Enjeux numériques

Des objets connectés aux objets communicants

UNE SÉRIE DES
ANNALES DES MINES
FONDÉES EN 1794

N° 16 - DÉCEMBRE 2021

Publiées avec le soutien de l'Institut MinesTélécom

UNE SÉRIE DES
ANNALES DES MINES
FONDÉES EN 1794

ENJEUX NUMÉRIQUES

Série trimestrielle • N°16 - Décembre 2021

Mise en page : Nadine Namer
Impression : EspaceGrafic
N° ISSN 2781-1263
Éditeur délégué
FFE – 15, rue des Sablons - 75116 PARIS
www.ffe.fr

Régie publicitaire : Belvédère Com
Fabrication : Yaël Sibony
Yaël.Sibony@belvederecom.fr
Tél. : 01 53 36 20 46
Directeur de la publicité : Bruno Slama
Tél. : 01 40 09 66 17
bruno.slama@belvederecom.fr

Le sigle « D. R. » en regard de certaines illustrations correspond à des documents ou photographies pour lesquels nos recherches d'ayants droit ou d'héritiers se sont avérées infructueuses.

Des objets connectés aux objets communicants

L'Internet des objets personnels : un oxymore ?

Ce numéro a été coordonné par Anne-Lise THOUROUDE

Introduction
Des objets connectés aux objets communicants

Par **Anne-Lise THOUROUDE**
Arcep

Les objets connectés, communicants, augmentés, font rêver depuis de nombreuses années. On a longtemps annoncé « la révolution » qu'allait entrainer dans leur sillage tous ces objets. Si leur nombre ne cesse d'augmenter et leurs usages de se développer, si les objets communicants n'ont de cesse d'envahir notre quotidien, peut-on réellement parler de révolution ?

La première difficulté rencontrée pour ce numéro est de poser des définitions. En effet, de nombreux concepts interfèrent et se contredisent, on parle indifféremment dans la presse d'objets connectés, de l'Internet des objets, d'interconnections d'objets, d'objets communicants, de bâtiment intelligent, de "*smart city*", etc.

Nous avons choisi volontairement pour ce numéro de ne pas donner de définition, *a priori* afin de recueillir des avis avec un spectre le plus large possible, mais également de souligner une évolution dans ces différents concepts : des objets connectés aux objets communicants. Si l'imaginaire porte aux objets connectés d'être de « simples » capteurs, l'« intelligence » de ces objets est de plus en plus présente dans la littérature, les objets devenant ainsi non seulement connectés mais communicants.

Ainsi, la valeur intrinsèque des objets communicants serait-elle non pas dans les objets eux-mêmes mais dans le fait qu'ils communiquent, créant ainsi une chaine de valeur ? En effet, pour que la valeur puisse être créée, il faut non seulement connecter les objets mais en collecter les données, les transporter, les analyser puis les valoriser et les partager. C'est de cet ensemble complet que naissent les applications concrètes et des bénéfices économiques ou sociétaux, autrement dit une création de valeur. La valeur des objets communicants s'articulerait alors autour de trois grands volets : les objets eux-mêmes, la connectivité, et enfin les données et leur traitement.

La connectivité, c'est-à-dire les réseaux et leurs équipements, est une couche avancée de cette chaine de valeur. Cette connectivité s'organise autour d'une multitude de réseaux, fixes ou mobiles, 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. Par ailleurs, la connectivité est d'ores et déjà présente dans le quotidien des utilisateurs qui disposent d'interfaces pour interagir avec de multiples objets, le *smartphone* étant un des exemples criants.

La couche des objets, quant à elle, est toujours en mutation. D'un côté, les évolutions technologiques de ces dernières années ont rendu les capteurs plus performants, moins consommateurs d'énergie et accessibles à des prix réduits. D'un autre côté, des solutions techniques restent encore à concevoir pour répondre à des besoins plus complexes, exigeant souvent de meilleurs débits ou une qualité de service supérieure, comme le véhicule connecté ou certains usages industriels critiques.

Dans ce contexte, 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.

Concernant la couche de valorisation de la donnée, elle peut s'effectuer à deux niveaux : d'abord, auprès de chaque utilisateur pour une collecte et une exploitation propre 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. De fait, 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.

Enfin, si comme nous l'avons vu la chaine de valeur des objets communicants commence à se dessiner, si des acteurs majeurs commencent à émerger, ces objets communicants suscitent également une certaine réserve de la part du grand public.

Finalement, pourquoi connectons-nous les objets ? Si la révolution annoncée n'a jamais réellement eu lieu, le changement est-il en cours ? Avons-nous besoin de ces objets ? Sommes-nous réellement en capacité de traiter toutes les données qu'ils communiquent ? Ces données peuvent-elles nous échapper ? La productivité est-elle réellement améliorée par la multiplication des objets communicants ? Le livre interactif est-il facilitateur des apprentissages ou au contraire efface-t-il la réflexion personnelle ? Peut-on perdre le contrôle de nos systèmes ? Devons-nous foncer tête baissée dans ce monde hyperconnecté où même nos frigos doivent l'être ? Jusqu'où irons-nous dans cette société où l'information en temps réel est devenue le Graal ?

Ce numéro n'a pas la prétention de répondre à toutes ces questions, mais l'ambition de montrer le point de vue et la vision des différentes parties prenantes dans la création de valeur(s) des objets connectés, et ainsi d'ouvrir quelques portes pour éclairer le lecteur sur les évolutions des objets communicants.

La première et la deuxième partie de ce numéro vont illustrer les usages et technologies extrêmement variés qui rendent possibles les objets communicants.

Tandis que la dernière partie ouvrira la réflexion sur les enjeux sociétaux qu'ils posent.

Très bonne lecture !

L'imaginaire de l'Internet des objets

Par **Pierre MUSSO**
Professeur à l'Université de Rennes 2 et associé à Télécom Paris

Aborder l'imaginaire de l'IoT (*Internet of Things* ou Internet des objets) soulève au moins deux difficultés : la première est de définir ce qu'est l'Internet des objets (ou des choses), qui se présente comme une nébuleuse, un « fourre-tout » ou ce qu'il faut appeler un « objet-valise », et la seconde est de préciser ce qu'est l'imaginaire, généralement confondu avec l'imagination et opposé au réel et au rationnel.

Pour définir l'IoT, on peut se référer à l'UIT (Union internationale des télécommunications) qui, en juin 2012 dans une recommandation intitulée *Présentation générale de l'Internet des objets*, dit qu'il s'agit d'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 ». Considéré comme la troisième évolution de l'Internet, l'IoT interconnecte des objets entre eux à l'échelle planétaire, et non des personnes entre elles. La définition de l'IoT demeure assez floue et ouverte : « réseau de réseaux », « système de systèmes », « nébuleuse » sont des formules qui cherchent à le cerner, car ce n'est pas une « technologie » de plus, mais un ensemble hétéroclite d'objets « technologisés ». La première représentation de l'IoT est donc son caractère indéterminé : c'est un champ sans limites, ni bornes, ni frontières : foisonnant et viral. Ainsi l'IoT a-t-il pu être qualifié de « révolution sans limites ». Il vise la totalité, voire, pour certains, une forme de totalitarisme tant il sera omniprésent et omnipotent. On peut dire qu'il recoupe trois composantes : des objets (*things*), des réseaux (*networks*) et des données (*data*).

Quant à la définition de l'imaginaire, catégorie essentielle en philosophie et en sociologie, il faut le différencier de l'imagination qui est une faculté psychologique individuelle. L'imaginaire est un ensemble structuré de représentations sociales dans des archétypes, des mythes, des images populaires ou de grands récits qu'un groupe ou une société se donne pour se définir et se raconter. Pour souligner l'importance de l'imaginaire comme phénomène social, voire anthropologique, le philosophe Cornelius Castoriadis affirmait que : « Il est impossible de comprendre ce qu'a été, ce qu'est l'histoire humaine, en dehors de la catégorie de l'imaginaire ».

Dans le discours ordinaire, « imaginaire » signifie le contraire du « réel » et devient rapidement synonyme de « chimérique ». Précisons immédiatement que l'imaginaire n'est pas le contraire du réel et du rationnel comme on le dit trop vite, mais bien leur complément. Le même Castoriadis dit que l'imaginaire n'est pas « la négation du réel » mais une « a-réalité » qui permet « de faire exister le possible », et le sociologue Gilbert Simondon affirme que l'imaginaire est « un second réel ».

De fait, l'imaginaire, comme le rêve, a une rationalité propre qui ne respecte pas le principe de non-contradiction de la logique aristotélicienne : par exemple, il est toujours ambivalent (dire le paradis, c'est dire aussi l'enfer). L'imaginaire est un langage dont on peut déceler la « grammaire » : a-logique, il dispose de ses propres structures ordonnées selon des schèmes et des archétypes. On peut dire que l'imaginaire est un langage composite fait de textes ou narrations, d'images possédant une dimension émotionnelle, un langage dynamique ayant une certaine cohérence et délivrant du sens.

Le philosophe Paul Ricoeur a montré que l'action est investie par un imaginaire qui la légitime ou l'oriente. L'imaginaire ne se dissocie pas de la pratique. Pas d'action humaine qui ne soit précédée

ou accompagnée de représentations. Étant donné que l'imaginaire se concrétise dans des objets, il est possible réciproquement de décrypter des imaginaires dans les objets techniques.

En effet, on peut lire dans n'importe quel objet (ou famille d'objets) technique(s) des fonctions potentielles et des fictions réalisées : si la fonctionnalité d'une technique ce sont ses usages, sa fictionnalité, ce sont ses représentations. C'est pourquoi le sociologue et anthropologue Georges Balandier a préféré parler de « techno-imaginaire » [(1)] plutôt que de technique. Ce « techno-imaginaire » – terme que nous retenons – prend le plus souvent la forme d'une ambivalence entre le « techno-messianisme », annonciateur de mille promesses, et le « techno-catastrophisme », prophète de menaces et de dangers. Cette ambivalence délimite à un moment donné l'espace des imaginaires possibles qui peut tourner au conflit de visions du monde.

Précisons que critiquer les « techno-imaginaires », ce n'est pas critiquer les techniques, mais bien au contraire les enrichir par l'analyse des fictions qui les accompagnent dès leur conception, dans leurs développements et leur diffusion. L'historien des techniques Bertrand Gille a bien souligné que les systèmes techniques sont indissociablement des phénomènes culturels et techniques.

Dans les limites de cet article, on se propose d'examiner d'abord l'ensemble du grand « techno-récit » de l'IoT, et, ensuite, de préciser les imaginaires associés à ses trois principales composantes : objets/réseaux/données.

Le méta-récit de l'IoT

L'IoT n'échappe pas à la loi de l'ambivalence de l'imaginaire, c'est-à-dire à un dualisme fondateur : d'un côté, des promesses d'hyperconnexion et de communication généralisées entre objets ou entre objets et êtres vivants grâce à des objets producteurs de données préfigurant une société automate censée libérer les individus, et, de l'autre, les menaces de contrôle continu et de la surveillance de masse inquiétante du fait de la captation des données personnelles.

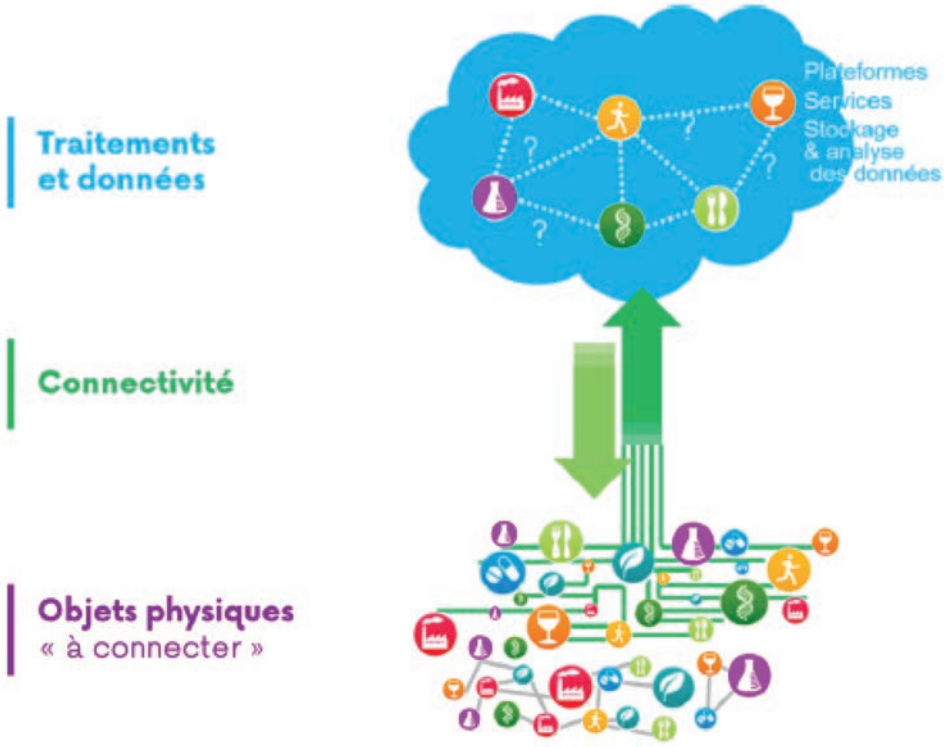
Dès 2005, l'UIT reprenait la promesse récurrente de toute innovation technologique, annonçant dans son rapport "The Internet of Things" que « l'avènement de l'Internet des objets créera une pléthore d'applications et de services innovants, qui amélioreront la qualité de la vie et réduiront les inégalités, tout en ouvrant de nouvelles opportunités de croissance à un très grand nombre d'entreprises ». Toutefois, la principale promesse de l'IoT est de faire pénétrer la technologie partout dans la vie quotidienne, aussi bien chez les particuliers que dans les territoires ou les entreprises. L'horizon qu'il dessine est une société de connexions, de données et d'algorithmes, comme avaient pu en rêver les premiers cybernéticiens. Il s'agirait même d'une société dédoublée : celle « visible » des objets – y compris des ordinateurs – massivement accumulés par la « société de consommation », et celle « invisible » de la « société de communication » qui traite en permanence et silencieusement les données issues de ces objets (communicants) munis de capteurs.

