages basés sur les technologies de l'internet des objets, d'une part ;
- la mise en réseau des acteurs nationaux et européens impliqués dans la chaîne de valeur de l'internet des objets, dans une logique de compétitivité et de filière industrielle, d'autre part.

Ainsi, ce premier dialogue entre l'Arcep, ses partenaires et les sociétés auditionnées a permis de mettre en lumière un manque de lisibilité du cadre réglementaire. En effet, les nouveaux usages (véhicule connecté, drone, santé connectée, usine du futur, *smartgrids*, *smart city*, etc.) issus de l'internet des objets affectent de nombreuses filières et se retrouvent au croisement de plusieurs régulations – données personnelles, communications électroniques, dont la neutralité du net, loyauté des plateformes et autres régulations sectorielles – dont la maîtrise n'est pas évidente pour tous les acteurs. Les acteurs appellent à un dialogue récurrent entre les pouvoirs publics et l'ensemble de l'écosystème afin de clarifier les contours de l'environnement réglementaire auquel sont soumises les solutions de l'internet des objets, sans pour autant avancer vers la mise en place d'un cadre réglementaire dédié car une régulation précipitée risquerait selon eux de freiner le déploiement de l'internet des objets qui n'en est encore qu'à son début.

Par ailleurs, au-delà des échanges avec les pouvoirs publics, les auditions ont également confirmé le besoin de fédérer les acteurs de la chaîne de valeur en assurant un dialogue entre eux. Dans un premier temps, en encourageant le partage d'expériences sur des enjeux, comme par exemple celui de la sécurité, afin de permettre d'accompagner les acteurs dans la maîtrise des différents enjeux liés aux objets connectés ainsi qu'aux réseaux associés. Dans un deuxième temps, certaines sociétés rencontrées souhaitent également des rapports simplifiés et accélérés entre startups, PME et grands groupes afin d'initier et d'encourager les partenariats entre entreprises, dont les collectivités locales sont également parties prenantes, pour booster l'internet des objets en France. Des dispositifs comme l'initiative French Tech ou les pôles de compétitivité permettent aujourd'hui de jouer ce rôle en simplifiant les échanges, facilitant les prises de contacts et encourageant les rencontres, mais

également en aidant à la projection sur les marchés mondiaux comme le prouve la présence d'acteurs français des objets connectés au CES sous la bannière French Tech.

6.2 La volonté de mises en œuvre concrètes des usages de l'internet des objets

Si la vague attendue de l'internet des objets ne semble pas encore d'actualité, c'est que les acteurs ont dans un premier temps préféré les démonstrations de faisabilité, ou « *Proof of Concept* » au détriment d'applications de plus grande envergure. Aujourd'hui, les auditions indiquent que les acteurs semblent sortir de cette phase d'expérimentation pour proposer des applications réelles au service des entreprises, des collectivités et du grand public.

Les entreprises sont d'ailleurs les premières utilisatrices à déployer de premières applications concrètes. Pour le moment, les solutions proposées aux entreprises restent essentiellement de la relève d'information à des échelles locales, mais devraient dans un avenir proche aller vers des applications plus complexes comme la commande, avant d'envisager un véritable déploiement industriel des solutions. Les particuliers profitent également d'applications concrètes issues de l'internet des objets alors que de nombreuses collectivités territoriales sont très demandeuses de démonstrateurs pour tester les différents montages et étudier l'organisation des nouveaux services des territoires. En effet, ces expérimentations sont l'occasion pour les collectivités de définir les exigences (sécurité, confidentialité, etc.) qu'elles souhaitent mettre en place dans les services dont elles délèguent la gestion.

6.3 Le positionnement international de la France et de l'Europe

Au-delà de la bonne adéquation du cadre réglementaire, nécessaire pour permettre aux usages de se développer et de se déployer, il importe également pour les pouvoirs publics d'organiser la mise en réseau des acteurs nationaux et européens impliqués dans la chaîne de valeur de l'internet des objets, dans une logique de compétitivité et de filière industrielle.

Le déploiement de l'internet des objets dépasse les frontières françaises et se joue sur la scène européenne et internationale. Il faudra pour les pouvoirs publics s'assurer d'une place forte de la France et de l'Europe parmi les acteurs de l'internet des objets en comparaison avec la Chine et les Etats-Unis et mettre en place un cadre réglementaire harmonisé au niveau européen.

Dans le cadre des travaux de la nouvelle France industrielle, la solution « Objets intelligents » permet de développer une stratégie nationale française et de se structurer en filière pour mener des actions coordonnées pour développer les entreprises française des objets intelligents, en associant les entreprises concernées. Des travaux sont également engagés pour consolider le positionnement français sur la *smart city via* la connexion avec la solution « Ville durable ».

