

Paris, le 22 mars 2018

## LES OBJETS CONNECTÉS

*Parlementaire référent :*

- M. Didier Baichère, député, vice-président de l'OPECST.

*Membres du conseil scientifique de l'OPECST consultés :*

- M. Stéphane Mangin, professeur de physique, université de Lorraine, Institut Jean Lamour – CNRS, membre de l'Institut universitaire de France ;
- Mme Virginie Tournay, directeur de recherche au CNRS en sciences politiques.

*Autres experts consultés :*

- M. Alain Berthoz, professeur honoraire au Collège de France, neurophysiologiste, spécialiste de la physiologie intégrative ;
- M. Dimitri Carbone, fondateur de Livosphere, expert en internet des objets et en intelligence artificielle auprès de la direction générale des entreprises du ministère de l'économie et des finances (DGE- plan objets intelligents) et de la Banque publique d'investissement (BPI) ;
- M. Ludovic Le Moan, directeur général (CEO) et cofondateur de Sigfox ;
- M. Christian Licoppe, professeur de sociologie des technologies d'information et de communication à Télécom ParisTech ;
- M. Hugo Mercier, ingénieur, polytechnicien, cofondateur et PDG de Rythm, jeune pousse (*start-up*) spécialisée dans les objets connectés dans le domaine de la santé.

*Secrétariat de l'Office :*

- M. Daniel Bokobza, conseiller ;
- M. Olivier Dussouillez, élève-ingénieur, stagiaire ;
- M. Nicolas Thomas, étudiant en master 2 de sciences politiques, stagiaire.

Cette note de synthèse, qui s’inscrit dans une nouvelle orientation des productions de l’Office sous forme de « note courte », traite des objets connectés<sup>(1)</sup>, également appelés « internet des objets » (*Internet of things*), avec une présentation des définitions (I), des enjeux (II) et des défis technologiques qu’ils posent. Ce sujet a été évoqué par des membres du conseil scientifique de l’OPECST, réuni le 27 septembre 2017, comme étant d’intérêt pour l’Office.

## I. QUE SONT LES OBJETS CONNECTÉS ?

### A. POURQUOI PARLE-T-ON D’OBJETS CONNECTÉS ET D’INTERNET DES OBJETS ?

Les objets connectés existent depuis de nombreuses années dans notre environnement quotidien (signalisation à distance, capteur de pression à l’entrée des parkings, etc.). Ces objets, qui étaient auparavant limités (connectés par câbles directement à un actionneur ou, au mieux, à un réseau local), se sont récemment développés.

Cela s’explique, dans un premier temps, par les progrès réalisés dans les domaines de l’électronique embarquée, des télécommunications ou encore du traitement des données.

À l’image des microsystèmes électromécaniques (« *MEMS* »), que l’on trouve dans nos terminaux de poche (*smartphones*), ainsi l’accéléromètre ou le gyroscope, les composants électroniques sont de plus en plus miniaturisés et efficaces. Les systèmes électroniques embarqués profitent d’une meilleure gestion de l’énergie et de batteries énergétiquement plus denses, qui les rendent plus autonomes. La qualité de la couverture réseau s’est améliorée, de même que les technologies de communication. Citons, par exemple, la technologie dite de « réorganisation dynamique des communications » entre les nœuds d’un réseau (*self-organizing-network*) de la « *4G LTE* », qui améliore la qualité de service et la consommation d’énergie de ces nœuds. Enfin, les possibilités de traitement des données se sont accrues grâce au développement de nouveaux algorithmes et de nouveaux outils logiciels relatifs, par exemple, aux « volumes massifs de données » (*Big Data*) ou à l’intelligence artificielle, et par la capacité de calcul disponible dans le « nuage » (*cloud*) et dans les puces embarquées.

**Du fait de ces progrès, les objets connectés ne sont donc plus des simples capteurs ou « actionneurs »<sup>(2)</sup> (*actuator*) : ils fonctionnent au sein de réseaux et peuvent créer, communiquer, agréger, analyser et agir sur des données.**

En outre, les améliorations technologiques se sont accompagnées d’une baisse significative du coût de ces technologies. Les systèmes électroniques embarqués sont donc non seulement plus performants, mais aussi bien moins chers à produire qu’auparavant. Par exemple, le coût moyen d’un accéléromètre était de 2 dollars américains en 2006 contre 0,40 dollars en 2015. De même, les améliorations technologiques et la guerre féroce entre les acteurs technologiques (en particulier Amazon et Microsoft) ont fait chuter les prix du « nuage » (*cloud*) : les prix de certains services proposés par Amazon ont été divisés par deux entre 2011 et 2014.

---

(1) Voir en partie II-A les différents types de connexion.

(2) « Appareil, organe d’un appareil agissant sur une machine de manière à modifier son état ou son comportement. » Dictionnaires Le Robert - Le Grand Robert de la langue française.

**En plus des progrès technologiques, la baisse des coûts rend l'électronique et le traitement des données de plus en plus abordables. Conséquemment, selon les experts du secteur, un changement d'échelle devrait avoir lieu : le nombre d'objets connectés dans le monde devrait exploser rapidement, atteignant jusqu'à 80 milliards <sup>(1)</sup> d'ici à trois ans. Cela donnerait ainsi naissance à un véritable « internet des objets ».**

#### QUELQUES REPÈRES CONCERNANT L'INTERNET DES OBJETS

1999 : Le terme *Internet of things* (internet des objets) est créé au *Massachusetts Institute of Technology* (MIT) pour désigner l'usage de radio-étiquettes « RFID », dans le but de traquer des biens dans une chaîne de distribution et de transmettre l'information par internet.

2008 : Les travaux de spécification et de standardisation de l'internet des objets débutent.

2009 : Un seuil symbolique est franchi : plus d'objets sont connectés à l'internet qu'il n'y a d'humains sur Terre.

2017 : Selon IBM, 90 % des données dans le monde ont été créées les deux dernières années. Plusieurs facteurs expliquent ces volumes massifs de données générés (*Big Data*), l'un étant l'usage de plus en plus répandu des objets connectés.

2020 : Le nombre d'objets connectés pourrait osciller entre 30 milliards (selon le cabinet d'études Gartner) et 80 milliards (selon le cabinet d'études iDate) <sup>(2)</sup>.

## B. L'INTERNET DES OBJETS IMPACTE TOUS LES SECTEURS

L'internet des objets touche tous les secteurs d'activité. En premier lieu, les technologies de l'internet des objets sont utilisées dans l'industrie pour faciliter la maintenance des équipements, pour améliorer la chaîne logistique (*supply chain*), pour surveiller la consommation et la production d'électricité, etc. En agriculture, les machines agricoles connectées permettent de rationaliser l'usage d'intrants et de cartographier des parcelles. En ce qui concerne les professionnels de la santé, ceux-ci vont de plus en plus recourir aux objets connectés pour améliorer la prise en charge des patients (localisation des patients dans un hôpital, lit d'hôpital « intelligent » qui suit en temps réel les données vitales des patients, etc.). L'espace public profite, lui aussi, de l'internet des objets : certaines métropoles sont déjà équipées de réseaux de capteurs permettant de mesurer la qualité de l'air.

#### DEUX EXEMPLES :

##### COSMO CONNECTED, LE FEU DE FREINAGE CONNECTÉ POUR LES CASQUES DE MOTO

Coûtant environ 120 euros, le feu de freinage connecté Cosmo Connected s'accroche au casque de moto de son utilisateur par aimantation. Équipé d'un accéléromètre, le feu de freinage s'allume pour indiquer aux autres usagers de la route que le motard équipé du Cosmo Connected ralentit. En cas de suspicion d'accident et moyennant un abonnement, le système contacte le motard puis envoie sa position GPS aux secours si celui-ci ne répond pas.

##### LES CAPTEURS DE LA SOCIÉTÉ AIRINOV POUR L'AGRICULTURE DE PRÉCISION

La société AIRINOV a développé un capteur prévu pour être embarqué sur un drone. L'analyse des données enregistrées grâce à ce capteur permet de cartographier de manière précise les champs survolés par le drone. Pour

(1) Les estimations divergent quant au nombre d'objets qui seront connectés en 2020, ce nombre oscillant entre 30 milliards selon le cabinet Gartner et 80 milliards selon le cabinet iDate. Quoi qu'il en soit, les investissements colossaux dans les technologies de l'internet des objets (à l'échelle mondiale, 800 milliards de dollars y ont été investis en 2017) démontrent l'ampleur que doit prendre l'internet des objets.