Un récit de synthèse

Le grand « techno-discours » de l'IoT – un techno-discours est un « langage parasitaire branché sur la technique, contribuant à la diffuser » (Dominique Janicaud, *La Puissance du rationnel*, 1985) – a l'intérêt de synthétiser les récits précédents de la société de consommation et de la société de communication, voire de « la connaissance », qui se sont succédé depuis les années 1970. C'est pourquoi nous parlons d'un « méta-récit » se déclinant dans une multitude d'objets métamorphosés, une multiplicité de réseaux interconnectés et une inflation de données (*big data*). La trilogie objets/réseaux/données se retrouve par exemple dans cette image (l'imaginaire, c'est

(1) BALANDIER G. (2001), *Le Grand Système*, Paris, Fayard, p. 20.

aussi des images) qui représente – et naturalise – la « nébuleuse » de l'IoT sous la forme d'un arbre dans un livre blanc de l'Arcep (Autorité de régulation des communications électroniques, des postes et de la distribution de la presse) intitulé « Préparer la révolution de l'Internet des objets » (novembre 2016), qui précise que « le champ des objets connectés est potentiellement infini ».



Source : « Préparer la révolution de l'Internet des objets », livre blanc de l'Arcep, 7 novembre 2016, page 8

Cette convergence des récits antérieurs dessine ce qui est communément appelé la « révolution de l'IoT », un nouvel univers en formation ou plutôt en « transformation ». Cette formule souvent usitée n'est pas anodine : depuis la « révolution industrielle » du XIX^{e} siècle associée à la mécanisation, toute innovation techno-industrielle est qualifiée de « révolution ». Ainsi nos sociétés hyper-technologisées ne cesseraient pas de changer à coups de révolutions techniques permanentes. Cette antienne de la « révolution » est l'indice de ce que les sociologues nomment le « déterminisme technique », qui consiste à fétichiser la technique – fétichiser veut dire prendre la partie pour le tout, ici la technique pour la société. Ainsi chaque innovation technique changerait par elle-même l'ensemble de la société. Le slogan de « révolution IoT » est ainsi devenu un poncif du marketing pour les industriels du secteur.

Parce que le « techno-discours » de l'IoT fait converger les récits de la « société de consommation » marquée par l'accumulation et la consumation d'objets, celui de la « société de communication », dans laquelle les réseaux font lien, et celui de la « société de la connaissance » confondue avec la production d'informations et de données, il active plusieurs « techno-mythes » liés à l'innovation identifiés par le sociologue Abraham Moles. D'abord, le mythe de l'usine sans ouvriers obtenue par l'autonomie des objets et des machines ; ensuite, le mythe de l'ubiquité, qui promet d'être présent partout à la fois, et le mythe du Golem, qui consiste à créer des êtres artificiels « intelligents » (robots, agents ou objets). Autonomie, ubiquité et « intelligence » sont les mots-clefs qui caractérisent

l'IoT. La Commission européenne a même fusionné ces concepts-images dans une vision générale dite d'« intelligence ambiante ». Un quatrième techno-mythe est constamment sollicité pour la promotion des innovations : la promesse d'un nouvel eldorado économique ouvert par un marché quasi illimité [(2)]. Bien que multipliant les références à des mythes, ce méta-récit de l'IoT déjà vieux de plus de vingt ans, voire trente avec l'informatique ubiquitaire, demeure encore une promesse pour le futur. Il désigne et dessine un « vieux futur ».

Les pionniers : l'informatique ubiquitaire et le paradigme cybernétique

Toute technique est pétrie de fictions et de représentations, et en premier lieu celles des innovateurs, des concepteurs ou des pionniers qui imaginent les développements techniques. Il s'agit pour eux d'accomplir un rêve ou d'accompagner leurs innovations par des promesses pour les promouvoir et financer leur développement. L'IoT dérive de l'idée originelle de rendre invisible l'informatique : ni terminaux ni câbleries, celle-ci sera banalisée dans l'environnement. Une innovation doit être « magique », pour émerveiller comme un tour de prestidigitateur (c'était même le slogan préféré de Steve Jobs).

Pour désigner sa vision du futur, Mark Weiser, responsable scientifique du Xerox PARC (centre de recherches en informatique), utilisa pour la première fois en 1988, l'expression "*ubiquitous computing*" (« informatique ubiquitaire »). Dans un article fondateur "The computer for the XXIst century" (1991), Weiser écrit : « Les technologies les plus profondes sont celles qui disparaissent. Elles se tissent dans la vie quotidienne au point qu'on ne sait plus les en distinguer […] Les machines s'adaptent à l'environnement humain, plutôt que de forcer l'humain à entrer dans le leur ». Ce thème vulgarisé par l'écrivain américain Adam Greenfield dans son ouvrage *Everyware: The Dawning Age of Ubiquitous Computing (*2007), est celui d'une « intelligence ambiante » conçue sur le modèle de l'électricité dispersée partout et devenue complètement intégrée à l'environnement quotidien. L'IoT doit être invisible pour l'utilisateur, ce qui produit aussitôt un imaginaire positif lié à la simplicité d'usage, mais aussi inquiétant quant à l'action possible de ce système invisible (espionnage, pouvoirs occultes, etc.).

La technologie informatique deviendrait donc invisible : là encore travaille un techno-mythe récurrent identifié par Abraham Moles, à savoir le mythe de Gygès, qui permet à la technologie de voir sans être vue, comme la caméra cachée ou le drone. Inspirée d'Hérodote et développée dans *La République* de Platon, l'histoire de Gygès est celle de la découverte d'un anneau qui permet de devenir invisible. C'est ce que dit explicitement Weiser : « L'informatique ubiquitaire envisage un monde physique enrichi et invisiblement entrelacé de capteurs, d'actuateurs, d'écrans et d'éléments computationnels… dans les objets de nos vies quotidiennes et connectés dans un réseau [(3)] ».

Dans ce cadre est née la formule de l'Internet des objets en 1999, dans le laboratoire Auto-ID du MIT dédié à la création d'objets connectés à l'aide de l'identification par radiofréquence et des réseaux de capteurs sans fil. Kevin Ashton, un jeune informaticien anglais cofondateur de ce laboratoire, qualifia ainsi le lien entre des objets identifiés par des étiquettes RFID et l'Internet. À l'occasion d'une présentation devant les dirigeants de Procter & Gamble, Kevin Ashton insista sur l'idée de l'étiquetage électronique des produits pour faciliter la logistique de production.

Dans son livre, Adam Greenfield décrit le paradigme d'interaction de l'informatique ubiquitaire, ou "*pervasive*", comme le « traitement de l'information se dissolvant dans le comportement ». Et il ajoute : « Nous aurons réussi quand les ordinateurs auront disparu et que le monde sera

(2) L'eldorado… Selon les études, entre 20 et 150 milliards d'objets seraient connectés dans le monde d'ici à 2025. D'autres évaluations considèrent qu'un être humain serait quotidiennement en « interaction » avec 1 000 à 5 000 objets connectés. Les secteurs les plus transformés seront les transports, la santé, le logement, l'industrie et la distribution.
(3) WEISER M., GOLD R. & BROWN J. S. (1999), "The origins of ubiquitous computing research at PARC in the late 1980s", *IBM systems journal*, (38)4, pp. 693-696.

devenu notre interface ». Faire disparaître l'ordinateur et les technologies informatiques, c'est transformer le corps physique en une interface de ce monde invisible de calculateurs. C'est un retour à l'imaginaire de la première cybernétique : l'idée d'une symbiose homme-machine, imaginée dès 1960 par Joseph Licklider dans *Man-Computer Symbiosis*, créant un transfert du contrôle aux machines et un monde géré par un pouvoir automate et algorithmique. Avec le méta-récit de l'IoT, tous les éléments constitutifs de « l'utopie de la communication » présents dans la première cybernétique (Philippe Breton) sont réactivés, notamment la quantification du monde et la « gouvernance par les nombres » (Alain Supiot) [(4)].

Un objet-valise comprenant des objets, des réseaux et des données

L'IoT est un objet-valise comme le furent les « autoroutes de l'information » au début de l'Internet, expliquant la puissance d'un imaginaire par son indétermination. Cet objet-valise est composé d'une trilogie magique : objets et environnements parlants-intelligents, réseaux de réseaux connectés sans limites, *big data* collectées, stockées et traitées *via* des algorithmes (intelligence artificielle).

Objets : maîtres ou esclaves ?

Dans l'IoT, les objets captent, parlent, interagissent ou travaillent, et même « pensent » selon Greenfield, donc ils sont anthropomorphisés tandis que les humains sont réduits à des paquets de données. Parce qu'il échange des informations, l'objet connecté est censé être interactif, « intelligent » et producteur de données ; autrement dit, il est proche d'un être vivant. Depuis le mythe du Golem jusqu'au canard de Vaucanson ou au Frankenstein de Mary Shelley, il s'agit d'imiter le vivant par le mécanique et l'artificiel.

Avec l'IoT, l'objet deviendrait un acteur autonome, capable de percevoir, d'analyser, voire de penser et d'agir… Et la « nébuleuse » de l'IoT se déplie comme une liste à la Prévert, sans limites dans tous les objets du quotidien, à commencer par les gadgets : la brosse à dents qui informe sur l'état de santé buccal, l'assiette connectée, ou *smartplate*, sorte de nutritionniste personnel, le pommeau de douche connecté ou le frigo connecté, comme le Family Hub de Samsung qui gère la nourriture disponible et offre plusieurs services, etc. Cette électronisation des objets quotidiens n'est pas nouvelle et fut déjà plusieurs fois envisagée par exemple avec la télématique, les réseaux câblés ou le *smartphone*. L'IoT ne fait que retrouver (réactiver) des techno-récits déjà actifs avec la télématique dans les années 1980, ceux de la « domotique », de « l'immotique », voire de ce qui était nommé « l'urbatique », revisités comme *smart home, smart building, smart cities*. Au-delà des objets quotidiens, ce sont tous les systèmes complexes qui sont inclus dans l'IoT, notamment les transports, la santé ou la ville.

Le développement le plus important de l'IoT est dans l'usine, avec l'échange d'informations entre machines en réseau et l'exécution automatique d'opérations M2M (*machine-to-machine*). Là travaille encore le mythe de l'usine automate sans ouvriers, complété par la prédiction et la recommandation avec « la maintenance prédictive » : identifier des risques ou prévoir des pannes est l'usage industriel fréquent grâce à des capteurs qui mesurent la pression, la température, les frottements ou l'usure pour prévenir des risques ou des pannes.

Comme souvent pour les techno-imaginaires, ce sont les écrivains de science-fiction (et les *blockbusters* hollywoodiens) qui mettent en scène ces représentations. Dans un ouvrage de 2005, *Shaping Things* (*Objets bavards*), Bruce Sterling a inventé un terme pour traiter de l'IoT,

(4) BRETON P. (2004), *L'utopie de la communication : le mythe du village planétaire*, La Découverte ; SUPIOT A. (2015), *La gouvernance par les nombres. Cours au Collège de France 2012-2014*, IEA de Nantes/Fayard.

les *"spimes"*– néologisme contractant *space* et *time* –qui sont des objets hybrides réel-virtuel dans l'Internet : « Les *spimes* sont des objets manufacturés dont la structure informative est si irrésistiblement étendue et riche qu'ils sont considérés comme les incarnations matérielles d'un système immatériel. Les *spimes* sont des données, du début à la fin de leur existence. […] Dans une infrastructure de *spimes*, les individus sont des "collecteurs" ». Chez Sterling, la vision de l'IoT est bien ambivalente : il prophétise à la fois une société de surveillance et une nouvelle capacité d'action et d'invention des *spimes* pour sauver le monde.

La vaste entreprise de numérisation du monde physique, qui relie individus et matériels, conduit à une hybridation entre le réel et le virtuel, et brouille aussi une distinction juridique majeure entre les personnes et les choses. Tout se passe comme dans un jeu de vases communicants : l'humain est réduit à un corps lui-même ramené à une banque de données, alors que l'environnement devient lui « intelligent » par la captation et la production de données. Ainsi l'objet connecté « recommande » des comportements aux personnes [5]. La distinction des choses et des personnes trace une ligne de démarcation dans les imaginaires : ceux qui sont acceptables (le traitement des choses) et ceux qui sont inacceptables ou mal acceptés (le comportement des personnes). En effet, il est essentiel en droit de distinguer les personnes et les choses, les personnes étant « sujets de droits » et les choses étant « objets de droit ». Cette frontière entre personnes et choses s'effacerait dans l'IoT : étant sans territoire, il se déploie de façon virale comme un rhizome sans limites ni frontières.

Données : assistance ou espionnage

Dans l'imaginaire collectif, les objets connectés produisant des données sont perçus tantôt comme des assistants, tantôt comme des espions. Cette ambivalence soulève de nombreuses questions sur la protection de la vie privée (*privacy*) et des données personnelles, et sur la gouvernance de cet Internet tentaculaire. Quel contrôle de l'IoT ? Peut-on « éteindre » la captation de données ? Quel serait l'interrupteur comparable à l'électricité ? Quelle prise sur cette espèce de méga-automate invisible ? Assistance ou espionnage, communication ou surveillance ?

En effet, dans l'IoT tout est « datifié » et quantifié – y compris la quantification de soi ou *quantified self* – et soumis à une gouvernance algorithmique et calculatrice. Le traitement des données par l'IA permet de dire à chacun comment se comporter en fixant des normes quantifiées (exemple des 10 000 pas/jour) pour demeurer en forme et performant. De même qu'il est « prédictif » pour les machines, l'IoT est normatif pour les individus : il livre des prescriptions à chacun sous prétexte de le « responsabiliser » en le mettant « face à ses données » quantifiées et mesurées en continu. Là aussi, c'est le paradigme cybernétique défini par Norbert Wiener, qui a introduit une nouvelle « méthode comportementale d'étude », qui s'applique à tous les phénomènes naturels, sociaux ou humains. La cybernétique traite des relations entre l'objet et son environnement, c'est-à-dire du « comportement » assimilé à un message et le message à de l'information. Dans la cybernétique, connaitre c'est simuler, imiter le comportement d'une machine : « penser, c'est calculer ». Ainsi la connaissance de soi – idéal de la sagesse pour la philosophie grecque (« connais-toi toi-même ») – est réduite et déduite de la quantification de ses données physiques corporelles. Ici est à l'œuvre un imaginaire de la connaissance basculant de la connaissance considérée comme culture/compréhension du monde et de soi, à la connaissance définie comme calcul et information (1950, cybernétique).