Le développement des *start-ups* françaises est également un enjeu : il faudra leur donner les moyens de se financer, de se structurer (sur le plan marketing, RH, ligne produit, et bien valoriser l'argent investi) et de développer leurs offres.

Les acteurs européens se montrent présents au sein des alliances industrielles mondiales et des organismes de normalisation menant des stratégies de standardisation autour des futures applications concrètes de l'internet des objets. C'est le cas par exemple de la LoRa Alliance qui réunit des opérateurs européens et des acteurs mondiaux pour travailler à plus de standardisation dans le

domaine de l'internet des objets. L'AFNOR⁵³ a de son côté créé début 2016 la Commission Nationale sur l'internet des objets (CN IoT) pour défendre les enjeux français lors des travaux internationaux menés par l'ISO. Également, l'ETSI participe à la création d'un projet partenarial « OneM2M », fondé sur le même modèle que le 3GPP et dédié à la standardisation de la couche service des équipements M2M et des objets connectés. Dans le cadre de la *smart city*, la Commission Nationale Aménagement Durable et résilient (CN ADR) intègre la problématique des services urbains intelligents.

Les principaux enjeux

La phase de transition dans le déploiement des solutions de l'internet des objets est un sujet abordé lors des auditions à la fois par les utilisateurs – collectivités territoriales et industriels – mais aussi par les acteurs de l'offre de l'internet des objets. Il en ressort deux aspects distincts et complémentaires.

Le message est tout d'abord celui d'une communication soutenue avec les pouvoirs publics, qui doivent rester au contact des acteurs de l'internet des objets, de ceux qui le font et de ceux qui l'utilisent, y compris le grand-public, afin de connaître et comprendre ces évolutions, et assurer la lisibilité et la bonne adéquation du cadre réglementaire.

Dans une logique différente mais complémentaire, de compétitivité et de filière industrielle, il s'agira par ailleurs de maintenir une position forte des acteurs français sur la scène internationale..

⁵³ Association française de normalisation.

Annexe n°1 – Liste des auditions menées

Date des auditions	Nom des entreprises
Jeudi 12 novembre 2015	Actility
Jeudi 12 novembre 2015	Intel
Mardi 17 novembre 2015	Connecthings
Mercredi 25 novembre 2015	Commission de régulation de l'énergie
Mercredi 25 novembre 2015	Idate
Mercredi 02 décembre 2015	Huawei
Jeudi 03 décembre 2015	Numericable-SFR
Mardi 08 décembre 2015	Adeunis RF
Mardi 08 décembre 2015	Chaire "Internet of Everything" de Polytechnique
Jeudi 10 décembre 2015	Bluelinéa
Jeudi 10 décembre 2015	ERDF
Lundi 14 décembre 2015	IBM
Jeudi 07 janvier 2016	Qowisio
Lundi 11 janvier 2016	Google
Mercredi 13 janvier 2016	Ericsson
Mardi 19 janvier 2016	Sequans
Mardi 19 janvier 2016	Optiflows
Mercredi 20 janvier 2016	Kerlink
Mercredi 20 janvier 2016	Nest
Jeudi 21 janvier 2016	Cisco
Jeudi 21 janvier 2016	STMicroelectronics

Mardi 26 janvier 2016	Bouygues Telecom
Mardi 26 janvier 2016	Sigfox
Jeudi 28 janvier 2016	Qualcomm
Mardi 02 février 2016	Sagemcom
Mardi 02 février 2016	Legrand (batiment)
Jeudi 11 février 2016	Orange
Mardi 16 février 2016	SNCF - Direction Digital
Jeudi 18 février 2016	Eutelsat
Jeudi 18 février 2016	Samsung

Annexe n °2 – Liste des ateliers menés

Nom des ateliers	Date des ateliers	Nom des entreprises
Industrie & Transport connectés	Lundi 23 mai 2016	Blue Solutions
		Hub One
		Mission Transport Intelligents
		Renault
		RTE
		SNCF
		Thalès
		Transdev
Bâtiment connecté & Ville intelligente	Jeudi 23 juin 2016	AFNOR
		AVICCA
		Enedis
		Ijenko
		JC Decaux
		M2ocity
		Nokia
		Oledcomm
		Sigfox
		Suez
		Vertical M2M
Santé connectée	Lundi 27 juin 2016	AFNOR
		Altran
		ASIPS

		DGCCRF
		INRIA
		Korian
		Medappcare
		Nokia
		Orange
		Télécom ParisTech