(2) « Le marché des objets connectés (quelques chiffres) », *Correspondant informatique et libertés du CNRS*, 7 septembre 2015 : <http://www.cil.cnrs.fr/CIL/spip.php?article2760>.

chaque parcelle, l'agriculteur accède ainsi à de nombreuses données : « besoins en engrais, dommages provoqués par les animaux sauvages ou les intempéries, indices de biomasse et hauteur des plants, etc. ».

Malgré la couverture médiatique dont il bénéficie, le marché grand public est moins mûr que le marché interentreprises (*B to B*). Au vu du prix, de la durée d'intérêt des objets connectés ou encore de l'obsolescence rapide de ceux-ci, la valeur ajoutée des objets connectés actuels n'apparaît pas évidente aux consommateurs. Se distinguent néanmoins, les objets connectés portables (les *wearables*)<sup>(1)</sup>, qui sont les objets connectés « grands publics » connaissant le plus grand succès. En effet, les *wearables* proposent un service clairement identifié par le consommateur et accompagnent une dynamique sociale qui prône performance, santé et bien-être. La domotique (*Smart Home*) est un autre marché « grand public » jugé particulièrement prometteur.

Ainsi, huit secteurs et une quarantaine d'applications ont été identifiés par le cabinet A.T Kearney comme pouvant être particulièrement impactés par l'internet des objets d'ici à 2025 :

Transport	Santé	Logement et hôtellerie	Industrie
<ul style="list-style-type: none"> <li>• Prévention des accidents</li> <li>• Partage de voitures</li> <li>• Plates-formes VTC et taxis</li> <li>• Voitures autonomes</li> <li>• Transport public et gestion des routes</li> <li>• Télématique</li> <li>• Réduction des embouteillages</li> </ul>	<ul style="list-style-type: none"> <li>• Convalescence à domicile</li> <li>• Surveillance de maladies chroniques</li> <li>• Optimisation de la consommation de médicaments</li> <li>• Réduction de la « non-observance thérapeutique »</li> <li>• Identification rapide de maladies et de risques</li> <li>• Gain de temps grâce à des meilleurs traitements</li> </ul>	<ul style="list-style-type: none"> <li>• Économies d'énergie</li> <li>• Alarmes incendies</li> <li>• Domotique</li> <li>• Alarme anti-intrusion à distance</li> <li>• Connectivité des biens</li> <li>• Télématique</li> <li>• Optimisation énergétique dans les hôtels</li> </ul>	<ul style="list-style-type: none"> <li>• Livraison fournisseurs/clients</li> <li>• Construction intelligente</li> <li>• Suivi des containers</li> <li>• Suivi des wagons ferroviaires</li> <li>• Gestion de flottes</li> <li>• Maintenance prédictive et optimisation de la production</li> </ul>
Vente	Services publics	Secteurs primaires	Administration publique
<ul style="list-style-type: none"> <li>• Réduction des ruptures de stocks et des vols</li> <li>• Gestion de flottes</li> <li>• Caisses automatisées</li> <li>• Livraison de colis</li> <li>• Articles de sport connectés</li> </ul>	<ul style="list-style-type: none"> <li>• Réseaux électriques intelligents</li> <li>• Réseaux de distribution de gaz intelligents</li> <li>• Réseaux de distribution d'eau intelligents</li> </ul>	<ul style="list-style-type: none"> <li>• Agriculture de précision : gestion des plantations</li> <li>• Agriculture de précision : gestion du bétail</li> <li>• Collecte de données et optimisation des procédés d'extraction de pétrole, de gaz, de métaux.</li> </ul>	<ul style="list-style-type: none"> <li>• Efficacité de l'administration publique</li> <li>• Contrôle de l'éclairage public</li> <li>• Gestion des déchets</li> <li>• Éducation</li> </ul>

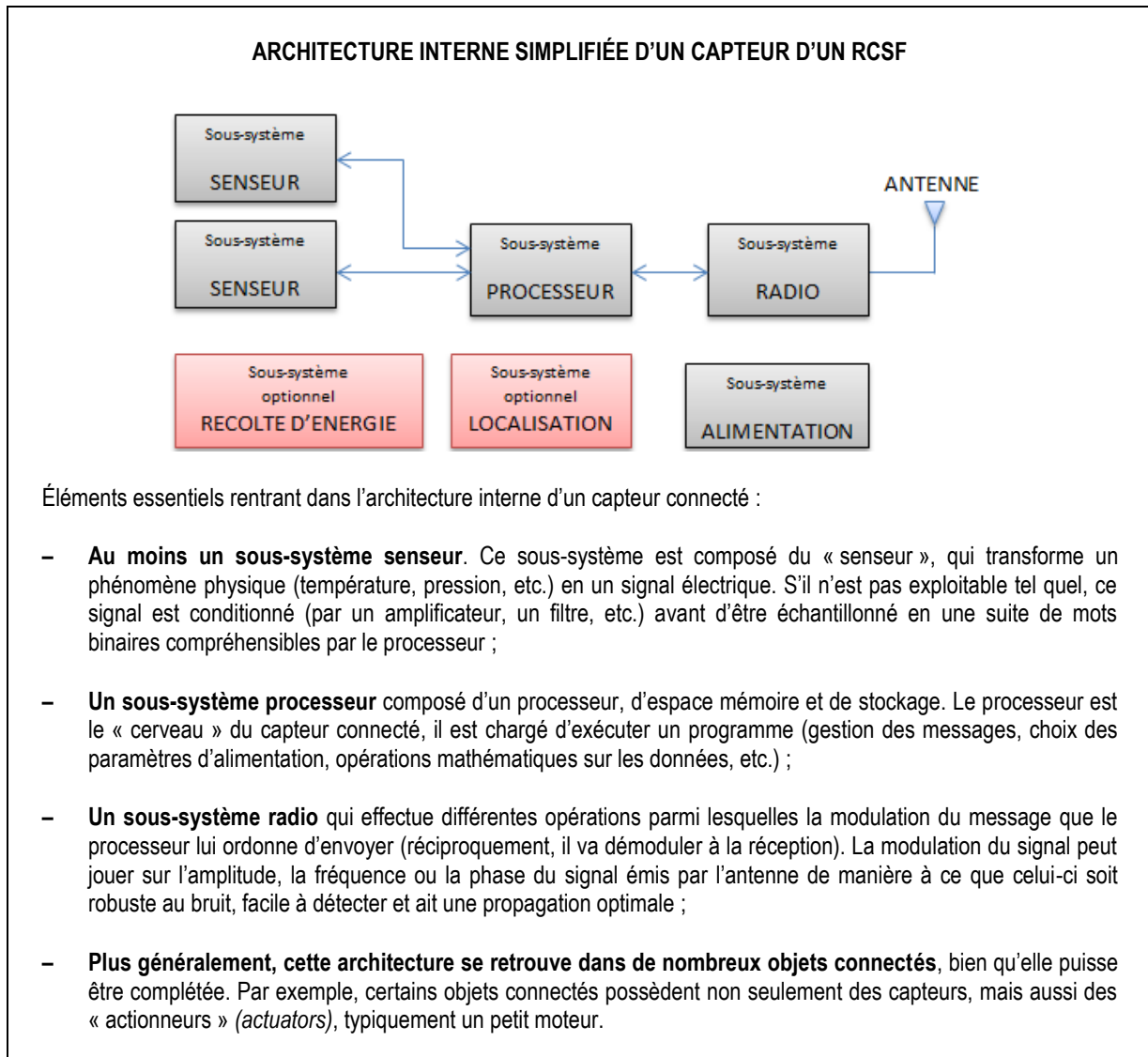
### C. UN EXEMPLE D'OBJETS CONNECTÉS : LA MAINTENANCE PRÉDICTIVE

La maintenance prédictive est, à ce jour, une des applications les plus probantes de l'internet des objets. Notamment utilisée dans l'industrie, elle s'appuie sur des réseaux de capteurs sans fil – RCSF (*Wireless Sensors Networks – WSN*).