Finalement, l'IoT promet à chacun de tout savoir sur tout *via* ses données personnelles, et finalement de ne rien comprendre par une avalanche de données et de nombres. Car, faut-il le rappeler, la donnée n'est pas l'information et encore moins la connaissance, mais cette confusion est au cœur des techno-récits sur l'IoT. Les données ne prennent sens que codifiées et transformées

(5) David Chavalarias parle de la « société de recommandation » dans *La société recommandée* (2012, Lavoisier), *i.e.* proposant un modèle de société. Ce qui est bien l'idée du paradigme cybernétique.

en informations. L'information donne des critères de pertinence pour parler le même langage, mais elle n'est pas la connaissance : « L'information est l'ennemie de l'intelligence » a même pu dire le poète américain Donald Hall. La connaissance donne le sens, elle sélectionne et trie par jugement, expérience, intuition, hiérarchisation…

Réseau : communication ou surveillance ?

La communication et le contrôle sont les deux faces de Janus de l'imaginaire réticulaire qui fait circuler et retient à la fois (comme un tissu ou un filet de pêche ou de chasse, figure originelle du réseau). Or ce sont les réseaux qui rendent possibles l'IoT et les échanges entre les objets et leur environnement. D'où cette définition de l'Internet des objets : « Un réseau de réseaux qui permet, *via* des systèmes d'identification électronique normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques mais aussi de pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s'y rattachant [(6)] ».

L'IoT étant « une extension de l'Internet actuel à tous les objets pouvant communiquer de manière directe ou indirecte avec des équipements électroniques eux-mêmes connectés à Internet [(7)] », il amplifie l'imaginaire de ce dernier. La connectivité semble sans limites, et les distinctions classiques éclatent (choses/personnes, réel/virtuel, etc.). Une première approche de l'IoT identifierait un imaginaire identique à celui de l'Internet, celui d'un réseau de réseaux dont la sphère applicative s'élargit. L'image de l'interconnexion généralisée et mondialisée porte toujours en elle deux figures opposées : le paradis de la communication et de la transparence, et l'enfer du contrôle et de la surveillance. La puissance de ces deux visions est augmentée dans l'IoT par la collecte invisible des données dans les objets transformés en assistants ou en espions. Empruntant l'imaginaire de l'Internet qu'il ne fait qu'étendre, celui de l'IoT demeure donc enfermé dans l'opposition entre la société de contrôle et la société de communication.

Fantasia ou le mythe de l'apprenti sorcier

La double promesse/menace de l'IoT est l'extension de l'informatisation aux choses et celle de l'hyperconnexion réticulaire. C'est un imaginaire issu de la cybernétique auquel s'ajoutent les apports des représentations de l'informatique et des télécommunications qui animent les récits sur la « société de communication » depuis quelques décennies. Le paradigme cybernétique est activé à chaque vague de nouveaux services issus de cette rencontre : l'ordinateur apporte l'autonomie et les télécoms la connexion. Tout est transformé par cette dynamique combinant les vertus et les mythes de « l'auto » (mythe de l'autonomie et de l'automate) et du « télé » (mythe du lien à distance).

Avec l'IoT, tout devient « auto » et « télé ». Faire agir à distance les objets de façon autonome et invisible, c'est convoquer une fois encore le mythe de l'apprenti sorcier décrit par le Grec Lucien de Samosate au II^{e} siècle avant d'être mis en mots dans une ballade de Goethe, adapté dans le poème symphonique de Paul Dukas et mis en images dans le dessin animé *Fantasia* de Walt Disney. Images, sons et mots sont combinés dans l'imaginaire populaire de l'apprenti sorcier. Le coté merveilleux et magique des technologies est toujours premier, comme l'avait souligné Jean-Jacques Rousseau, mais ensuite la machine merveilleuse peut se transformer en machine autonome incontrôlable. Quel magicien ou quel pouvoir régulera et contrôlera l'IoT ? Quel sera le tiers garant de cette grande machinerie pour éviter qu'elle ne devienne une machination orwellienne ? Tel est le nouveau spectre qui hante le monde prédictif et prescriptif dessiné par l'IoT.

(6) BENGHOZI P.-J., BUREAU S. & MASSIT-FOLLÉA F. (2009), *L'Internet des objets - Quels enjeux pour l'Europe ?*, Paris, Éditions de la Maison des sciences de l'homme.
(7) WEILL M. & SOUISSI M. (2010), « L'Internet des objets : concept ou réalité ? », *Réalités industrielles*, novembre, pp. 90-96.

L'histoire des objets connectés

Par **Jean-Pierre CORNIOU**
Économiste, ancien élève de l'Ena

« Objets inanimés, avez-vous donc une âme ? »,
Alphonse de Lamartine.

Désormais installés dans notre quotidien, les objets connectés sont devenus une porte d'entrée familière et naturelle dans le monde du *web*. Leur histoire est courte et féconde. En deux décennies, les objets connectés seraient aujourd'hui près de 30 milliards. Toutefois, la profusion des formes et fonctions de ces « objets » en font un domaine flou et mouvant de la révolution numérique. Un « objet connecté » est simplement un objet classique – brosse à dents, montre, thermomètre, balance, serrure, automate, vêtement ou véhicule… – auquel on a greffé des capteurs et des capacités de communication permettant d'analyser son comportement et, dans certains cas, d'agir. Si l'expression « Internet des objets » est utilisée depuis 1999, elle recouvre donc des situations très différentes dans le monde des applications domestiques, industrielles, dans le transport et l'énergie ou la santé. C'est donc un domaine fluide qui fait les beaux jours des chasseurs d'innovations spectaculaires, arpentant chaque année les couloirs du CES, la plus grande manifestation mondiale dédiée au numérique, à Las Vegas, où ces produits nouveaux sont présentés chaque année. Mais le monde des objets connectés ne se limite pas aux usages individuels et domestiques. Il porte sur tous les secteurs, toutes les activités, et contribue à la recherche de l'efficience des processus industriels et à l'optimisation de la gestion des ressources.

Leur histoire apporte un éclairage précieux sur le processus d'innovation accéléré que connaît le monde de l'Internet, nourri par le rapport dialectique entre capacité technique et logique d'usage. Les percées technologiques alimentent l'innovation qui se traduit par de nouvelles propositions d'objets et de services qui partent à la rencontre du public. Si leur propagation est rapide, comme le fut celle du téléphone mobile, la diffusion à large échelle d'objets connectés en réseau permet de créer de nouveaux usages et de nouveaux marchés. Au-delà d'effets de mode éphémères, l'addition de ces objets pose désormais la question de leur utilité collective. La multiplication de milliards de capteurs connectés exploitant la capacité de traitement du cœur de la machine numérique – *data centers*, réseaux à haute capacité, logiciels de traitement des données de masse – permet-elle de donner une dimension cohérente à cet agrégat d'objets et de données hétérogènes ? Pourra-t-on ainsi enrichir notre capacité à comprendre et à piloter notre environnement tout en préservant notre liberté de discernement et notre capacité à rester anonyme ?

L'histoire des objets connectés s'inscrit dans la longue perspective de l'histoire des techniques de traitement automatisé de l'information, de l'invention des machines mécanographiques programmables aux ordinateurs centraux à partir de la fin de la Seconde Guerre mondiale, puis au micro-ordinateur à partir de 1980. L'informatisation de la société a franchi une étape majeure à la fin du XX^{e} siècle avec la conquête de la sphère grand public par des outils naguère réservés, à cause de leur coût et de leur complexité d'usage, au monde de l'entreprise.

Le marché des premiers micro-ordinateurs, dans les années 1980, a souffert de l'infirmité de cette machine puissante à communiquer. Échanger des données avec l'extérieur est devenu une nécessité. Ceci a donné naissance à une première connexion, celle de l'ordinateur à son imprimante, pour produire et diffuser des informations. L'épopée de l'Internet, engagée en 1969,

s'est accélérée à partir de 1994 avec la mise en place des outils logiciels qui permettaient d'exploiter facilement la capacité de connexion offerte par les réseaux de télécommunications. L'habile architecture de l'Internet (réseaux TCP/IP, serveurs DNS) a permis d'accueillir de façon continue nouveaux objets et nouvelles fonctionnalités. Cette révolution technique, accompagnée d'une baisse des coûts et de la dérégulation des télécommunications, a ouvert le champ de l'innovation à une généralisation des échanges numériques entre ordinateurs puis, par couches progressives, entre objets électroniques et physiques n'ayant pas été initialement conçus pour communiquer.

La dissolution des frontières entre catégories d'objets

Le MIT Media Lab, créé en 1985, a été le creuset de travaux pluridisciplinaires sur les usages technologiques dans tous les domaines de la société inspirant les chercheurs et les pionniers de l'industrie. Au début des années 2000 est apparu le concept d'ATAWAD – *anytime, anywhere, any device* – qui illustre parfaitement l'ambition de tous les acteurs du *web* : créer un monde d'interconnexion généralisée offrant à chacun la capacité de puiser dans les ressources numériques mondiales pour travailler, s'informer, se distraire, se déplacer. Cette révolution de l'omni-communication a très vite fait exploser le cadre normatif qu'avait installé l'informatique classique, autour du terminal passif, puis du micro-ordinateur connecté, pour généraliser la multiplicité des sources. Néanmoins, l'architecture de ce nouveau système est restée fidèle à la vision de von Neumann, séparer les données et les traitements. Le travail des informaticiens consiste à numériser tout type d'information et à dissocier l'information de son support. Cette rupture technique a entraîné l'effondrement d'un monde d'ingéniosité et de maîtrise qui avait poussé la qualité des systèmes mécaniques et chimiques de capture d'information, de mesure et de reproduction du son et de l'image à un degré élevé de performance. L'informatique a pénétré chacun de ces domaines d'excellence, où le génie humain avait su repousser les limites physiques, de l'horlogerie à la photographie, de la métrologie au son, du calcul à l'art de la localisation, de la régulation à l'automatisme. En transformant les données analogiques en données numériques, on a appris à les interpréter, les stocker, les restituer sous des formes de plus en plus ergonomiques, et étendu le domaine des connaissances, désormais encore amplifié par l'intelligence artificielle.

Par exemple, pour la musique, un disque microsillon contient de l'information qui ne peut être dissociée de son support physique, la transcription de cette information en signal sonore se faisant par un ingénieux système physique qui consiste à lire les sillons gravés sur le disque, traduits en signal électrique par une cellule électromagnétique. L'industrie phonographique a déployé des trésors d'intelligence pour reproduire un son le plus fidèle possible au son d'origine enregistré. En quelques années, cet édifice a été balayé par la numérisation du signal qui permet tout au long de la chaîne de maintenir l'intégrité de l'information sous forme de 0 et de 1. Transformant chaque secteur vertical, la numérisation du signal a également permis de rapprocher des domaines qui s'ignoraient pour créer des objets et des services nouveaux. De mécanique et physique, la compétence devient logicielle.

L'histoire des objets connectés est celle d'une expansion continue des possibilités techniques et des usages, servie par la miniaturisation des composants, la baisse des coûts, les progrès des logiciels et l'ouverture des possibilités de communication.

La conquête de la démocratisation

Le succès des objets connectés est alimenté par leur utilité. L'imagination est sans limites, car il est tentant d'adjoindre à un objet classique les équipements qui vont le rendre « connecté ». Les *start-up* n'hésitent pas à proposer des rapprochements étonnants, souvent sans lendemain, car le marché ne suit pas ces défricheurs de la connectivité. Le succès durable n'est en effet atteint que lorsque

l'évolution de l'objet répond à un double examen : est-ce utile ? Est-ce agréable ? De plus, est-ce que la promesse d'utilité et d'agrément est atteinte avec un coût acceptable au regard de la valeur perçue ?

Car il n'est pas évident de faire un produit pertinent qui ne finit pas prématurément sa carrière dans l'oubli d'un placard, soit parce qu'il ne fonctionne pas convenablement, soit parce que, plus prosaïquement, son possesseur finit par conclure… à son inutilité.

Le plus grand succès de tous les objets connectés a été le téléphone mobile. Le téléphone mobile dans sa version initiale ne fonctionnait que comme un téléphone conventionnel, mais sans fil pour échanger par la voix. Il a fallu l'invention du "*smartphone*" en 2007 pour transformer cet outil simple en objet complexe multifonctionnel. En effet, outre l'ergonomie et le clavier tactile immédiatement reconnus comme clivants, Steve Jobs a eu l'intuition d'équiper son téléphone de capteurs inusités par ses concurrents et qui ont conduit à propager de nouveaux usages. Ainsi, le premier iPhone était équipé d'un appareil photo et de fonctions audio puissantes ; la fonction de géolocalisation a fait son apparition dès la version 2, en 2008, exploitant la 3G. La photographie a connu une transformation spectaculaire avec la généralisation de la capture d'images en toutes circonstances et de leur diffusion instantanée.

Mais c'est certainement la géolocalisation qui a le plus transformé la vie quotidienne. Elle a permis de mettre au point des applications multiples permettant l'exploitation des données contextuelles. Uber est né de la géolocalisation. Et la géolocalisation s'est développée grâce à l'effondrement du prix des capteurs, d'une centaine de dollars en 2000 à quelques dollars aujourd'hui. Plus encore, les performances de ce couteau suisse qu'est devenu le *smartphone* ont rendu la possession d'autres objets dédiés inutile dans la plupart des cas, asséchant des marchés bien établis comme celui des appareils photos.

Pour rendre connectable tout objet, l'idée de leur adjoindre une étiquette active a été une des premières pistes pour répondre au problème du suivi d'objets de masse. La technique de Radio Frequency IDentification (RFID) a fait l'objet de nombreux essais et mises au point depuis son origine dans les années 1930. Il s'agit d'envoyer une onde électromagnétique sur un objet qui, doté d'une étiquette passive, non alimentée, va renvoyer un signal grâce à un composant électronique doté d'une antenne. Cette technique s'est révélée simple, efficace, et peu coûteuse. Plusieurs types d'étiquettes ont été mis au point permettant le transfert d'information sur des distances allant de quelques centimètres à plusieurs centaines de mètres selon les bandes de fréquence et la possibilité de les alimenter électriquement de façon autonome. Une des limites actuelles à la multiplication des capteurs est leur alimentation en énergie.

Les objets connectés doivent leur succès à un nombre limité d'infrastructures qui permettent leur collaboration. Il s'agit bien évidement des progrès considérables des télécommunications mobiles depuis les années 1980, arrivées aujourd'hui à leur cinquième génération. Les normes de communication, dont Bluetooth, WiFi, ZigBee, LoRa, jouent le rôle essentiel d'assurer la communication bidirectionnelle à courte distance entre objets. La normalisation a été l'accélérateur attendu de l'Internet des objets, permettant l'interopérabilité et la durabilité des systèmes, ce que ne pouvaient garantir les premiers systèmes propriétaires.

Le développement de systèmes de géolocalisation par satellite, dont le système américain Navstar GPS a été le pionnier à partir de 1975, est également un composant majeur du système d'échanges entre objets en apportant une référence physique de positionnement ultra précise. GPS, d'origine militaire, n'a été ouvert aux usages civils, sans être bridé, qu'en 2000 alors que depuis de nouveaux systèmes, comme Galileo pour l'Europe, ont une vocation civile et commerciale. Russes, avec GLONASS, et Chinois, avec Beidou, se sont dotés de leurs propres systèmes. Plusieurs milliards de capteurs des signaux satellites de géolocalisation sont en fonctionnement, notamment depuis que les *smartphones* sont équipés en série de ce composant.

Parmi les objets usuels que la connectivité a déjà profondément transformés, l'automobile offre un exemple en pleine effervescence. Dans un ouvrage publié en 2001, *Naissance de l'automobile moderne 1930-2000*, les auteurs jugent l'évolution électronique des véhicules : « Régulateur de vitesse automatique, radar, commandes vocales et navigation par satellite étaient annoncés pour les années 1990 sur la plupart des modèles mais, en réalité, ils sont encore trop complexes et coûteux pour un modèle familial courant ». Tous les pionniers de l'aide à la navigation dans la décennie 1990, dont Renault avec le système Carminat, doutaient de la possibilité de parvenir un jour à créer un système attractif, fiable et surtout économique tant les obstacles techniques pour numériser l'ensemble du territoire et assurer le suivi du véhicule étaient nombreux. En moins de vingt ans, toutes les voitures disposent d'un équipement qui aurait fait rêver les possesseurs de voiture de luxe des années 1980. Tous les constructeurs et équipementiers travaillent à l'intégration de ces capteurs en assurant une continuité d'informations entre le véhicule, les véhicules qui l'entourent et l'infrastructure au sol. Ces technologies sont nommées V2X, *vehicule-to-everything*. L'enjeu est désormais de faire en sorte que l'addition d'informations n'en vienne à perturber le conducteur au lieu de renforcer sa protection et facilité de conduite.

L'automobile est devenue un produit hybride entre mécanique et électronique. Se pose désormais un nouveau défi pour l'industrie automobile, celui de la dépendance envers les éditeurs de logiciels, les fabricants de microprocesseurs et composants électroniques, ce qui conduit à de nouvelles alliances entre constructeurs, équipementiers et spécialistes du numérique embarqué.

De l'objet connecté à l'information

En développant de multiples objets dotés d'une capacité de communication, l'industrie a généré la production d'un volume considérable de données qui représentent un potentiel d'informations très riche. Faire de ce potentiel hétérogène un actif utile à la communauté semble bien être un des enjeux de ce XXI^{e} siècle.

En effet, chaque machine, chaque équipement, fixe ou mobile, peut être équipé de ressources renseignant sur son état et son niveau de performance. Cette faculté présente évidemment le potentiel de surveiller le fonctionnement des installations opérationnelles et de gérer de façon précise les dysfonctionnements des équipements. La promesse de comprendre et de maîtriser le fonctionnement d'ensembles complexes est évidemment la vitrine alléchante du monde des objets connectés. Ainsi, la plateforme chinoise de commerce en ligne Alibaba présentait au CES de 2018 son concept "City Brain", déployé dans la ville d'Hangzhou. Il s'agit de connecter 1 300 feux de circulation pour analyser en temps réel la circulation de la ville, et d'optimiser la fluidité du trafic en prédisant, grâce à l'intelligence artificielle, l'évolution du trafic et en réagissant à tous les incidents. Si de tels systèmes ont pu être exploités dès les années 1980, c'est bien la qualité des capteurs, la fusion des informations et la puissance des logiciels qui permettent d'atteindre un haut niveau de performances. Il y a un envers moins séduisant, celui d'une omni-surveillance potentielle de tous les comportements, ce que la Chine admet au nom du bénéfice social que la communauté retirerait de ces outils.

En rassemblant les données, il est désormais possible de produire un modèle fidèle du fonctionnement d'une installation. Il s'agit de la technique du jumeau numérique. L'objectif premier est de comprendre les interactions entre les composants d'un système, afin de parvenir à en optimiser le fonctionnement global et à anticiper les dysfonctionnements pour intervenir en maintenance préventive.

Les objets connectés permettent d'établir le lien entre la réalité physique et sa représentation numérique. Ils constituent une pièce essentielle de la numérisation de la société, car ils ouvrent la possibilité de contribuer à régler les problèmes de fonctionnement des systèmes complexes.

Il y a certes beaucoup de promesses sans lendemain dans cette marche en avant désordonnée, mais féconde. Ainsi, le pari de la voiture autonome est encore loin d'être gagné ! Mais les progrès enregistrés dans la compréhension du vivant, du climat, des systèmes de production industrielle rendent optimiste sur la capacité à comprendre notre environnement physique et social, et à agir dans une nouvelle culture de la frugalité et de l'efficience.

La traçabilité

Par **Matthieu HUG**
Cofondateur et CEO de Tilkal

Avec la crise du Covid-19, beaucoup d'entreprises se penchent sur la résilience de leur chaine d'approvisionnement : c'est-à-dire sur sa « capacité à maintenir un système d'actions organisé face à une situation inhabituelle dans le but de préserver son existence » [(1)]. Pour assurer cette résilience, connaitre, évaluer et suivre sa chaine d'approvisionnement est indispensable : ce que l'on appelle couramment la traçabilité. Or, fin 2020, une étude de Bain et du World Economic Forum montrait que seuls 15 % des dirigeants d'entreprises pensent que leur *supply chain* offre une traçabilité suffisante et consistante [(2)].

Ceci a deux conséquences très observables : les fraudes et les déficiences des rappels sanitaires. Ces phénomènes sont favorisés par la fragmentation des chaines d'approvisionnement qui a progressivement rendu les suivis inopérants, créé de nombreux interstices opaques et dilué les responsabilités.

Des fraudes aux rappels

En 2016, près de 7 % des produits importés dans l'Union européenne étaient de la contrefaçon, soit + 40 % par rapport à 2013 [(3)]. Aux États-Unis, 20 % du poisson vendu est frauduleux [(4)]. L'alcool illicite représente 25 % de la consommation mondiale et 40 % en Afrique [(5)]. Récemment en France, un grossiste en fruits et légumes a pu frauder sur l'origine de plusieurs centaines de tonnes de légumes à l'insu de toute la distribution [(6)]. Plus étonnant, au dernier trimestre 2020, les cigarettes illicites représentaient 28 % du marché dans les Hauts-de-France [(7)], démontrant une perte nette de contrôle sur un marché pourtant très réglementé. Ces exemples peuvent être déclinés à tous types de produits, et reflètent souvent une infiltration croissante, volontaire et notoire d'organisations criminelles dans la production et le commerce mondial [(8,9)] : à l'origine pour du blanchiment, de plus en plus pour le commerce illicite en lui-même, peu dangereux et très lucratif, notamment *via* les grandes places de marché *e*-commerce.

Dans un cas sur deux, ces produits illicites présentent un risque pour la santé. Lorsqu'une anomalie sanitaire ou autre est détectée, un rappel produit est déclenché pour retirer des rayons les produits concernés : en France, 80 retraits ou rappels sont déclenchés chaque mois [(10)]. Or en 2018, la

(1) https://fr.wikipedia.org/wiki/Résilience_weickienne
(2) https://www.bain.com/about/media-center/press-releases/2020/more_than_85_percent_of_executives_believe_their_current_supply_chain_capabilities_will_not_deliver_the_traceability_needed_to_remain_resilient_and_sustainable_in_a_post_covid_world/
(3) https://euipo.europa.eu/ohimportal/fr/web/observatory/trends-in-trade-in-counterfeit-and-pirated-goods
(4) https://www.weforum.org/agenda/2019/08/a-seafood-fraud-investigation-dna-tested-fish-sold-in-the-us-here-s-what-they-found/
(5) https://www.tracit.org/uploads/1/0/2/2/102238034/illicit_alcohol__-_white_paper.pdf
(6) https://www.lepoint.fr/economie/fraude-sur-l-origine-un-grossiste-soupconne-d-avoir-francise-des-legumes-05-07-2021-2434190_28.php
(7) https://france3-regions.francetvinfo.fr/hauts-de-france/entretien-les-dessous-d-un-trafic-de-cigarettes-de-grande-ampleur-dans-les-hauts-de-france-2208955.html
(8) https://www.europol.europa.eu/publications-documents/2017-situation-report-counterfeiting-and-piracy-in-european-union
(9) https://www.franceculture.fr/emissions/entendez-vous-leco/leconomie-du-crime-13-les-mafias-dans-la-mondialisation
(10) https://www.oulah.fr/a-propos/

commission d'enquête sénatoriale sur le rappel de lait pour enfants contaminé à la salmonelle [11] constatait dans son rapport « des dysfonctionnements préoccupants dans la protection sanitaire offerte aux consommateurs ». Trois ans après, le rappel sur l'oxyde d'éthylène tend à démontrer malheureusement que ce constat est toujours d'actualité.

L'oxyde d'éthylène est un insecticide dangereux pour la santé, interdit en Europe depuis 2011. En septembre 2020, une alerte européenne est lancée à la suite de taux 1 000 fois supérieurs aux normes dans 34 lots de graines de sésame importés d'Inde [12]. Une vingtaine de distributeurs, des dizaines d'industriels et des centaines de produits sont concernés (glaces, biscuits, houmous, baguettes, salades, burgers, farines, huiles, purées, biscottes ou encore chocolats).

Un an après, ce rappel n'est pas clos, loin de là : le nombre de lots rappelés en France a crû de 40 % entre juin et août 2021. La liste des 10 000 lots concernés est disponible et mise à jour par la DGCCRF (Direction générale de la concurrence, de la consommation et de la répression des fraudes) [13,14]. En revanche, la simple liste des magasins ayant ces lots en rayons n'existe pas : il n'y a pas de suivi utilisable et partagé des lots de la production au magasin. À l'évidence, cela empêche de localiser des lots incriminés et donc d'en assurer un rappel exhaustif. C'est ainsi que la commission d'enquête sénatoriale constatait en 2018 que « des produits relevant de lots potentiellement contaminés ont continué à être offerts à la vente dans certaines surfaces des réseaux de la grande distribution ainsi que dans certaines officines de pharmacie ».

Ce constat s'applique aussi aux géants de la distribution *e*-commerce : chez Amazon, des produits contrefaits ou périmés, y compris des laits pour enfants, sont laissés en vente dans des proportions significatives [15]. L'analyse du consommateur pour optimiser son panier moyen semble plus prioritaire que le suivi des produits pour protéger ce même consommateur.

Dans une note de 2005, la direction générale de l'alimentation (DGAL) évoquait un manque essentiel à l'origine de ces dysfonctionnements : « La traçabilité des denrées alimentaires doit être mise en œuvre par l'ensemble des opérateurs de la chaine alimentaire, de la production à la distribution » [16]. Mais qu'entend-on par « traçabilité » ?

La traçabilité : une notion évolutive

La malléabilité du terme « traçabilité » en fait une notion riche et évolutive, mais crée aussi une ambigüité sur ce que cela recouvre en pratique.

Dès le Premier Empire babylonien, il y a 3 800 ans, le code Hammurabi imposait l'identification des animaux d'élevage par un marquage corporel et la tenue des registres correspondants : ces registres sont ce que l'on peut appeler la « traçabilité », au sens de la « possibilité d'identifier l'origine et de reconstituer le parcours (d'un produit), de la production à la distribution [17] ». À partir du XIVe siècle et de la Grande Peste, ce type de suivi a été mis au point du fait d'une préoccupation essentiellement sanitaire [18].

(11) https://www.emballagesmagazine.com/marquage-codage/quelle-tracabilite-apres-l-affaire-lactalis.46837 (11)
(12) https://www.quechoisir.org/actualite-pesticide-cancerogene-contamination-massive-de-produits-au-sesame-n84707/
(13) https://www.economie.gouv.fr/dgccrf/sesame-psyllium-epices-et-autres-produits-rappeles-comprenant-ces-ingredients
(14) https://rappel.conso.gouv.fr
(15) https://www.cnbc.com/2019/10/20/amazon-is-shipping-expired-baby-formula-and-other-out-of-date-foods.html
(16) http://archive.wikiwix.com/cache/index2.php?url=http%3A%2F%2Fwww.astrolabe-fr.com%2Fdoc%2Fdgaln20058205z.pdf
(17) https://dictionnaire.lerobert.com/definition/tracabilite
(18) BLANCOU J. (2001), "A history of the traceability of animals and animal products", *Rev. Sci. Tech.*, 20(2), août, pp. 413-425.

Avec l'industrialisation, un glissement de sens et d'objectif intervient. Dans un contexte de production de masse, la tenue de registres des biens individuels est assez irréaliste sans numérisation. De plus, par hypothèse, tous les biens issus d'une même production sont équivalents : ce qui importe, c'est la répétabilité du processus, contrôlée par des normes et des labels. Dès lors, la traçabilité vise principalement les processus de production des biens, plutôt que les biens produits. Même quand certains marquages de biens sont établis (numéros de lot), ils donnent rarement lieu à la tenue de registres utilisables à grande échelle ou pour de l'analyse, c'est-à-dire des registres numériques. Finalement, la traçabilité se restreint à un angle de vue « local » à l'entité de production : dans une production de masse indifférenciée, le parcours et l'origine des biens sont indifférenciés, voire indifférents [19].

Au XXIe siècle, la notion de traçabilité s'enrichit. Le devoir de vigilance implique, d'une part, de connaitre l'impact social ou environnemental de la production, d'autre part, il rend les industriels largement responsables de ce qui se passe chez leurs fournisseurs : en instituant une « responsabilité bout en bout », il ré-institue le besoin d'une « traçabilité bout en bout », ou, pour reprendre la norme ISO 9000:2015, d'une « aptitude à retrouver l'historique, la mise en œuvre ou l'emplacement d'un objet (produit, service, processus, personne, organisme, système, ressource [20] ».

Ces différents types de traçabilité sont complémentaires et nécessaires pour s'adapter aux évolutions le long de la chaine d'approvisionnement. La nature des biens évolue, au gré des transformations, des mélanges ou des compositions, passant de matières premières en vrac à un bien unitaire. Ce que l'on trace va évoluer : parfois le bien directement, mais la plupart du temps un de ses contenants (carton, palette, conteneur, etc.). L'objectif de la traçabilité évolue lui aussi : origine, localisation, composition, conditions de travail, chaine de froid, etc.