Les capteurs du RCSF sont disposés à des endroits stratégiques de l'objet à surveiller (infrastructures, chaîne de production, etc.). L'ensemble de ces capteurs connectés recueillent d'importants volumes de données qui peuvent être de différentes natures (pression, température, humidité, etc.) en fonction des besoins. Leur analyse permet de prédire de manière localisée (dans le temps et dans l'espace) des dysfonctionnements et ainsi d'anticiper

(1) Aucun équivalent en français ne semble émerger.

des interventions de maintenance. Cette solution est bien plus efficace que la maintenance préventive, dont le caractère systématique induit des coûts importants pour un résultat moindre.



À titre d'exemple, un RCSF composé de 64 capteurs connectés a été mis en place pour surveiller, à distance, les propriétés mécaniques du *Golden Gate Bridge* (San Francisco). Les vibrations mesurées tous les millièmes de seconde par chaque capteur du pont sont analysées au regard du modèle mécanique théorique du *Golden Gate Bridge*, de manière à prédire des anomalies éventuelles. La mise en place de ce RCSF permet donc d'assurer la sécurité du pont, à un faible coût, de manière fiable et sans interférer avec son exploitation.

## II. LES ENJEUX DES OBJETS CONNECTÉS SONT CONSIDÉRABLES

### A. ENJEUX ÉCONOMIQUES ET SUR L'EMPLOI

#### 1. Une hypothèse chiffrée à mille milliards d'euros d'ici à 2025 pour l'Union européenne

L'internet des objets est un enjeu économique de premier plan. Le cabinet AT Kearney estime que, grâce à la vente et à l'usage des objets connectés, la création de valeur

pour l'Union européenne<sup>(1)</sup> s'élèverait à environ **mille milliards d'euros, représentant 7 points de PIB, d'ici à 2025, soit :**

– **80 milliards d'euros seraient générés par le marché des objets connectés en lui-même.** Différents cabinets et entreprises se sont essayés à estimer le nombre d'objets connectés qu'il y aura dans le monde en 2020. L'hypothèse basse prévoit environ 30 milliards d'objets connectés en 2020 (Gartner) tandis que d'autres cabinets (iDate) sont encore plus optimistes, prévoyant jusqu'à 80 milliards d'objets connectés en 2020<sup>(2)</sup> ;

– **210 milliards d'euros seraient économisés par la réduction des risques de santé des utilisateurs d'objets connectés et générés par le gain de temps dans la vie quotidienne des individus réemployés dans des tâches productives.** Par exemple, le cabinet McKinsey estime que l'internet des objets pourrait réduire de 17 % le travail nécessaire à l'entretien d'une maison, grâce à l'automatisation de certaines corvées (aspirateur, tonte du gazon, etc.) ;

– **le pouvoir d'achat des citoyens européens pourrait augmenter de 300 milliards d'euros, notamment en raison d'une meilleure maîtrise de leurs dépenses d'énergie ;**

– **430 milliards d'euros seraient dus à l'augmentation de la productivité dans les entreprises** (meilleures prises de décisions dues au croisement des données produites par les objets connectés, actions à distance, optimisation de processus, etc.).

## **2. Le risque de captation de valeur par des acteurs étrangers**

**L'intérêt de l'objet connecté réside avant tout dans les données qu'il génère, celles-ci étant nécessaires à la mise en place de services.**

En particulier, la capacité à faire fonctionner ensemble des réseaux d'objets connectés conçus pour des applications différentes est essentielle, la mise en relation des données de ces réseaux pouvant donner lieu à des solutions à haute valeur ajoutée économique.

Néanmoins, toute conception d'un réseau d'objets connectés s'accompagne de nombreuses contraintes portant sur la topologie du réseau, sur les infrastructures à utiliser, sur la portée des communications entre les objets connectés, sur la quantité de données à faire transiter par jour, sur la qualité de service attendue, sur la gestion de l'énergie, etc. Ainsi, en mai 2017, selon l'IEEE<sup>(3)</sup>, il existait environ 350 standards de communication (et 110 autres étaient en cours de développement) applicables à l'internet des objets. Certains objets sont connectés via le réseau mobile, d'autres grâce à un smartphone (en wifi ou en Bluetooth), tandis que d'autres utilisent des réseaux dédiés à l'internet des objets, à l'instar de Sigfox et LoRa. Les objets connectés ne sont pas tous, *stricto sensu*, reliés à l'internet. Par exemple, les objets connectés de domotique, commercialisés par Legrand, utilisent les protocoles KNX ou ZigBee pour communiquer au sein d'un « réseau local »<sup>(4)</sup>. L'achat d'une « passerelle » permet de faire le pont entre ce réseau local et l'internet.

---

(1) Royaume-Uni compris.

(2) Voir supra.

(3) Institut des ingénieurs électriciens et électroniciens.

(4) Des initiatives visent à imposer un standard unique en domotique. Elles n'ont pas réussi jusqu'à présent.

**EXEMPLE : LA CONNECTIVITÉ POUR TOUS DE SIGFOX  
LE RÉSEAU DES BÉNÉFICIAIRES DE L'ALLOCATION PERSONNALISÉE  
D'AUTONOMIE (APA) DANS LE DÉPARTEMENT DU LOIRET**

L'entreprise française Sigfox propose un réseau mondial de communication pour les objets connectés. Actuellement 45 pays sont connectés, dont la France, l'objectif étant de couvrir le territoire national de 60 pays avant la fin de l'année 2018. Le réseau bas débit de Sigfox permet l'échange de petits messages avec le même protocole partout dans le monde. Il repose sur une technologie simple, fiable et autonome. Il présente l'avantage d'un coût réduit et d'une consommation d'énergie réduite par rapport à l'internet. Il n'a fallu que 5 millions d'euros pour couvrir d'antennes tout le territoire français, ce qui permet de réduire la fracture numérique.

Alors que les modules 4G intégrés dans les objets connectés coûtent une vingtaine d'euros, ceux du réseau Sigfox coûtent environ 20 centimes, avec une perspective de seulement 2 ou 3 centimes demain. Une montre connectée au réseau Sigfox coûte une vingtaine d'euros. L'abonnement au réseau coûte 3 euros par an.

Le Département du Loiret a créé Lysbox, un dispositif d'accompagnement et de protection des personnes âgées à distance, en partenariat avec Sigfox. L'investissement réalisé par le conseil général a été rentabilisé en 9 mois.

Ce boîtier permet le suivi des prestations d'aide à domicile reçues par les personnes âgées. Les bénéficiaires et leurs familles peuvent accéder à l'ensemble des données en temps réel via un portail social. Ce boîtier pourra à terme proposer un bouquet de services aux usagers, tel que le relevé de températures automatique et l'alerte si nécessaire (plan canicule ou grand froid). L'objectif est de lutter contre l'isolement des personnes dépendantes et de leur permettre de conserver un maximum d'autonomie pour rester à leur domicile, tout en bénéficiant d'aides, d'assistance, de protection et de soins optimaux.

Le dispositif a été déployé chez les bénéficiaires de l'allocation personnalisée d'autonomie (APA) résidant dans le département. Équipés d'un badge, les auxiliaires peuvent ensuite consulter les plans d'aides, saisir des compléments d'intervention et même contacter le département si besoin.

La Lysbox utilise la technologie innovante bas débit de Sigfox. Le Loiret a été le premier département de France à être couvert en bas débit grâce à des antennes installées dans les casernes de pompiers et les mairies volontaires. Pour tous les départements ruraux, la démographie vieillissante est une véritable problématique de santé publique. Le Loiret se donne les moyens d'agir sur le bien-vieillir et fait le pari de développer une économie d'avenir au service de ses aînés.

Pour permettre d'agrèger les données générées par des réseaux d'objets connectés divers (éventuellement ces objets sont de marques, de natures différentes et utilisent des formatages de données singuliers) et pour permettre l'interaction des objets connectés d'une manière simple et standardisée, des plates-formes tendent à émerger. Celles-ci seront un élément clé de l'interopérabilité des objets connectés.