Enfin, la finesse de traçabilité peut évoluer suivant la nature du bien. Pour les biens de grande consommation par exemple, une traçabilité au lot, de la production aux magasins, est à l'évidence indispensable pour des raisons sanitaires et de rappel. C'est ce que rendent obligatoire des réglementations récentes aux États-Unis (FSMA, section 204) [21] ou en Russie ("Federal Act No. 487-FZ") [22]. Celle-ci n'est pourtant envisageable et viable que si elle repose sur un registre partageable et exploitable, c'est-à-dire 100 % numérique.

Les objets connectés pour améliorer la traçabilité

Pour ce faire, les différents points de collecte d'informations doivent être numérisés : grâce à de simples *smartphones* ou grâce à des objets connectés plus spécialisés.

Objets connectés et *smartphones* interviennent comme des systèmes de marquage actif, permettant de multiplier les points de capture d'informations, et donc de combler progressivement les angles morts des chaines d'approvisionnement. Leur rôle naturel dans la traçabilité est de créer de nouvelles informations (capteur de température, GPS ou tag RFID) ou de les numériser en remplaçant le papier (*smartphone* ou tablette).

(19) https://france3-regions.francetvinfo.fr/centre-val-de-loire/lait-produits-laitiers-sur-decision-du-conseil-d-etat-l-etiquetage-de-l-origine-geographique-n-est-plus-obligatoire-2003188.html
(20) https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v2:fr
(21) Le "Food Safety Modernization Act" (section 204) impose d'ici à 2025 une traçabilité de la ferme à la fourchette des lots de produits alimentaires distribués aux États-Unis.
(22) Le "Federal Act No. 487-FZ" impose pour 2024 une traçabilité au lot pour tous les produits de grande consommation vendus en Russie.

La « traçabilité » finale d'un bien résulte de l'association des différentes traçabilités de ses composants, de ses processus et de ses transports. Elle va agréger les données issues de marquage passif (numéro de série ou de lot, QR code, datamatrix, SSCC, etc.), de systèmes de gestion (ERP, WMS, etc.) et d'objets connectés. Agrégées sur l'ensemble de la *supply chain* (chaîne d'approvisionnement), ces données vont permettre d'en analyser le fonctionnement pour détecter des anomalies ou des incohérences révélatrices de fraudes, mais aussi pour effectuer des analyses d'impact. Ainsi, agréger des données de capteurs, de localisation, d'expédition et de réception, peut permettre de réduire les pertes liées à des ruptures de la chaine du froid sur des trajets en camion, et d'en analyser automatiquement les causes et les responsabilités [23].

Au total, ceci dessine, pour un coût assez limité, eu égard aux enjeux, une traçabilité adaptée à l'échelle des *supply chains* modernes : en temps réel, totalement numérisée, évolutive, bout en bout plutôt que ponctuelle.

Extension du domaine de la traçabilité

Mais les objets connectés ne sont pas uniquement des sources pour la traçabilité, ils en sont aussi des sujets. Une voiture moderne est désormais avant tout un ordinateur avec des roues : Tesla pousse cette logique à l'extrême en permettant que la puissance moteur soit augmentée par une simple mise à jour logicielle [24]. Or une telle mise à jour modifie les caractéristiques de la voiture, et donc fait partie de sa chaine d'approvisionnement. Ceci se passant «*over the air*», on en perçoit assez peu la matérialité, les effets peuvent être importants, soulevant de nouvelles questions de responsabilité.

À l'été 2021, une mise à jour du logiciel embarqué de caméras de surveillance a permis à des utilisateurs d'accéder au flux vidéo d'autres personnes, c'est-à-dire à la surveillance de maisons qui n'étaient pas les leurs [25]. En 2019, des chercheurs ont montré comment utiliser les déficiences de contrôle des mises à jour d'applications pour les enceintes connectées Google Home et Amazon Alexa, pour en prendre le contrôle et par exemple écouter ainsi des conversations [26]. Enfin, en décembre 2020, une mise à jour de Google User ID Service a bloqué l'accès à Google Home pour de nombreuses personnes qui se sont retrouvées sans lumière, parfois enfermées chez elles avec des bébés ou enfermées dehors sans pouvoir rentrer [27].

L'utilisateur d'un objet connecté est confronté à des modifications plus ou moins visibles de son bien ou des services *cloud* sur lesquels ce bien repose. Ces mises à jour peuvent avoir des impacts significatifs sur le fonctionnement du bien, y compris des impacts vitaux. Si le moteur d'une voiture nécessite une mise à jour, que se passe-t-il si cette mise à jour est déclenchée de manière intempestive pendant que le véhicule roule ? Que se passe-t-il si une mise à jour indispensable pour la sécurité d'un véhicule est refusée par le propriétaire ? Le véhicule doit-il même démarrer ? Que se passe-t-il si (ou plutôt quand) une mise à jour permet le contrôle d'une voiture, voire de millions de véhicules simultanément par un tiers ? Dans chaque cas, qui est responsable en cas d'accident ou de dommages ?

(23) https://www.tilkal.com/post/traçabilité-donner-une-nouvelle-dimension-à-la-collecte-de-données
(24) https://electrek.co/2019/10/24/tesla-increase-vehicle-power-range-software-update/
(25) https://www.01net.com/actualites/un-bug-a-rendu-les-flux-videos-de-cameras-de-surveillance-eufy-accessibles-a-d-autres-utilisateurs-2042838.html
(26) https://www.futura-sciences.com/tech/actualites/objets-connectes-alexa-google-home-nouvelles-failles-exploitees-pirates-vous-ecouter-68518/
(27) https://www.bloomberg.com/news/newsletters/2020-12-16/google-outage-reignites-worries-about-smart-home-without-backups

En fait, ces mises à jour logicielles sont des évènements de production industrielle. Ils seront l'objet de l'équivalent des rappels, des fraudes et de la contrefaçon de leurs *alter ego* physiques. Il n'y a aucune raison de penser qu'ils en soient exempts ni que l'ampleur soit moindre : à l'évidence, même les entreprises les plus avancées dans le numérique ne sont pas à l'abri. Bien plus, l'absence notoire de sécurité sur beaucoup d'objets connectés quotidiens multiplie les risques d'attaques (prise de contrôle à distance, mise en marche ou arrêt indus, introduction de dysfonctionnements, verrouillage contre rançon, etc) [28]. Or les conséquences peuvent avoir une ampleur dramatique compte tenu de la facilité de diffusion d'une mise à jour logicielle.

Conclusion

Si l'on considère des objets connectés dans une configuration figée, ils contribuent à la numérisation de la traçabilité des autres biens, de la production à la distribution. Leurs enjeux de responsabilité peuvent être abordés sous l'angle de la prise de décision par un objet autonome, à l'instar du test Moral Machine du MIT (Massachusetts Institute of Technology) [29].

Mais dès qu'il y a du logiciel, aucun état n'est figé. Tout objet connecté va voir sa structure logicielle, ou celle du système qui le supporte, modifiée pendant l'utilisation, donc bien après sa distribution. Un peu comme si le cadre carbone d'un vélo pouvait être transformé en cadre acier après son achat. Ceci induit sans doute une extension de la traçabilité des objets connectés, nécessitant d'y inclure aussi bien les mises à jour que les décisions des propriétaires ou des utilisateurs de ces biens vis-à-vis de ces mises à jour. Se pose ensuite la question de garantir cette traçabilité contre toute altération et de la rendre accessible à tout moment, à l'utilisateur tout comme à un enquêteur ou un juge, afin d'établir la chaine de responsabilité.

(28) https://www.futura-sciences.com/tech/actualites/securite-attaques-objets-connectes-explosent-2019-54695/
(29) https://www.moralmachine.net

L'usage des objets communicants dans le monde des entreprises électriques

Par **Vincent AUDEBERT**
EDF R&D, France

Une longue histoire

Du fait de certains de leurs ouvrages, tels la production hydroélectrique logée le long d'une vallée ou le réseau de distribution s'étalant sur un département, les électriciens se sont rapidement intéressés à faire communiquer leurs équipements.

Bien sûr, à la fin des années 1980, début des années 1990, les termes employés étaient différents, on faisait de la télésurveillance, des télécommandes, voire de la télégestion. Et le minitel était une interface homme-machine très courante pour paramétrer les systèmes.

La mise en place de ces systèmes était complexe, demandait des ingénieurs qualifiés pour maitriser les différents composants de la chaine, suivait le plus souvent des standards d'entreprise et quelques normes internationales émergentes. Et dès qu'il fallait créer un système similaire pour une autre application, tout était à refabriquer.

C'est pourquoi il n'y a pas eu de multiplication de la diversité de ces objets communicants sur ces trente dernières années : il fallait multiplier les systèmes et les ingénieurs, mais ça n'a pas empêché le système électrique de continuer à bien fonctionner.

Une évolution de fonctionnement

La communauté européenne dans sa lutte contre le changement climatique a lancé depuis plusieurs années un grand plan pour promouvoir l'installation d'énergies renouvelables. Les réseaux qui étaient conçus à l'origine pour acheminer de l'électricité depuis quelques gros centres de production vers les consommateurs ont vu leur utilisation modifiée. Des systèmes de génération d'électricité, beaucoup plus petits, par exemple quelques kW (kilowatts) de panneaux photovoltaïques, sont installés jusque chez les clients particuliers. Il y a aussi des systèmes éoliens de plus grosse capacité, quelques MW (mégawatts), qui sont installés et raccordés sur le réseau HTA (haute tension A). Tout ceci crée de la production d'électricité qui peut, dans certains cas, utiliser le réseau dans un sens non conventionnel.

Une autre caractéristique de ces générateurs distribués, c'est qu'ils n'ont pas une production pilotable : ils sont liés à la présence de soleil et de vent. Afin de retrouver de la flexibilité pour pouvoir à tout moment produire autant d'électricité que ce qui est consommé, les électriciens ont travaillé sur la modulation de la demande, vu que le niveau de production de ce type de production est fixé par des éléments extérieurs. Il faut donc pouvoir inciter les consommateurs à faire évoluer leur niveau de consommation dynamiquement. Cette possibilité étant renforcée par de nouveaux usages comme les batteries et les véhicules électriques. Pour une description plus approfondie des *smart grids*, on pourra se référer à la publication Enedis [(1)].

Cette évolution du système électrique peut être facilitée par des objets communicants.

(1) https://www.enedis.fr/sites/default/files/documents/pdf/2021-01/smart-grids-innovation-au-service-des-clients-et-enjeux-energetiques-des-territoires.pdf

L'objet communicant emblématique des électriciens : le compteur électrique

Depuis le début des années 1990, tous les compteurs qui ont été conçus pour le marché français étaient communicants. On trouve une communication locale pour pouvoir recueillir les informations de comptage depuis l'extérieur des logements, une autre communication locale pour fournir des informations aux clients et pour les modèles à destination des clients industriels et tertiaires, et une communication utilisant le réseau téléphonique commuté.

À partir des années 2000, les solutions permettant de relever à distance les compteurs se sont généralisées dans le monde, par exemple avec le plan Obama aux États-Unis. En France, c'est le compteur Linky qui, fin 2021, sera déployé à 35 millions d'unités.

La caractéristique de tous ces déploiements mondiaux, c'est qu'ils sont, à leurs débuts, encore sur le schéma classique de systèmes spécifiques. Le fait que le nombre de points terminaux soit très important, se comptant en centaines de milliers, voire millions d'unités, permet de mobiliser les nombreux ingénieurs requis sur ces projets. Les progrès faits dans le domaine de la normalisation autour des systèmes de comptage, grâce aux travaux des comités techniques 13 et 57 de la Commission électrotechnique internationale ainsi qu'à l'organisation non gouvernementale DLMS User Association, facilitent la conception.

Tour d'horizon des écueils autour des objets communicants

Comme présenté précédemment, les objets communicants au service des électriciens, c'est une longue histoire, et la profession sait donc que ça fonctionne. Cependant, on n'a pas vu de déploiements massifs de ces nouveaux objets dans la communauté électrique, ni d'ailleurs parmi les autres verticaux, depuis les prévisions mirifiques du milieu des années 2010 (voir celles de Machina Research [2]).

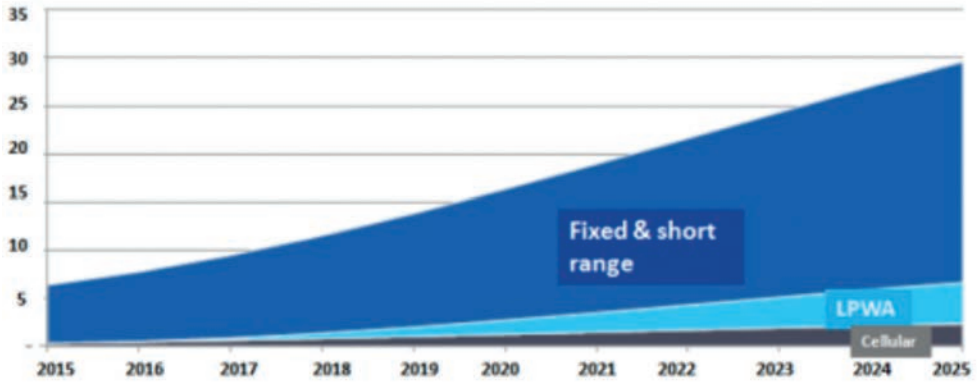


Figure 1: Évolution du nombre d'objets connectés dans le monde (Source : IOT Global Forecast Analysis)

Ce qui va être demandé aux objets communicants, c'est d'apporter de la valeur sur des métiers existants. Il faut donc pouvoir les intégrer avec les solutions existantes et non pas re-créer un nouveau système parallèle. De plus, comme ces objets vont être nombreux et divers, il faut pouvoir mutualiser leur gestion, afin de mobiliser moins d'ingénieurs pour leur mise en œuvre.

(2) https://fr.scribd.com/document/414161131/2016-08-03-Iot-Global-Forecast-Analysis-2015-2025

Leur gestion se doit d'être sécurisée, aussi bien à l'installation que sur le temps long, car l'une des particularités des électriciens est de travailler avec des équipements qui vont fonctionner plusieurs dizaines d'années.

Il va donc falloir s'appuyer sur des systèmes les plus découpés possibles pour permettre aux différents éléments d'évoluer selon les besoins, en utilisant un maximum de normes et standards.

On peut voir ci-dessous un schéma global tel que proposé par le groupe EDF en 2019.