Différents acteurs développent actuellement leur plate-forme : des opérateurs télécoms (Orange, Bouygues, SFR, etc.), des industriels (Schneider Electric), des jeunes pousses (Sigfox), des géants du nuage informatique (*cloud computing*) (Amazon, Microsoft, Google, IBM, etc.).

Le risque est donc que les acteurs économiques qui parviendront à imposer leur plate-forme en attirant concepteurs d'objets connectés, prestataires de services associés, développeurs d'applications, utilisateurs, etc. soient les géants du numérique américains (ou plus généralement non européens). Ceux-ci capteraient alors systématiquement une partie de la valeur ajoutée des services utilisant l'internet des objets. Au vu des enjeux économiques et stratégiques, il est donc nécessaire que la France et l'Europe (qui ont déjà perdu la guerre de l'ordinateur personnel, du téléphone, des moteurs de recherche, des navigateurs internet, du paiement en ligne, etc.) arrivent à se positionner sur ce marché.

### 3. Des effets incertains sur l'emploi

Le rapport d'information sur « Les objets connectés » de la commission des affaires économiques de l'Assemblée nationale de janvier 2017<sup>(1)</sup> notait le retard de l'industrie française en matière de numérisation par rapport à ses voisins européens (l'Allemagne en premier lieu). Ce rapport estimait que l'internet des objets pourrait être un facteur de ré-industrialisation de la France en permettant de produire davantage de solutions<sup>(2)</sup> technologiques à haute valeur ajoutée, alliant produits industriels et services associés.

L'usage de l'internet des objets aurait néanmoins un effet incertain sur l'emploi industriel. Des optimisations dans la chaîne de production pourraient le dégrader, à l'image d'un fournisseur chinois d'Apple et de Samsung, qui a licencié, en 2016, des milliers d'employés, à la suite de l'usage combiné de robots et d'un système permettant d'identifier (ou « taguer ») les objets utilisés dans la chaîne de production. Inversement, le fabricant d'enceintes « haut de gamme » Devialet, a pu s'implanter en France et y créer des emplois, du fait de la forte automatisation de son usine.

Ainsi, ici comme ailleurs, les emplois nécessitant peu de qualifications risqueraient d'être les plus touchés tandis qu'un besoin accru de travailleurs dans le domaine des technologies de l'information et de la supervision des équipements industriels est attendu. De nombreuses entreprises, en particulier des PME installées en province, pourraient voir leur développement entravé par manque de personnel qualifié en France. La formation est donc cruciale, afin que les emplois générés par l'internet des objets puissent bénéficier aux travailleurs français.

Outre les disparités socio-professionnelles, l'internet des objets pourrait aussi creuser les effets de la fracture numérique et favoriser, économiquement parlant, les régions les mieux connectées. Aussi, sous cet angle comme sous les autres, il importe d'accompagner le développement du très haut débit sur l'ensemble du territoire. À cette condition, des solutions numériques connectées (e-santé, e-éducation, etc.) susceptibles de dynamiser l'emploi et l'économie pourront se développer dans les territoires plus isolés.

## B. ENJEUX ÉNERGÉTIQUES ET ÉCOLOGIQUES

### 1. Le paradoxe énergétique de l'internet des objets

Ainsi qu'il a été précédemment indiqué, certaines applications de l'internet des objets doivent permettre d'optimiser la consommation d'énergie et la gestion des ressources énergétiques et naturelles. **Tout d'abord, l'internet des objets doit favoriser l'émergence de services d'économie collaborative et donc de services de partage des ressources.** Ainsi, il est loisible d'imaginer partager un véhicule connecté, puisqu'il est géo-localisable et peut être ouvert à distance. On optimiserait ainsi la consommation d'essence de manière directe (covoiturage) ou indirecte (par un trafic plus fluide).

**En outre, l'utilisation généralisée de l'internet des objets doit permettre d'optimiser la gestion des réseaux de distribution de ressources** (électricité, eau, pétrole, gaz, etc.) et de détecter des problèmes d'acheminement, par exemple des fuites.

---

(1) Rapport d'information n° 4362 sur « Les objets connectés » présenté le 10 janvier 2017 par Mmes Corinne Erhel et Laure de La Raudière, députées, au nom de la commission des affaires économiques de l'Assemblée nationale.

(2) Le produit industriel est associé à une offre de services joints. Ces services vont permettre de différencier les produits et vont constituer la valeur ajoutée de la solution.



Sur ce point, le concept de réseau électrique intelligent – REI (*smart grid*) est particulièrement intéressant. Le principe du REI est de surveiller, de manière précise, l'état du réseau de distribution d'électricité (puissances consommées et transitées, courants, tensions, etc.) et l'état de fonctionnement des équipements (température des transformateurs de distribution, etc.).

Cette surveillance (*monitoring*) s'appuie sur l'usage de nombreux objets connectés tout le long du réseau, tels que des compteurs numériques « haute tension », des transformateurs connectés, des compteurs domestiques communicants (Linky pour la consommation d'électricité), voire des lignes électriques équipées de capteurs de température <sup>(1)</sup> connectés.

L'usage des technologies de l'internet des objets permet ainsi d'optimiser la production d'électricité en fonction de la demande (ce qui induit des économies d'énergie et un meilleur service), et aussi d'assurer une maintenance plus efficiente du matériel du réseau.

Au bout des REI, les bâtiments intelligents utiliseront, eux aussi, les objets connectés. Ils seront équipés d'éclairage intelligent, de systèmes de contrôle des flux d'air connectés, de thermostats intelligents, ou encore de prises connectées réduisant le gâchis d'électricité <sup>(2)</sup>.

**Ces avancées sont un enjeu majeur pour la France. Le secteur du bâtiment représente, en effet, plus de 45 % de la consommation d'énergie finale en France (40 % en moyenne dans l'Union européenne) et de l'ordre de 25 % des émissions de gaz à effet de serre.**

#### EXEMPLE : LE THERMOSTAT INTELLIGENT WEEN

Ween est un thermostat « intelligent » grand public. Pour réguler la température du logement dans lequel il est installé, Ween commande, à distance, un actionneur branché au système de chauffage. L'association de Ween et de son actionneur permet de réguler le chauffage du logement en fonction des préférences des membres du domicile <sup>(\*)</sup>, de la température ambiante, du temps nécessaire pour chauffer ou refroidir le domicile, des conditions météorologiques, etc. Selon les concepteurs de Ween, cet appareil permet d'économiser jusqu'à 25 % d'énergie.



Source : ween.fr.

<sup>(\*)</sup> Les préférences sont « apprises » par l'appareil grâce à des algorithmes d'intelligence artificielle permettant d'analyser les habitudes de chauffage.

(1) La surchauffe des câbles électriques et des transformateurs réduit leur durée de vie, d'où l'intérêt de contrôler leur température.

(2) Ces prises sont paramétrées par l'utilisateur (typiquement le gestionnaire du bâtiment) pour être désactivées en fonction de l'heure, de la détection de personnes dans la pièce et du type d'appareil connecté (ordinateur, lampe, etc.).

Pour autant, selon le rapport de l'Agence internationale de l'énergie (AIE) « *More Data Less Energy* » (« Plus de données, moins d'énergie »), la consommation annuelle en électricité de l'ensemble des appareils connectables <sup>(1)</sup> à l'échelle mondiale était de 420 TWh en 2008 (soit quasiment la consommation française en électricité, 480 TWh), dépassant 600 TWh en 2013. Selon ce même rapport, cette consommation devrait dépasser 1 100 TWh en 2025.

**Paradoxalement, certaines applications de l'internet des objets vont donc tendre à réduire la consommation énergétique (réseaux électriques intelligents, etc.), tandis que, à l'opposé, la consommation électrique due aux objets connectés et à leurs centres de données (*data centers*) devient de plus en plus conséquente.**

## **2. Les coûts environnementaux liés à la fabrication massive d'objets connectés**

De manière analogue au marché des terminaux de poche (*smartphones*), se pose la question de la durée de vie et de l'obsolescence programmée des objets connectés : certains objets connectés (en particulier ceux destinés au grand public) sont perçus comme des gadgets et ont une faible durée d'utilisation tandis que d'autres sont conçus sans système de mise à jour logicielle, ce qui pourrait nécessiter de les remplacer (en cas d'évolution du service, de problèmes de sécurité importants). Au vu de l'explosion attendue du nombre d'objets connectés, **les objets connectés pourraient donc être une source massive de déchets électroniques.**

Par ailleurs, comme dans tout appareil technologique, la conception d'objets connectés nécessite l'utilisation de « terres rares » <sup>(2)</sup>, dont les procédés d'extraction et de raffinage actuels ont des conséquences environnementales sévères (rejet d'éléments toxiques, de métaux lourds, d'acide sulfurique et d'éléments radioactifs). **La multiplication du nombre d'objets connectés pourrait donc amplifier la pollution due aux terres rares.**

## **C. ENJEUX DE SANTÉ PUBLIQUE**

### **• La télémédecine**

Dans le cadre de la télémédecine, sont apparues des « cabines de santé » permettant la téléconsultation et le bilan de santé. Ainsi, la *Consult Station* de la société française Health for Development (H4D) est équipée de plus de dix instruments de mesure connectés : tensiomètre, thermomètre, oxymètre (oxygène en circulation), dermatoscope, otoscope (conduit auditif), stéthoscope, balance et toise, électrocardiogramme, audiogramme tonal, tests visuels, etc. <sup>(3)</sup>.

---

(1) L'étude englobe, dans une acception très large, tous les objets pouvant être connectés sur un réseau, par exemple, les imprimantes.

(2) Voir le rapport (n° 3771 Assemblée nationale – n° 617 Sénat) sur « Les enjeux stratégiques des terres rares et des matières premières stratégiques et critiques » présenté en mai 2016 au nom de l'OPECST par M. Patrick Hetzel, député, et Mme Delphine Bataille, sénatrice.

(3) [https://www.h-4-d.com/la-consult-station/http://www.h-4-d.com/wp-content/uploads/2017/10/H4D\\_plaquette.pdf](https://www.h-4-d.com/la-consult-station/http://www.h-4-d.com/wp-content/uploads/2017/10/H4D_plaquette.pdf)



En cas d'absence du médecin traitant, la *Consult Station* permet de consulter un médecin dans des conditions comparables à une visite en cabinet classique. Les instruments de mesure présents dans la cabine et le dialogue qui s'opère *via* visioconférence permettent au médecin d'établir un diagnostic à distance. À la fin de la téléconsultation, le médecin peut, si besoin, délivrer une ordonnance. Elle sera directement imprimée dans la cabine.

La *Consult Station* permet également de réaliser des bilans de santé de façon autonome. L'utilisateur s'installe dans la cabine et suit les instructions s'affichant à l'écran : un tutoriel vidéo le guide et l'accompagne pour prendre ses mesures. Le bilan de santé est imprimé dans la cabine en deux exemplaires, un pour le patient et un pour le médecin traitant, s'il le souhaite.

## 1. L'« automesure connectée » (*quantified self*) à des fins de médecine prédictive

Dans le domaine de la santé, les objets connectés sont porteurs de nombreuses promesses : télémédecine, dépistage en « temps réel », amélioration de la prise en charge des patients, surveillance (*monitoring*) de la prise des traitements, etc. C'est pourquoi les objets connectés « grand public » les plus populaires sont les « *wearables* » dont l'argument de vente est d'améliorer notre santé, notre bien-être ou nos performances en :

– **traquant et interprétant des données physiologiques de leurs utilisateurs, en temps réel.** Ainsi, cette « automesure connectée » renseigne l'utilisateur sur ses performances physiques (par exemple le nombre de pas effectué dans la journée) ou sur des données concernant sa santé (par exemple son rythme cardiaque) ;

– **proposant une solution pour améliorer les performances ou les données de santé mesurées.** Ces solutions sont plus ou moins complexes, allant de la mise en place d'un programme personnalisé à la mise en place d'une action qui soulage, voire traite le problème (par exemple, le bandeau « *Dreem* » module l'activité cérébrale de son porteur à l'aide d'ondes sonores pour améliorer la qualité du sommeil profond de son utilisateur).

**Étant donné le caractère permanent de l'automesure connectée, l'objet connecté doit pouvoir faire entrer la médecine dans l'ère de la médecine prédictive.** Il n'est plus question d'aller chez le médecin seulement une fois malade, l'interprétation des données mesurées devant permettre d'anticiper ou de prendre en charge rapidement des problèmes de santé et, en parallèle, de réaliser d'importantes économies.

- **Vers l'humain connecté ?**

Très récemment, un « comprimé connecté » traitant la schizophrénie s'est vu accorder une autorisation de mise sur le marché (AMM) aux États-Unis. Au contact des sucs gastriques secrétés dans l'estomac du patient, la puce électronique logée dans le comprimé subit une réaction d'oxydo-réduction<sup>(1)</sup> donnant naissance à un courant électrique suffisant pour l'alimenter. La puce électronique émet alors un signal indiquant que le comprimé a bien été pris. Un patch collé sur les côtes du patient se charge ensuite de recevoir ce signal puis de le transmettre à une application du terminal de poche (*smartphone*) du patient. Via l'application, le patient décide alors qui de son médecin ou de ses proches aura accès à cette information.

Il s'agit là, peut-être, d'une première étape vers l'« humain connecté ». Si aujourd'hui prendre un médicament connecté induit une action éphémère sur le corps (toute trace du médicament étant éliminée), demain il est possible que nous soyons connectés de manière permanente, par exemple, via des implants-capteurs surveillant notre santé.

**Cette question de l'humain connecté appelle ainsi de nombreuses questions d'ordre éthique, juridique, d'employabilité, etc.**

## **D. ENJEUX SOCIAUX**

### **1. Comment anticiper l'acceptabilité des objets connectés ?**

**Anticiper l'acceptabilité sociale d'un objet connecté** est une question complexe, qui **suppose de considérer de multiples critères :**

- **le secteur d'utilisation et les applications permises par l'objet.** Du fait de leurs applications, les *wearables* de santé fascinent. Bien que très intrusifs, ils sont pourtant facilement acceptés par les consommateurs ;

- **le périmètre d'utilisation de l'objet.** Un RCSF de maintenance prédictive d'une installation industrielle concerne une unité collective et peut apparaître plus acceptable qu'un objet connecté utilisé dans le périmètre domestique ;

- **le caractère imposé ou volontaire de l'usage de l'objet connecté ;**

- **la nature de l'intrusion de l'objet connecté**, cette dernière pouvant être nominative, personnelle ou statistique ;

- **la nature de l'interaction de l'utilisateur avec l'objet connecté.** L'usage d'une montre connectée de suivi des performances sportives suppose une participation active de son utilisateur. Ce dernier consent donc, dans une certaine mesure, à la récolte de ses données.

**Au vu de sa complexité, l'anticipation de l'acceptabilité sociale des objets connectés utilisés dans le cadre de projets publics doit donc être idéalement menée dès la phase d'étude d'impacts de ces projets.** Par exemple, le compteur communicant Linky n'est pas accepté par une partie significative de la population française, qui se sent flouée. Pour le client, le bénéfice d'usage du compteur communicant Linky par rapport à un compteur classique n'est pas démontré, bien que son installation dans le périmètre domestique soit imposée. En outre, le compteur communique des données clients (donc nominatives), et

---

(1) La réaction d'oxydo-réduction est le principe de fonctionnement de base d'une pile électrique.

ce, de manière totalement passive, sans aucune action possible de la part du consommateur. Ces raisons, parmi d'autres <sup>(1)</sup>, expliquent les « frondes anti-Linky » et les retards de déploiement.

## 2. Les objets connectés sont-ils créateurs de liberté ou de contrainte ?

Dans une certaine mesure, les objets connectés sont créateurs de liberté. Par exemple, les données collectées par les REI – et plus généralement par les infrastructures similaires de production et de traitement de données – pourraient **favoriser l'autonomisation (*empowerment*)** des clients du réseau s'il était décidé que ces données leur soient remises afin qu'ils puissent optimiser leur consommation d'électricité (ce qui pourrait favoriser l'acceptabilité de ces REI).