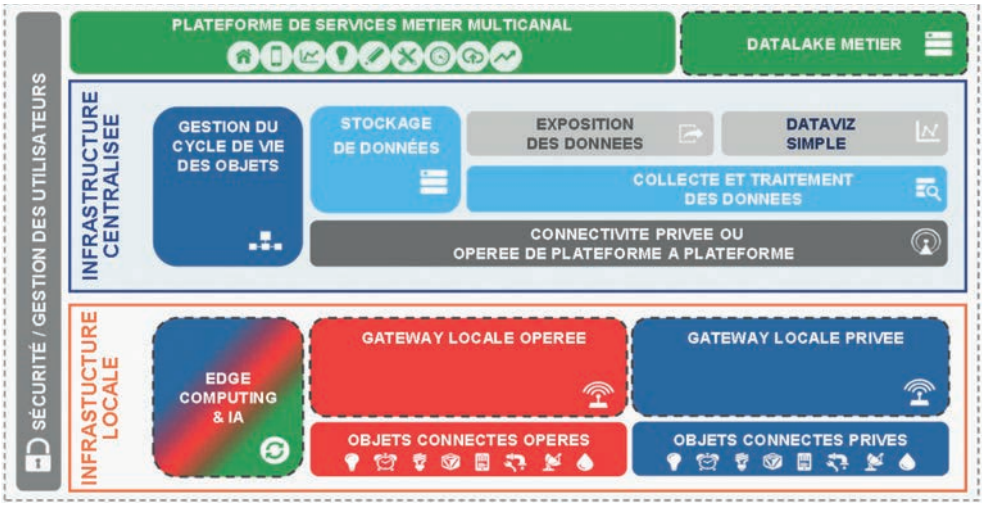


Figure 2 : Exemple d'architecture de plateforme IoT (Source : EDF 2019)

On y remarque un point qui n'a pas été abordé jusqu'à présent : les objets communicants évoluent vers des systèmes intelligents, où l'intelligence peut être répartie tout le long du cheminement de la donnée : dans l'objet, dans une passerelle, dans le réseau de communication, jusqu'au *cloud*. La gestion de tous ces niveaux de *edge computing* (ou informatique en périphérie de réseau) ajoute encore de la complexité au système technique présenté, car les standards pour gérer cette informatique sont balbutiants.

Certains cas d'usages peuvent être très coûteux à faire évoluer en cas de mauvais choix technologiques. Un objet de suivi de positionnement peut être facilement remplacé lors du retour de l'équipement sur un entrepôt alors qu'un équipement enfoui sur le terrain sera coûteux en temps en cas de remplacement par suite d'un mauvais choix technique. Ce critère de facilité d'évolution en cas de souci peut expliquer pourquoi certains cas d'usages prometteurs ne dépassent pas le niveau du pilote.

La gestion d'un accès local sécurisé et standardisé sur les objets à seules fins de mise à jour ou calibration est aussi un problème à prendre en compte. L'arrivée du standard ACE-OAuth [3] de l'IETF (Internet Engineering Task Force qui élabore et promeut des standards Internet) pourra aider.

Potentiel pour des objets communicants dans le monde des électriciens

Comme toute entreprise industrielle avec des équipements qui s'étendent sur de larges zones et du personnel technique pour les installer et les entretenir, les entreprises du domaine électrique sont intéressées par l'apport des objets communicants.

(3) https://datatracker.ietf.org/doc/draft-ietf-ace-oauth-authz/

Les objets communicants pour améliorer l'exploitation

On va trouver dans cette catégorie les objets qui par leurs données ou actions permettent d'optimiser le quotidien de certains métiers. Par exemple : ajouts de capteurs permettant de connaitre les niveaux de neige, les niveaux d'eau aussi bien dans une rivière que dans un ouvrage avec risques d'inondation, les transits énergétiques dans les câbles électriques, la présence d'un défaut sur un réseau électrique HTA, la localisation d'un matériel mobile et son état (touret de câble, groupe électrogène, outils industriels).

Les objets communiants pour améliorer la maintenance

Cette catégorie d'objet vise en priorité à connaitre l'état d'un équipement pour pouvoir réaliser la maintenance au meilleur moment. Il peut d'agir d'un boitier pour surveiller les transformateurs HTB/HTA, des nombreux capteurs non intrusifs qui portent sur les multiples moteurs électriques des installations industrielles en mesurant leur consommation électrique, les vibrations ou les sons émis par ces équipements. L'intelligence de traitement peut être intégrée au capteur, déportée sur une passerelle, voire même dans le *cloud*.

Les objets pour sécuriser et augmenter les intervenants

Les électriciens peuvent aussi bénéficier des objets communicants, avec des vêtements ou équipements de protection communicants. Par exemple : des détecteurs de proximité de réseau électrique, des dispositifs de sécurité permettant de rester en communication avec sa base ou son équipe en cas de travail isolé. Il y a aussi des solutions d'assistance à distance utilisant des lunettes équipées de caméras, voire des solutions de réalité augmentée.

Les objets communicants du monde connexe

Comme présenté précédemment, les électriciens ont de plus en plus besoin d'interagir avec les équipements au-delà du compteur, pour assurer de la flexibilité au système électrique. Les écosystèmes de la maison intelligente et du véhicule électrique, de par leur capacité à moduler leur consommation en allant même jusqu'à produire de l'énergie sur le réseau, doivent être pris en charge. Ici, un nouveau défi attend les électriciens : autant les objets issus du monde industriel en ligne avec les métiers pouvaient s'intégrer dans des systèmes existants en utilisant des normes et standards habituels, autant ces nouveaux domaines se sont construits sur leurs propres standards, nécessitant des passerelles pour faire fonctionner les solutions de bout en bout. Des travaux sur des ontologies communes sont en cours pour faciliter une gestion sans coutures de la flexibilité sur les réseaux électriques.

Deux exemples d'objets communicants du monde électrique

Comment connecter un manomètre ?

Figure 3 : Lecteur de manomètre (Source : D. R.)

On souhaite remplacer la lecture manuelle de manomètres par un système automatique. Ça ne semble pas compliqué, des systèmes de mesure de pression communicant sur pile existent. Oui, mais le système des manomètres suit une règlementation des plus strictes qui ne permet pas leur remplacement simplement. Alors, on va pouvoir opter pour un capteur qui va lire le manomètre grâce à une intelligence embarquée, puis transmettre la valeur interprétée au système d'information.

C'est ce que fait le produit de la société Cypress, déjà utilisé aux États-Unis.

Suivre les condamnations et consignations d'ouvrages

On cherche un objet qui permet de s'assurer qu'un équipement est bloqué dans l'état prévu. On va utiliser pour cela un cadenas à câble, qui auto-surveille son état (détérioration du câble, ouverture intempestive) et peut être supervisé à distance. Le système offre aussi la possibilité de vérifier qu'il est posé sur le bon équipement, grâce à une communication locale par QR code ou RFID (Radio Frequency IDentification) avec la tablette de l'intervenant et le cadenas avec une communication BLE (Bluetooth Low Energy).

Ce type de produit commence à arriver sur le terrain, comme, entre autres, celui de la société française Ineo-sense.

Figure 4 : Cadenas connecté (Source : D. R.)

Conclusion

Les progrès réalisés par l'électronique permettant d'avoir des capteurs autonomes, embarquant de l'intelligence, des réseaux de communications spécialisés pour envoyer quelques bits par jours tels LoRaWAN et de la vidéo en temps réel avec la 5G favorisent l'arrivée d'objets communicants dans le monde de l'électricité. IRENA (Agence internationale pour les énergies renouvelables) en prévoit 75 milliards en 2025 [4].

L'émergence de normes et standards rassure quant à l'exploitabilité sur le long terme.

Ceux-ci permettront à l'écosystème autour des entreprises électriques de mieux appréhender les défis de la décarbonation de l'économie.

(4) https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Sep/IRENA_Internet_of_things_2019.pdf

Les objets connectés dans les missions judiciaires

Par **François BOUCHAUD**
Capitaine de gendarmerie, Centre de lutte contre les criminalités numériques (C3N) au sein du Commandement de la gendarmerie dans le cyberespace (ComCyberGend)
Et **Thomas VANTROYS**
Maître de conférences à l'Université de Lille et membre du laboratoire CRIStAL (UMR 9189) et de l'IRCICA (USR 3380)

La généralisation des technologies de l'information interactives dans le quotidien constitue, avec la prolifération des objets intelligents communicants, un enjeu d'actualité dans le cadre des missions judiciaires. Peu visibles, à l'exception des plus populaires d'entre eux comme, entre autres, les montres connectées, ces derniers s'invitent et participent à notre quotidien. Tous les secteurs d'activité sont touchés par cette numérisation accélérée. L'Internet des objets, IdO (en anglais, IoT), suscite aujourd'hui autant de promesses d'opportunités économiques, sociétales et judiciaires que de questions, voire d'inquiétudes, certaines de portée stratégique. Dans cet article, nous exposons les opportunités offertes par les objets connectés dans le cadre des missions judiciaires. Nous nous intéressons également à quelques-unes des nouvelles menaces liées à l'usage et au déploiement de ces écosystèmes.

Les objets connectés, de nouvelles opportunités pour les forces de sécurité

La révolution de l'IdO permet aux objets de la vie quotidienne d'intégrer une multitude de capteurs et d'actionneurs. La multiplication et la massification de ces équipements entraînent une numérisation du réel. Le numérique se superpose et interagit avec le monde physique. Les objets connectés scrutent et interfèrent avec notre quotidien. Ils génèrent une grande diversité d'informations : des données d'utilisateurs, de contexte, de système, des logs de fonctionnement, etc. L'accroissement des objets déployés amène à un volume total d'informations échangées extrêmement élevé. Les données collectées constituent une nouvelle manne économique. Elles sont l'« or noir » du XXI^{e} siècle. Ainsi, tous les deux ans, la volumétrie des données générées par l'Internet des objets double la taille de l'univers numérique, il est estimé en 2020 à 44 000 milliards de giga-octets (Cosquer, 2016). L'horizon de l'Internet des objets dans un écosystème numérique, désormais global, ouvre à d'importants enjeux et à des promesses d'opportunités pour le renseignement, la conduite opérationnelle, l'investigation judiciaire et la défense. Ces données participent également à l'innovation dans la création de services personnalisés, en réponse aux besoins actuels et futurs. Ainsi, ce phénomène bouleverse les frontières traditionnelles. Il révolutionne les chaînes de valeur de l'entreprise et l'organisation territoriale. La limite entre le virtuel et le réel est en passe d'être abolie. Elle s'inscrit dans une logique de *continuum* cyberespace-espace physique (Hazane, 2018).

Les objets connectés inscrits dans l'infrastructure de l'IdO créent une donnée longitudinale qui propose non seulement de pouvoir identifier et de fournir tous les éléments matériels nécessaires à la manifestation de la vérité judiciaire, mais offre également des champs à la prévention et à

l'analyse des phénomènes. Le croisement des traces autorise des recoupements d'informations et des investigations inédites. La presse internationale se fait l'écho de plusieurs enquêtes criminelles incorporant des écosystèmes connectés. Des enquêteurs du Merseyside (Royaume-Uni) ont exploité les logs de fonctionnement et les données de géolocalisation d'une montre sportive GPS dans la résolution de l'affaire Paul Massey (Thomas, 2019). Les informations recueillies ont permis de reconstruire la chronologie des évènements survenus et de qualifier l'infraction en mettant en avant une préméditation du fait criminel. En Arkansas (États-Unis), l'appareil Amazon Echo a servi de témoin dans un meurtre en enregistrant les bruits ambiants (Chavez, 2017). Dans l'affaire Anthony Aiello en Californie (États-Unis), la correspondance entre les données du bracelet connecté de la victime et les informations du système domotique a permis de confondre le meurtrier en contextualisant le crime (Cassidy, 2018). L'objet connecté détourné de son usage premier offre des informations inédites pour l'investigation judiciaire. C'est notamment le cas des thermostats connectés disposant de facultés d'apprentissage. Couplés à l'écosystème de la maison, ces équipements sont en mesure de déclencher des actions automatiques tel l'allumage du chauffage lorsque le téléphone est reconnu dans un champ proche. Cette information est exploitable pour reconstituer la chronologie des événements révolus, et déterminer des présences ou des déplacements dans un périmètre donné. L'objet connecté est la face visible et locale de l'infrastructure de l'Internet des objets, porte d'entrée des investigations judiciaires. La recherche, l'identification et l'analyse de cet élément catalyseur sont primordiales pour comprendre l'architecture globale et obtenir une information pertinente au regard de l'enquête. L'enquêteur doit être en mesure d'associer à un phénomène criminel et sa donnée, un dispositif physique. Il doit ainsi comprendre le parcours de l'information dans l'architecture connectée, de son initialisation à son interception. Cette perception oriente les investigations et les actes techniques dans l'obtention de preuves pour le procès pénal. La valeur ajoutée de l'Internet des objets vient du fait que le tout est plus grand que la somme des parties, ce qui explique que les approches unité par unité passent à côté de la valeur ajoutée de l'IdO (Bouchaud, 2021).

L'identification des objets et leur caractérisation technique sont la clef de voûte pour l'extraction et l'étude de l'information pertinente. Or, la diversité d'usage, de fonctionnement dans la remontée et la synchronisation de l'information, l'hétérogénéité des objets interdépendants rendent jusqu'à présent ce travail d'investigation très chronophage et fastidieux en l'absence d'une approche intégrale d'analyse. Parcellaire dans un objet, la donnée prend son sens dans l'architecture globale. Comment appréhender avec intelligence les objets et leur environnement de connexion dans un contexte judiciaire ? Comment accéder à ce gisement d'information eu égard aux nombreuses dépendances, aux liens cachés, à sa dispersion et à sa fragmentation dans l'infrastructure connectée ? Quelle crédibilité donner aux traces recueillies et reconstruites ? Sont-elles fiables et robustes pour l'enquête, et donc présentables devant une cour de justice ?

L'interception des données sensibles par l'exploitation des failles de sécurité des appareils connectés et des données systèmes s'avère primordiale pour l'investigation. L'authentification des agents communicants, l'exploitation et la contextualisation des données à des fins d'analyse, le croisement entre les informations recueillies, le contrôle de l'exposition des données nécessitent en effet une amélioration continue des techniques d'expertise. Pour l'investigation judiciaire, il s'agit d'anticiper l'apparition de nouvelles formes de criminalité, de gagner en agilité et en fiabilité, et dès lors répondre à la demande croissante d'expertise. L'objectif est également de limiter les usages impropres qui pourraient être faits à partir des données. L'expert criminel en nouvelles technologies doit s'assurer du maintien de l'intégrité et de la qualité des données, de la collecte des éléments matériels pertinents à leur présentation devant une cour de justice. Or, la collecte des données se heurte à plusieurs difficultés : ces données numériques sont souvent dispersées et rendues anonymes, contraintes par des politiques propres de gestion. Leurs manipulations à des fins d'exploitation ou de conservation s'avèrent difficiles et les rendent sujettes à de potentielles

altérations. Il est de plus essentiel de réaliser le chaînage des données pour obtenir une lecture de l'information lisible.