Les objets connectés peuvent aussi être créateurs de contraintes. Les *wearables*, par exemple, doivent permettre d'améliorer notre santé, de mettre en relation patients et médecins à distance, etc. Pour autant, il est légitime de se poser la question de la fiabilité des diagnostics proposés par ces objets connectés. Ai-je correctement utilisé l'objet connecté ? Quelle confiance puis-je avoir dans les mesures et avec quelle marge d'erreur ? Les données mesurées par l'objet connecté sont-elles celles qui sont les plus pertinentes au regard de ma situation de santé personnelle ? Un manque de recul sur ces diagnostics peut donc inciter l'utilisateur à :

– avoir un excès de confiance en lui et donc sous-estimer ses problèmes de santé (ou réciproquement accroître ses préoccupations et donc surestimer ses problèmes de santé) ;

– se conformer à une norme non nécessairement adaptée à sa condition ou non pertinente. Les podomètres connectés incitent leurs utilisateurs à faire « 10 000 pas par jour », malgré le fait qu'aucune étude scientifique n'en atteste le bienfait.

## 3. Les objets connectés sont-ils créateurs de lien social ou d'inégalités ?

Selon le professeur Christian Liccope, la mise en place de réseaux d'objets connectés et l'exploitation des données qu'ils collectent peut ouvrir des possibilités nouvelles de régulation de questions sociales de grande ampleur (pollution due aux transports, embouteillages, etc.) engageant différentes formes de solidarité et de responsabilité du corps social.

Réciproquement, l'usage des objets connectés peut aussi être générateur d'exclusion car il accentue la fracture numérique de « second degré » (les personnes âgées, par exemple, ayant parfois plus de difficultés à utiliser les nouvelles technologies).

## 4. La question de la protection des données personnelles

Comme avec les applications de nos terminaux de poche (*smartphones*), les objets connectés « grands publics » produisent des données qui se rapportent à des personnes physiques identifiées (ou identifiables), donc des données personnelles.

---

(1) Voir les tables rondes sur « les enjeux des compteurs communicants » conjointement organisées, le 14 décembre 2017, par l'OPECST et la commission des affaires économiques. - Rapport n° 672 du 15 février 2018 de l'OPECST sur les enjeux des compteurs communicants.

Ces objets sont souvent conçus pour être des technologies améliorant le quotidien de l'utilisateur en s'intégrant naturellement dans le cadre de vie de celui-ci et en limitant au maximum l'interaction avec lui (l'objet connecté devant essayer de prévoir les besoins de l'utilisateur).

Du fait de cette facilité d'utilisation, les possesseurs d'objets connectés ne sont pas nécessairement conscients de la quantité de données qu'ils génèrent et des risques auxquels ils s'exposent <sup>(1)</sup>. Ils n'ont, en effet, pas toujours connaissance du destinataire avec qui ils partagent leurs données (qui peut exercer dans un pays où les garanties quant aux traitements des données personnelles sont moins rigoureuses que celles prévalant dans l'Union européenne), de l'usage ultérieur que le destinataire peut faire de ces données et des conséquences pour leur vie privée – voire leur liberté individuelle. En outre, l'utilisateur s'expose à un risque évident de piratage informatique de ses données personnelles.

La loi française protège néanmoins les citoyens des dérives liées à l'exploitation de leurs données personnelles. Par exemple, les assureurs peuvent légalement utiliser des données de santé volontairement transmises par leurs clients afin de leur proposer des bonus. Ainsi, en 2014, Axa offrait des chèques-cadeaux aux utilisateurs consentants dont le podomètre connecté Withings enregistrait un nombre minimum de pas par jour. En France, le code de la sécurité sociale permet ainsi aux assureurs de développer des programmes de prévention sur la base du volontariat. Néanmoins, et contrairement à une idée largement répandue, les codes français de la mutualité et des assurances interdisent aux assureurs de moduler leur tarification par des malus en fonction de la santé des personnes. Ces malus seraient contraires au principe de mutualisation des risques. La seule exception concerne les assurances liées aux prêts immobiliers.

Sur ce sujet sensible de la protection des données personnelles, le nouveau règlement général sur la protection des données (RGPD), qui entrera en vigueur le 25 mai 2018, apporte des améliorations significatives. Celles-ci sont présentées en annexe.

## 5. Comment les objets connectés sont-ils perçus par les français ?

**Selon un sondage <sup>(2)</sup> réalisé par OpinionWay en mars 2017, les enjeux des objets connectés « grand public » semblent être de mieux en mieux perçus.** Les principaux avantages des objets connectés identifiés par les français sondés sont la « possibilité d'être alerté en temps réel en cas d'urgence » (fuite d'eau, proche malade, etc.), la « surveillance du logement à distance », le contrôle de la consommation d'énergie, l'amélioration de la sécurité routière, ou encore la possibilité de mieux suivre son état de santé. Ainsi, l'équipement des français en termes d'objets connectés progresse.

Néanmoins, 46 %, des sondés estiment que les coûts des objets connectés sont trop élevés et une partie significative du panel d'OpinionWay <sup>(3)</sup> considère que l'offre des constructeurs n'est pas satisfaisante. En outre, de plus en plus de français prennent conscience des risques liés à l'usage des objets connectés : en 2017, 42 % des sondés se déclaraient inquiétés par la récolte de leurs données personnelles contre 33% en 2016.

---

(1) Les Français sont néanmoins de plus en plus conscients de ces risques (cf. infra).

(2) <https://www.opinion-way.com/fr/sondage-d-opinion/sondages-publies/marketing/opinionway-pour-distreeconnect-2017-les-francais-et-les-objets-econnectes-mars-2017.html> .

(3) Seulement 53 % des sondés de l'étude d'opinionway considèrent que l'offre des fabricants d'objets connectés est satisfaisante.

**L'ÉQUIPEMENT DES FRANÇAIS EN OBJETS CONNECTÉS SELON OPINIONWAY  
(1070 SONDÉS, MARGE D'INCERTITUDE ENTRE 2 ET 3 %)**

Objet connecté	Français équipés en 2016	Français équipés en 2017
Télévision connectée	22%	29%
Dispositif de sécurité connecté	5%	12%
Bracelet sportif connecté		12%
Montre connectée	6%	11%
Détecteur de fumée connecté		11%
Véhicule connecté		10%
Station météo connectée		7%
Prise ou interrupteur connectés		6%
Thermostat connecté		5%
Porte-clés connecté		4%
Balance connectée		4%
Ampoule connectée		3%
Brosse à dents connectée		3%
Drone connecté		2%
Tensiomètre connecté		2%
Clé connectée		2%
Pot de fleur connecté		1%

### **III. LES DÉFIS TECHNOLOGIQUES POSÉS PAR LES OBJETS CONNECTÉS DEVRONT ÊTRE RELEVÉS**

L'informatique et l'internet ont profondément modifié notre société. Pourtant, certains décideurs politiques contemporains ont manqué de clairvoyance sur ces sujets à l'occasion de l'essor de ces technologies. Ainsi, en 1997, était décidée la suppression de l'informatique dans l'enseignement français, au moment même de l'explosion d'internet. De manière analogue, et qu'on le veuille ou non, l'internet des objets va lui aussi transformer notre société et bouleverser nombre de secteurs économiques. Ainsi, la France ne doit pas, cette fois-ci, rester en marge de ce mouvement mais doit prendre part à la résolution des défis technologiques posés par l'internet des objets.

#### **A. DÉFI SUR L'AUTONOMIE DES OBJETS CONNECTÉS**

La baisse des coûts de l'électronique et les progrès techniques facilitent l'émergence de l'internet des objets. Néanmoins, une des contraintes les plus critiques lors de la conception d'un objet connecté demeure la gestion de l'énergie, ce que notait déjà l'ANFR en 2014 : « *La contrainte liée à l'autonomie des batteries concernera 80 % de ces objets [connectés]* »<sup>(1)</sup>.

Certaines applications nécessitent, en effet, que des objets connectés travaillent de manière autonome pendant plusieurs mois sans aucune intervention humaine. Par exemple, certains RCSF ont été conçus pour surveiller les fuites de pétrole dans les oléoducs, ce qui nécessite la mise en place de capteurs difficilement accessibles et donc rarement (si ce n'est jamais) rechargeables.