Ce constat est également applicable à la collecte d'information dans le cadre du renseignement. Un rapport publié le 1er février 2016 par le centre de recherche Berkman de l'université Harvard (Gasser, 2016) estime que la quantité de données rassemblées par les objets connectés en fait l'une des pistes privilégiées pour que les agences de renseignement puissent contourner les protections mises en place sur les moyens de communication « classiques ». En 2016, James Clapper, directeur du renseignement national des États-Unis, a déclaré lors d'une audition devant le Sénat américain : « À l'avenir, les services de renseignements pourraient tirer parti de l'Internet des objets pour identifier, surveiller ou localiser des suspects, découvrir des indicateurs potentiels, ou obtenir des mots de passe » (*Le Monde*, 2016).

Une nouvelle source de menaces à l'échelle internationale

Une nouvelle porte d'entrée dans les systèmes d'information

L'utilisation croissante des objets connectés a de fortes implications en matière de sécurité et de confidentialité des données échangées. Les dispositifs détournés par malveillance de leurs usages premiers introduisent de nouveaux risques, des menaces d'atteintes numériques et économiques. Le cas récent d'un vol de données provenant du système d'information d'un casino aux États-Unis, passant par un thermomètre connecté d'aquarium, illustre ce phénomène grandissant (Williams-Grut, 2018). L'environnement connecté se transforme en un vecteur criminel : de façon accessoire en facilitant la commission d'une infraction, de manière principale lorsqu'elle se rapporte au contenu ou bien en constituant son objet. Concrètement, cette singularité cybercriminelle se traduit de plusieurs manières : par des perturbations du fonctionnement nominal d'un dispositif connecté en l'empêchant de transmettre des données, par la prise de contrôle logique ou physique de l'environnement connecté en le détournant de son usage premier, et/ou par un accès illégal aux informations échangées ou stockées en portant atteinte aux données personnelles. Pour les entreprises, il s'agit de préserver la confiance des clients en garantissant la confidentialité des données personnelles, la sécurité des transactions, la protection à l'égard des logiciels malveillants et des attaques informatiques.

À ces risques identifiés s'ajoutent la maîtrise et la supervision d'un parc d'objets en cohérence avec les habitudes et les usages de consommateurs de services. En effet, la facilité de déploiement et d'utilisation des objets connectés devient un nouveau défi pour les administrateurs des systèmes et des réseaux d'entreprise. Un déploiement anarchique de solutions par des salariés occasionne des perturbations des réseaux existants. La question de la détection et de l'identification des objets connectés devient donc un élément central pour garantir la sécurité des systèmes d'information.

Par ailleurs, la mise en péril de la santé publique ou d'un écosystème est également réelle s'agissant d'appareils dont l'utilisation a un lien direct avec la santé ou la sécurité. Ces menaces sont amplifiées par la diffusion et la massification accélérées de dispositifs composites dans un écosystème anarchique non régulé et non réglementé. Cet environnement informatique souffre d'une insuffisance de vision globale en matière de sécurité (*security by design*). Une récente étude de la société Palo Alto Networks révèle ainsi que 98 % du trafic des objets connectés utilisés dans un environnement professionnel ne sont pas chiffrés et 57 % d'entre eux comprendraient des vulnérabilités (Unit 42, 2020), générant un risque systémique préfiguré par le *botnet* Mirai (2016). En effet, l'absence de standards de sécurité, l'hétérogénéité des protocoles et des technologies utilisés, le manque de bonnes pratiques en matière de conception, notamment dans le maintien en condition de sécurité ou la mise à jour des *firmwares* des objets déjà déployés génèrent des risques élevés. Ainsi, les objets connectés sont vulnérables et sujets à des actions malveillantes pouvant mener à des menaces sérieuses pour une société hyperconnectée.

Une diversification d'usages

Les objets connectés sont hétérogènes dans leur nature, leur usage et leur fonctionnement. Les phénomènes du « fait maison » (*maker kit*) et du "DIY" (*Do It Yourself*) se développent. Ils passent notamment par la transformation d'éléments divers en objets connectés par l'apposition de moyens de communication. Ainsi, les appareils ne sont pas toujours reconnaissables. Certains dispositifs demeurent cachés dans leur environnement et émettent une faible signature. Nous pouvons citer l'exemple d'une caméra embarquée dans un ours en peluche ou celui d'un déodorant contenant un système de stockage Wi-Fi avec des données à caractère pornographique mettant en scène des mineurs. Ces situations rencontrées proviennent de perquisitions domiciliaires.

Un autre phénomène réside dans le détournement de l'usage initial, notamment pour cacher des agissements. Le cas du réseau de communication sans infrastructure, développé lors des manifestations à Hong Kong en 2014 (Dunand, 2014), en est une illustration. Cette structuration de l'espace numérique s'appuie sur une application exploitant un réseau Bluetooth. L'usage des technologies de communication, détournées de leur fonction primaire, se meut en nouvelles solutions ou services.

La proximité entre l'objet et l'humain pose des interrogations sur le potentiel destructeur du premier dans le cadre d'un piratage d'une infrastructure connectée par un individu ou par un groupe aux intentions hostiles ou malveillantes. À ce phénomène, les objets ouvrent de nouvelles surfaces d'attaque pour intercepter des informations dans une logique de « guerre électronique ». L'utilisation de données personnelles ou de fonctionnement transitant sur les réseaux sans l'autorisation des propriétaires est la norme et complexifie la donne. Néanmoins, le risque est maîtrisable par une connaissance fine des systèmes et de leur fonctionnement.

Conclusion

L'importance des objets connectés dans le cadre des missions judiciaires n'est plus à démontrer. En tant que témoins de nos activités quotidiennes, ils sont des sources riches d'informations dans la recherche de la vérité et la résolution des enquêtes. Ces traces numériques soulèvent cependant de nombreuses questions, notamment dans l'appréhension de l'écosystème avec pertinence : son identification, la collecte et l'analyse de l'information au regard d'un contexte. Cette démarche passe par la sensibilisation, l'acculturation et la formation des acteurs cyber, notamment par l'apprentissage d'actes réflexes ainsi que par la production de solutions techniques pour le primo-intervenant et le technicien du numérique. Face à la dispersion de la donnée entre cyberespace-espace physique et la pluralité des écosystèmes, la démarche d'investigation est nécessairement coordonnée et structurée.

Les objets connectés sont également des facteurs externes à prendre en considération dans un raisonnement tactique pour le succès d'une intervention et d'une mission. En effet, une manœuvre et son effet majeur peuvent être compromis par ce type de dispositifs et l'externalisation de la donnée. Ces équipements constituent une contrainte dans la recherche d'une discrétion ou d'un élément de surprise lors d'une progression. Détournés de leurs usages premiers, les objets connectés sont susceptibles d'attenter à la vie des unités d'intervention. Il est donc primordial pour les acteurs d'identifier en amont les dispositifs, afin d'adapter une réponse opérationnelle satisfaisante à la menace.

Bibliographie

BOUCHAUD F. (2021), *Analyse forensique des écosystèmes intelligents communicants de l'Internet des objets*, thèse de doctorat, Université de Lille.

CASSIDY M. (2018), "Fitbit offers key clue to slain San Jose woman's alleged 90-year-old killer", https://www.sfchronicle.com/crime/article/Fitbit-offers-key-clue-to-slain-San-Jose-13266777.php

CHAVEZ N. (2017), "Arkansas judge drops murder charge in Amazon echo case", https://edition.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html

COSQUER C. & LANCKRIET J. (2016), « Les objets connectés et la défense », *Revue défense nationale*, N° 787, pp. 97-103.

DUNAND C. A. (2014), « À Hong Kong, les manifestants adoptent FireChat pour communiquer sans réseau », https://www.lesechos.fr/30/09/2014/lesechos.fr/0203817723785_a-hong-kong--les-manifestants-adoptent-firechat-pour-communiquer-sans-reseau.htm

GASSER U., GERTNER N., GOLDSMITH J. L., LANDAU S., NYE J. S., O'BRIEN D., OLSEN M. G., RENAN D., SANCHEZ J., SCHNEIDER B. *et al.* (2016), *Don't panic: Making progress on the "going dark" debate*, Berkman Center Research Publication.

HAZANE E. (2018), « Sécurité numérique des objets connectes, l'heure des choix », https://www.frstrategie.org/sites/default/files/documents/publications/notes/2018/201815.pdf

LE MONDE (2016), « Le directeur du renseignement américain reconnaît s'intéresser aux objets connectés », https://www.lemonde.fr/pixels/article/2016/02/10/le-directeur-du-renseignement-americain-reconnait-s-interesser-aux-objets-connectes_4862587_4408996.html

THOMAS J. (2019), "How police unmasked 'Iceman' assassin behind one of Britain's most notorious gangland murders", https://www.liverpoolecho.co.uk/news/liverpool-news/how-police-unmasked-iceman-assassin-15649613

UNIT 42 (2020), "IoT Threat Report", https://unit42.paloaltonetworks.com/iot-threat-report-2020/

WILIAMS-GRUT O. (2018), "Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank", https://www.businessinsider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4?IR=T

Les protocoles de l'Internet au service de l'interopérabilité de l'Internet des objets

Par **Marianne LAURENT**
Directrice marketing au sein de la start-up Acklio
Alexander PELOV
Président et cofondateur d'Acklio
Et **Laurent TOUTAIN**
Professeur associé au département Systèmes réseaux, Cybersécurité et Droit du numérique de l'IMT-Atlantique

L'Internet des objets (IoT) est un des piliers des transformations numériques, énergétiques et industrielles du XXIe siècle. Il définit un monde multi-connecté, multipliant nos sources d'information pour piloter nos processus par la donnée. Le I de IoT sous-entend que l'Internet des objets serait une extension de l'Internet à de nouveaux objets communicants entre eux et avec le réseau. Pourtant, la déferlante attendue de milliards d'objets repose sur des ruptures majeures avec le modèle de l'Internet classique, impliquant des compromis qui soulèvent des défis d'interopérabilité et de pérennité des solutions.

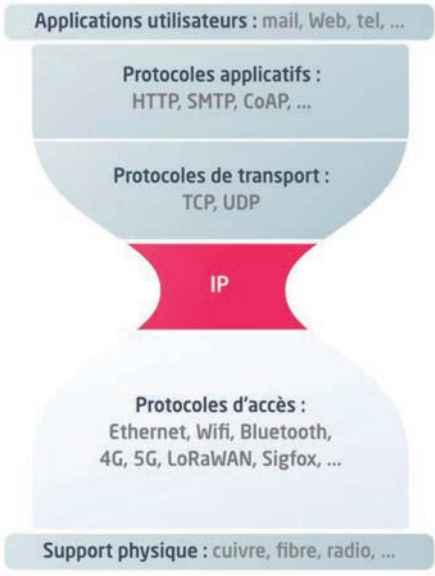
IP : protocole d'interopérabilité universel

Internet connaît une croissance exponentielle depuis la connexion des deux premiers ordinateurs en 1969. Ce succès à l'échelle planétaire repose sur deux grands principes architecturaux. D'abord, le principe de reconfiguration automatique permet au réseau de croître à l'infini, en adaptant sa topologie à chaque entrée ou sortie d'un équipement dans le réseau. Ensuite, le principe de bout en bout reporte un maximum de fonctionnalités vers les extrémités du réseau pour maintenir son cœur le plus simple et efficace possible.

Le principe de bout en bout repose sur IP (pour Internet Protocol). Souvent confondu avec le nom du réseau, Internet est le nom du protocole qui y assure l'adressage et le routage. Il est utilisé par toutes les applications (navigation *web*, *email*, *streaming*, etc.) et est déployé dans tous les nœuds d'Internet. Les routeurs IP font transiter les paquets, sans se soucier des technologies réseaux sous-jacentes. IP interconnecte les réseaux en toute transparence. Ainsi, l'infrastructure du réseau IP n'est rien d'autre qu'un véhicule pour le transport des données d'un bout à l'autre de la planète, fournissant des interfaces simples pour des applications « intelligentes » !

Internet est souvent représenté par une pile de protocoles en forme de sablier : le goulot d'étranglement illustre la simplicité fonctionnelle d'IP et son rôle de pivot entre les protocoles de haut niveau dédiés aux applications et les protocoles de bas niveau relatifs aux réseaux d'accès. Autrement dit, il masque les différences entre les technologies d'accès, et présente une interface de service unifiée aux applications, supprimant toute corrélation entre le support physique et son utilisation.

En mutualisant une même infrastructure à de multiples services, on réduit les coûts tout en enrichissant l'offre. C'est par exemple le cas du courrier, du téléphone ou de la télévision. Traditionnellement liés à leur réseau de distribution, sur Internet ils sont proposés dans des modèles gratuits pour un niveau de service souvent meilleur (haute définition, contenus à la



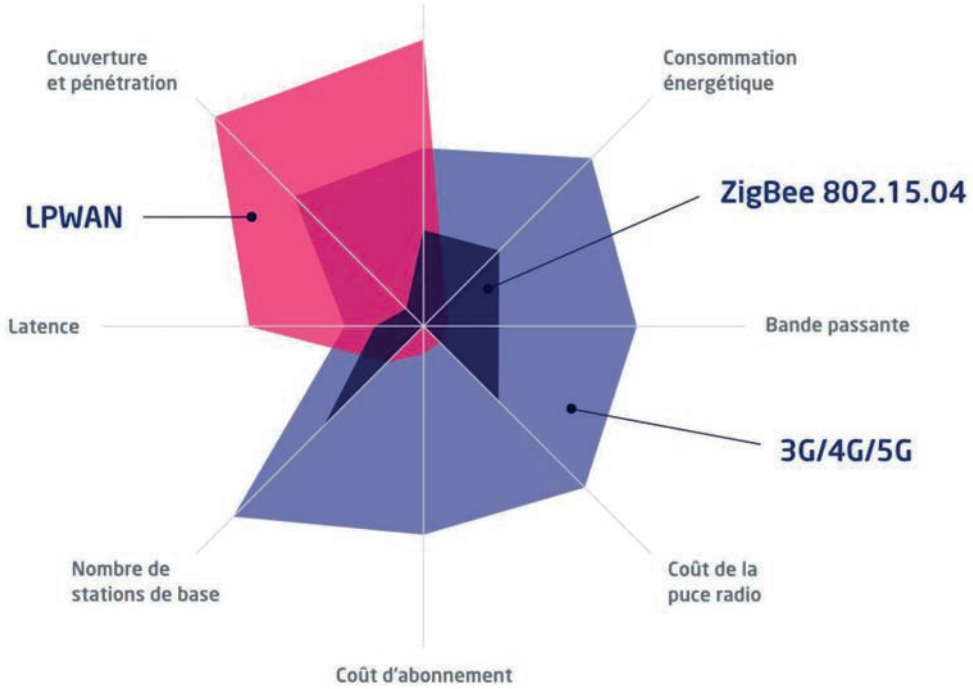
Source : D. R.

demande, archivage, multi-utilisateurs, etc.). Qui plus est, tous les développeurs maîtrisent IP et les technologies inhérentes au développement Internet. Quant à l'utilisateur final, peu importe comment Internet fonctionne, ses services lui sont désormais disponibles en mobilité, quels que soient le périphérique, la technologie d'accès ou la région du globe.