En outre, la conception des objets connectés suit des contraintes de dimensionnement. On se doute que les capteurs d'un RCSF de maintenance prédictive d'un réseau ferroviaire doivent être suffisamment compacts pour pouvoir être insérés sur les rails sans gêner le

---

(1) Conférence « Les fréquences au service de l'individu » – Paris, jeudi 27 novembre 2014.

passage des trains. De même, les objets connectés grands publics sont souvent très ergonomiques, portables et discrets. Il y a donc un compromis à trouver entre compacité et énergie : moins d'espace disponible suppose d'embarquer des batteries moins importantes.

**La R&D est donc essentielle en ce qui concerne les techniques et technologies de production, de stockage et de gestion de l'énergie dans les systèmes embarqués. La France pourrait donc particulièrement encourager la recherche dans différents domaines tels que les batteries, « la gestion dynamique de l'énergie »<sup>(1)</sup>, les systèmes de « récolte d'énergie », les protocoles de communication « basse consommation » ou encore les nanomatériaux<sup>(2)</sup>.**

#### EXEMPLE : LES INTERRUPTEURS SANS FIL NI BATTERIE DE ENOCEAN

La société EnOcean commercialise des objets connectés de domotique ne nécessitant aucune batterie. En particulier, les interrupteurs connectés d'EnOcean n'ont pas de piles. Ils ont été conçus pour « récolter » suffisamment d'énergie lors de l'appui sur le bouton de l'interrupteur pour pouvoir envoyer le signal de commande (« allumer » ou « éteindre ») à l'actionneur associé à cet interrupteur (par exemple une lampe).

## B. DÉFI SUR L'UTILISATION DU SPECTRE DES FRÉQUENCES

Le spectre hertzien est l'ensemble des fréquences sur lequel les systèmes de radiocommunications peuvent opérer.

Ce spectre, aujourd'hui largement saturé, est partagé et régulé de manière à éviter, au mieux, que les ondes radioélectriques des différents systèmes interfèrent et se brouillent. Ce partage se fait selon des contraintes géographique, temporelle (durée d'émission, périodicité des émissions, etc.), de puissance (puissance maximale rayonnée par les antennes des systèmes) et sur une base fréquentielle. Certaines bandes de fréquences sont réservées aux usages militaires, d'autres sont soumises à des licences coûteuses<sup>(3)</sup> tandis que certaines ne sont pas licenciées<sup>(4)</sup>. Ces bandes non licenciées sont utilisées pour des applications industrielles, scientifiques, médicales (d'où leur nom de bandes « ISM ») et aussi domestiques. Par exemple, les protocoles de communication Bluetooth et Wifi fonctionnent sur certaines bandes ISM et partagent les mêmes fréquences (autour de 2,4 GHz).

Des stratégies technologiques existent déjà pour partager au mieux ce spectre (émission sur des portions de spectre très étroites<sup>(5)</sup>, maillage du réseau en « petites cellules »<sup>(6)</sup> pour la 5G, etc.) et d'autres se développent. Par exemple, certaines recherches prometteuses propres au domaine de la « radio cognitive » portent sur l'accès opportuniste,

---

(1) Technique qui permet d'économiser de l'énergie en jouant contextuellement sur l'état d'éveil et la performance des différents composants matériels de l'objet connecté.

(2) Les nanomatériaux permettent de réaliser des capteurs de plus en plus efficaces, plus compacts et plus économes en énergie.

(3) Par exemple, SFR a dû déboursier plus d'un milliard d'euros pour obtenir la licence d'utilisation, en France, des bandes 801-811MHz et 842-852 MHz utilisées pour la « 4G ».

(4) Plus exactement, le régime d'autorisation général fixe les conditions d'accès à ces bandes.

(5) « Ultra Narrow Band », technologie utilisée, par exemple, par l'opérateur français Sigfox.

(6) L'emploi de petites cellules « small cells », c'est-à-dire d'antennes « basse consommation » et « faible portée », doit permettre de densifier le réseau d'antennes (donc de limiter le nombre d'utilisateurs connectés à chaque antenne) et d'améliorer la gestion de l'énergie (en adaptant les puissances d'émission en fonction du besoin).



par des objets connectés, à des bandes de fréquences temporairement sous-utilisées et éventuellement licenciées (l'idée sous-jacente étant, en temps réel, d'exploiter au mieux le spectre disponible sans déranger les utilisateurs existants). Ces évolutions futures, nécessiteront des études de faisabilité et, le cas échéant, la mise en place de nouvelles réglementations.

**Ainsi, la gestion du spectre et les dispositions légales encadrant celle-ci constituent des éléments clés du développement des objets connectés, à l'heure de l'explosion prévisible de leur nombre.**

### **C. DÉFI SUR LA SÉCURITÉ INFORMATIQUE**

Avec l'internet des objets, l'exploitation de lacunes de sécurité peut nuire d'une manière nouvelle, les attaques informatiques pouvant avoir un impact sérieux sur le monde réel ; fréquemment, des chercheurs en sécurité informatique ont ainsi été capables de prendre le contrôle à distance de certains modèles de voitures connectées.

En plus d'être des cibles, les objets connectés peuvent être utilisés pour participer à des attaques d'autres systèmes d'information. Ainsi en septembre 2016, l'hébergeur de site français OVH a été frappé pendant cinq jours par une attaque « *DDOS* »<sup>(1)</sup> massive impliquant 145 607 caméras connectées piratées. Ce type d'attaque risque de se répéter ; les chercheurs en sécurité des sociétés Qihoo 360 et Check Point ont constaté, en septembre 2017, l'infection par des pirates de plus d'un million d'appareils connectés, principalement des caméras IP, des routeurs et des NAS<sup>(2)</sup>.

La réglementation européenne incite ainsi les concepteurs d'objets connectés à commercialiser des objets sécurisés, ne collectant et ne transmettant que des données strictement nécessaires à l'usage.

**Pour autant, les standards et les pratiques de conception assurant la sécurité informatique des technologies de l'internet des objets sont toujours en cours de développement et ne sont pas encore généralisés. Les défauts de sécurisation des réseaux d'objets connectés sont pourtant des risques majeurs liés à l'usage de l'internet des objets et une attention particulière doit y être prêtée par les pouvoirs publics.**

## **IV. CONCLUSIONS ET RECOMMANDATIONS**

### **Activité économique :**

– Constater la forte croissance de l'internet des objets dans un grand nombre de secteurs économiques et partout dans le monde ;

– Se féliciter des potentialités considérables de l'internet des objets pour un grand nombre de domaines d'applications, par exemple en maintenance industrielle, logement, transports, énergie, gestion de l'espace publique, agriculture, logistique, santé humaine ou encore objets grand publics (*wearables*) ;

---

(1) Une attaque *DDOS* – « Distributed Denial of Service » – ou « attaque par déni de service » vise à rendre un serveur indisponible en surchargeant la bande passante du serveur, ou en accaparant ses ressources jusqu'à épuisement.

(2) Un *NAS* – « Network Attached Storage » – est un serveur de fichiers sur réseau.

– Souhaiter le développement de politiques de filière à l'échelle nationale et européenne ;

– Souhaiter le développement du très haut débit sur l'ensemble du territoire, afin que les territoires les moins bien connectés actuellement puissent profiter des avantages liés aux objets connectés.

**Recherche :**

– Encourager la recherche dans des domaines liés à l'internet des objets, par exemple sur les batteries, la gestion dynamique de l'énergie, les systèmes de « récolte d'énergie », les protocoles de communication « basse consommation » ou encore les nanomatériaux.

**Éthique :**

– Sensibiliser les particuliers aux risques liés à l'usage des objets connectés (protection des données personnelles et de la vie privée).

**Sécurité informatique :**

– Élaborer des normes de conception en matière de sécurité informatique (défaillance technique ou cybercriminalité).

**Environnement :**

– Interroger ou auditionner l'Union internationale des télécommunications (UIT) sur la question du traitement des déchets électroniques.

**Utilisation du spectre :**

– Demander à l'Agence nationale des fréquences (ANFR) et à l'Autorité de régulation des communications électroniques et des postes (ARCEP) d'envisager les évolutions possibles de la réglementation du spectre, du fait de l'internet des objets.

## ANNEXE

### LÉGISLATION RELATIVE AU TRAITEMENT DES DONNÉES PERSONNELLES PRODUITES PAR LES OBJETS CONNECTÉS

La protection des données personnelles est un souci majeur résultant de l'utilisation d'objets connectés. Le nouveau **règlement européen sur la protection des données (RGPD)** reconnaît de nouveaux droits aux individus vis-à-vis de leurs données personnelles et responsabilise les responsables de traitement, tout en renforçant considérablement le champ d'action et de sanction des autorités de contrôle <sup>(1)</sup>. Le nouveau RGPD répond au besoin de maîtrise des données par les personnes qui les génèrent et doit permettre de répondre aux questions suivantes : quelles données sont collectées ? Pour quoi faire ? Qui collecte les données ? Qui est responsable des données ? Auprès de qui faire valoir ses droits ? En réponse, une information claire et complète doit être fournie aux utilisateurs.

Ce règlement doit entrer en vigueur le 25 mai 2018. S'il est d'application directe en droit national, il prévoit toutefois des marges de manœuvre pour les États membres qui souhaiteraient renforcer certaines de ses dispositions. En France, un projet de loi relatif à la protection des données personnelles est ainsi en cours d'examen par le Parlement <sup>(2)</sup>. Adopté en première lecture à l'Assemblée nationale, il prévoit entre autres une mise à jour importante de la loi « Informatique et Libertés » (LIL) <sup>(3)</sup> et adapte le fonctionnement de la Commission nationale de l'informatique et des libertés (CNIL) à l'évolution de son champ d'action résultant des dispositions du RGPD.

Tous les traitements informatiques de données produites par les objets connectés ne tombent pas dans le champ de la LIL. Les données doivent en effet avoir un caractère personnel, c'est-à-dire être relatives à une personne identifiée ou pouvant être identifiée (ce qui peut inclure des données de géolocalisation). Sont cependant exclus les traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles, c'est-à-dire en l'absence de diffusion à un tiers <sup>(4)</sup>.

Il est toujours possible de déroger aux règles applicables si la personne concernée exprime son consentement, de manière « explicite » et « positive » <sup>(5)</sup>. La sensibilisation des citoyens à leur responsabilité dans la protection de leurs données personnelles reste donc primordiale.

Le projet de loi relatif à la protection des données personnelles prévoit le passage d'un régime d'autorisation et de déclaration *a priori* à un régime de contrôle *a posteriori*. Les responsables de traitements sont appelés envisager la protection de la vie privée dès la conception d'un objet connecté en respectant les principes de proportionnalité, de finalité, de respect des droits des personnes, de limitation dans le temps, de sécurité et d'intégrité des données (« *privacy by design* ») <sup>(6)</sup>.

---

(1) Règlement (UE) (n° 2016/679) du 27 avril 2016 du Parlement européen et du Conseil portant règlement général sur la protection des données.

(2) [Projet de loi](http://www.assemblee-nationale.fr/15/dossiers/donnees_personnelles_protection.asp) (AN n° 490) du 13 décembre 2017 relatif à la protection des données personnelles : [http://www.assemblee-nationale.fr/15/dossiers/donnees\\_personnelles\\_protection.asp](http://www.assemblee-nationale.fr/15/dossiers/donnees_personnelles_protection.asp)

(3) Loi (n° 78-17) du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(4) Article 2 de la LIL.

(5) Article 51 du RGPD.

(6) Article 5 du RGPD.

Afin de s'en assurer, les entreprises les plus impliquées dans le traitement de données personnelles devront obligatoirement nommer un délégué à la protection des données <sup>(1)</sup>, interlocuteur privilégié des autorités de contrôle. Lorsque les opérations de traitement seront susceptibles d'engendrer un risque élevé pour les droits et libertés, elles devront faire l'objet d'études d'impact préalables, conduisant éventuellement à une demande d'autorisation <sup>(2)</sup>.

De leur côté, les personnes concernées se voient reconnaître de nouveaux droits vis-à-vis de leurs données, en particulier le droit à l'effacement <sup>(3)</sup> et à la portabilité <sup>(4)</sup>, qui s'ajoutent à ceux existant, notamment les droits à l'opposition <sup>(5)</sup>, à l'information <sup>(6)</sup> ou à la rectification <sup>(7)</sup>.

La principale inquiétude vis-à-vis des objets connectés tient toutefois au fait qu'ils sont produits ou exploités par des entreprises non européennes, en particulier américaines. À ce titre, le RGPD prévoit que ses dispositions sont opposables aux entreprises extra-européenne si elles ciblent des résidents européens ou leurs proposent des biens et services <sup>(8)</sup>.

Au sein même de l'Union européenne, une autre inquiétude tient au risque qu'une entreprise choisisse de s'installer dans un État afin de profiter d'une réglementation plus souple sur la protection des données (« *forum shopping* »). Pour y répondre, le règlement européen harmonise le cadre communautaire et le « G29 », qui regroupe les autorités nationales de protection des données, a défini des règles communes et des modalités d'arbitrage. Enfin le projet de loi prévoit l'application de la réglementation nationale lorsque la personne concernée réside en France, y compris lorsque le responsable du traitement est établi hors de France <sup>(9)</sup>. En contrepartie de la suppression des régimes d'autorisation préalable, les sanctions ont été considérablement renforcées. Les amendes administratives applicables par les autorités de contrôle voient ainsi leur plafond considérablement augmenter, pouvant atteindre en cas de récidive jusqu'à 4 % du chiffre d'affaire mondial total et 20 millions d'euros <sup>(10)</sup>.

Par ailleurs, le Conseil et le Parlement européens examinent actuellement une proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques <sup>(11)</sup>, aussi appelé « **règlement ePrivacy** », qui doit mettre à jour les principes de la directive 2002/58/CE. Elle constitue une *lex specialis* par rapport au RGPD, qu'elle vient préciser et compléter concernant les données de communication électronique.

---

(1) Article 37 du RGPD.

(2) Article 35 du RGPD.

(3) Article 17 du RGPD.

(4) Article 20 du RGPD.

(5) Article 38 de la LIL.

(6) Article 39 de la LIL.

(7) Article 40 de la LIL.

(8) Article 3 du RGPD.

(9) Article 8 du projet de loi sur la protection des données personnelles.

(10) Article 83(6) du RGPD ; Article 5(7) du projet de loi relatif à la protection des données personnelles.

<sup>11</sup> Proposition de règlement (COM/2017/010 final) du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « *vie privée et communications électroniques* »).

Elle aura aussi un impact sur la protection des données personnelles traitées par les objets connectés. En effet, d'une part, elle prévoit d'élargir le champ du principe de confidentialité des communications au-delà des seuls opérateurs directs de réseaux (fournisseurs d'accès à internet ou au téléphone), pour l'étendre aux services *dits* « *over the top* », qui utilisent ces réseaux (Messenger, Snapchat, Whatsapp, etc.). D'autre part, elle veut renforcer et harmoniser les mécanismes d'expression du consentement à la collecte et à l'utilisation de données, pour passer d'une logique « *opt-out* » (consentement présumé sauf mention contraire de l'utilisateur) à une logique « *opt-in* » (absence de consentement présumée jusqu'à autorisation expresse de l'utilisateur).

Le 12<sup>e</sup> considérant de la proposition de règlement *ePrivacy* mentionne explicitement les données échangées par l'internet des objets, y compris dans les interactions de machines à machines. Cette évolution réglementaire est perçue assez négativement par certaines entreprises du secteur, qui regrettent un champ d'application trop large ou mal défini.

Une dernière interrogation persiste concernant les produits s'appuyant sur la technologie des **chaînes de blocs** (*blockchain*), qui pourraient être appelés à se développer et à couvrir les objets connectés. Une des caractéristiques majeures de cette innovation réside en effet dans l'incorruptibilité des données stockées, ce qui dans le cas de données personnelles apparaît comme incompatible avec le respect des droits des personnes concernées, en particulier les droits à la rectification et à l'effacement. Il serait souhaitable que les données échangées par les objets connectés avec un tel protocole ne permettent pas d'identifier des personnes, notamment grâce à l'utilisation de divers procédés cryptographiques.