Émergence d'un IoT en rupture avec le modèle de l'Internet

LPWAN : les nouvelles connectivités réseaux IoT

L'IoT permet de capturer de l'information sur nos environnements pour optimiser nos processus, économiser des ressources ou augmenter la productivité. On peut contrôler une chaine logistique à l'aide de capteurs et actuateurs, faire dialoguer des voitures pour éviter les collisions ou améliorer les circuits de collecte des bennes de recyclage en connaissant leur taux de remplissage. Ces cas d'usages nécessitent des solutions de capture et de transmission de données à bas coût, et économes en énergie. Pour y répondre, des technologies émergent depuis une dizaine d'années : une nouvelle génération d'objets communicants, et des réseaux à longue portée et basse consommation (dits "LPWAN" pour Low-Power Wide-Area Networks).



Source : https://www.techplayon.com/low-power-wide-area-networks-lpwan/, adaptée pour Acklio

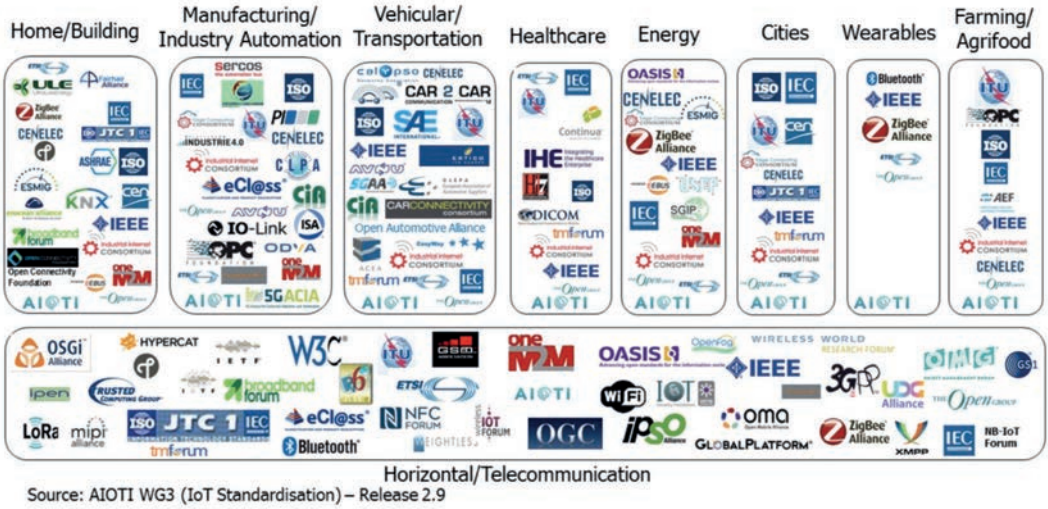
Ces derniers assurent des portées de plusieurs kilomètres et une très faible consommation énergétique aux terminaux pour des durées de vie atteignant jusqu'à dix ans sur une pile bouton. Les réseaux LPWAN complètent ainsi le paysage des connectivités IoT réunissant déjà les protocoles sans-fil courte portée (Bluetooth, Zigbee), les réseaux locaux sans-fil hérités (Wi-Fi) ou les technologies cellulaires (GSM, UMTS, LTE). Né avec l'émergence de technologies dans le spectre de fréquences libres telles que Sigfox et LoRaWAN®, l'espace LPWAN s'étoffe rapidement sur bandes de fréquences licenciées (NB-IoT et LTE-M) grâce au soutien des opérateurs de réseau mobile. Dernièrement, de nouvelles solutions satellites portées par des constellations en orbite basse offrent des couvertures mondiales.

Rupture technologique et fragmentation du marché

Mais ces avantages ont un prix. IP a été pensé pour des réseaux sans contrainte de débit, supportant des fonctionnalités non accessibles aux LPWAN du fait de leur bande passante limitée et du mécanisme de mise en veille profonde des terminaux. IP impose au réseau d'accès de prendre en charge des paquets d'au moins 1 280 octets (RFC 8376), bien au-delà des capacités LPWAN (notamment 12 octets pour Sigfox et maximum 256 pour LoRaWAN). Pour finir, IPv6 ajoute au moins 40 octets d'entêtes aux messages, soit parfois plusieurs trames LPWAN.

Ainsi, les réseaux LPWAN se sont développés en marge du monde IP, impliquant des arrangements avec le modèle du sablier. En l'absence d'IP, les services des couches réseaux et transport sont pris en charge au niveau applicatif, ou à défaut par la couche liaison. Ainsi, cette dernière est optimisée et spécifique à chaque technologie radio tandis que l'application est le plus souvent liée directement au format de trame. Il en résulte des déploiements conçus, sécurisés et exploités en silos. Sans IP, pas d'interopérabilité possible entre technologies LPWAN – ni entre elles, ni avec l'Internet. La migration d'une connectivité à une autre implique de reconstruire l'ensemble de la chaîne. Pour un projet IoT, les industriels doivent d'abord choisir la technologie d'accès, puis ajuster le choix des capteurs, des plateformes et enfin assurer l'intégration à l'architecture existante. Choisir une connectivité, c'est donc prendre un risque sur l'obsolescence, la pérennité de l'investissement, et l'utilisation simple et sécurisée des données.

Face à cette complexité, le marché de l'IoT tend à se « verticaliser » autour de solutions préconfigurées de bout en bout. Le nombre de plateformes explose (600 plateformes répertoriées



Paysage des organismes de normalisation et alliances IoT (Source : AIOTI 2019)

en 2019 [1]) soutenant indirectement des écosystèmes cloisonnés par un choix limité de protocoles, de formats de données et souvent des interfaces (API) propriétaires. En parallèle, le panorama AIOTI 2019 [2] met en évidence la nécessité de simplifier le paysage normatif IoT, foisonnant d'activités de normalisation liées aux verticales métiers et aux connectivités.

Gestion de la convergence dans les couches hautes

Face à la fragmentation du marché et à l'absence de support des couches IP dans l'IoT, l'interopérabilité est communément abordée au niveau applicatif.

Pour faire le pont entre environnements hétérogènes et raccorder des déploiements IoT à des déploiements hérités du monde IP, il est commun d'utiliser des passerelles de traduction protocolaires. Solutions logicielles ou matérielles, celles-ci peuvent parfois raccorder plus d'une dizaine de protocoles. Néanmoins, ces équipements ne sont pas transparents : ils doivent être interfacés avec l'ensemble des éléments du réseau pour re-router les messages. Chaque trame est réinterprétée au niveau de la passerelle, ce qui nuit aux performances du réseau, rend difficile le passage à l'échelle et ouvre de potentielles failles de sécurité en cassant le chiffrement de bout en bout.

Une autre solution est d'utiliser des plateformes horizontales multi-technos, qui offrent l'intégralité des fonctions nécessaires à la mise au point et à l'opération d'un service. Ces plateformes peuvent être génériques ou spécialisées, propriétaires ou standardisées. Les fournisseurs de *cloud* tels que Microsoft Azure et AWS sont des exemples pour des plateformes génériques et propriétaires. Des plateformes génériques et standardisées, telles que l'Open Connectivity Foundation (OCF) [3] et oneM2M [4], sont accompagnées par des implémentations *open-source*, parfois intégrées à des solutions propriétaires. Les plateformes spécialisées et standardisées sont liées aux cas d'usages (notamment DLMS [5] pour les compteurs électriques, KNX pour les bâtiments connectés), ou à des fonctions spécifiques telles que LightweightM2M [6] pour la gestion des modules cellulaires.

Mais si la plupart de ces plateformes s'appuient sur IP, l'échange d'information est structuré et sécurisé en fonction de chacune. Par exemple, MQTT est un protocole basé sur TCP/IP, massivement utilisé par les fournisseurs de *cloud*. Cependant, deux objets conçus pour deux *clouds* distincts ne pourront ni communiquer librement, ni changer leur *cloud* d'origine, quand bien même les deux utiliseraient MQTT/TCP/IP. D'autres approches d'interopérabilité sémantique tentent d'apporter une réponse générique comme le Web of Things du W3C [7], ou plus pragmatique comme le Semantic Definition Format de OneDM [8] et l'IETF [9], soutenu par Zigbee, OMA SpecWorks et OCF.

D'une part, l'existence de systèmes historiques et, d'autre part, la diversité des exigences liées aux cas d'usages IoT font qu'aujourd'hui, il n'existe ni *framework* ni standard universel capable de couvrir l'ensemble. Il faut donc avoir une approche pragmatique, dans laquelle on cherche à avoir une interopérabilité sur un domaine plus restreint et assurer au maximum l'interopérabilité avec les domaines adjacents.

(1) IoT Analytics (2019), "IoT platform companies landscape 2019/2020: 620 IoT platforms globally", https://iot-analytics.com/iot-platform-companies-landscape-2020/
(2) "IoT LSP standard framework concepts release 2.9 AIOTI WG03 – IoT standardisation", October 2019, https://aioti.eu/wp-content/uploads/2019/10/AIOTI-WG3-SDOs-Alliance-Landscape-IoT-LSP-standrad-framework-R2.9-Published.pdf
(3) https://openconnectivity.org/
(4) https://www.onem2m.org/
(5) https://www.dlms.com/
(6) https://technical.openmobilealliance.org/Overviews/lightweightm2m_overview.html
(7) World Wide Web Consortium, https://www.w3.org/WoT/
(8) https://onedm.org/
(9) https://datatracker.ietf.org/wg/asdf/about/

La couche IP désormais disponible aux LPWAN pour unifier les solutions IoT

On comprend donc que, quand bien même ces solutions applicatives répondent à des problématiques de convergence à petite échelle, un réseau qui fait l'économie d'IP perd de sa valeur. Silotage des solutions, coûts inhérents aux développements sur mesure et à leur évolution, dépendance aux fournisseurs et spécialisation des compétences forment un faisceau de freins pour le décollage tant attendu de l'IoT. Mais le marché gagne aujourd'hui en maturité. Des acteurs clés, ayant jusqu'ici construit leurs solutions sur des technologies propriétaires, convergent à présent sur des solutions construites au-dessus d'IP.

C'est le cas d'Amazon, Apple et Google, qui, en partenariat avec la Connectivity Standards Alliance (CSA), ont lancé l'initiative "Connected Home over IP" fin 2019 pour aligner le développement de leurs solutions domotiques sur un socle applicatif commun basé sur IP. Cette alliance nommée Matter réunit déjà près de 200 membres [(10)]. Une initiative similaire est portée par BACnet, KNX, OCF, Thread et CSA dans le bâtiment connecté. Ensemble, ils préconisent l'adoption d'une infrastructure IP sécurisée et multistandard comme épine dorsale du pilotage et de l'automatisation des bâtiments. IP-BLiS entend ainsi garantir aux gestionnaires de bâtiments une connectivité plus rapide et moins coûteuse, une meilleure intégration entre applications et un large choix de connectivités [(11)]. Tout porte à croire que cette tendance va s'accélérer et s'étendre rapidement à d'autres verticales métiers. D'ailleurs, des recherches sur la théorie des jeux ont montré que les systèmes en couche convergent invariablement vers un modèle en sablier (Akhshabi et Dovrolis, 2011).

Et pour les LPWAN ? La problématique se résume dans cette équation : appliquer les principes qui ont fait le succès de l'Internet tout en s'adaptant aux contraintes de consommation énergétique, de temps de calcul et d'échange de données. L'Internet Engineering Task Force (IETF), instance de standardisation qui définit les architectures et protocoles de l'Internet, dédie depuis 2016 un groupe de travail à la mise en œuvre d'IPv6 sur les LPWAN. Cet effort se concrétise aujourd'hui dans une suite de standards dédiés. SCHC (prononcé « chic ») pour Static Context Header Compression (RFC 8724) est un mécanisme de compression et de fragmentation qui évite la synchronisation entre les éléments d'un réseau LPWAN – opération couteuse en bande passante. Étant donné la nature hautement prévisible des flux de données en IoT, on peut décrire, partager et stocker à l'avance le contexte de communication. On allège ainsi la quantité de données transmises, tout en rendant possible l'utilisation d'IPv6 et de nombreux protocoles associés.

L'IETF apporte ainsi le principe de bout en bout aux réseaux LPWAN, en offrant une couche d'adaptation entre IPv6 et la connectivité sous-jacente. SCHC transforme un objet LPWAN en un objet IP, adressable facilement depuis n'importe quelle application Internet. En permettant d'utiliser IP de bout en bout, depuis le *cloud* jusqu'au terminal, SCHC permet une intégration sans couture avec le reste des solutions réseaux et applicatives des clients.

Pour l'IoT, c'est une nouvelle rupture qui libère les LPWAN des compromis jusqu'alors réalisés sur l'interopérabilité. Il devient possible de tirer le meilleur parti des LPWAN pour construire des solutions sur un portefeuille de connectivités variées : SCHC prend en charge l'adaptation à la couche réseau sous-jacente. Les LPWAN supportant désormais IP, on peut en bénéficier pour remplacer ou compléter des environnements hérités du monde IP. L'implémentation SCHC d'Acklio permet par exemple de déployer des compteurs électriques ou de densifier des réseaux d'automates industriels Modbus sur LoRaWAN, mais aussi d'utiliser les LPWAN comme connectivité de secours pour des routeurs IP classiques.

(10) https://buildwithmatter.com/
(11) https://www.ipblis.org

L'utilisation d'IP supprime ainsi le besoin de passerelles sur mesure pour traduire le trafic réseau d'une technologie à une autre. SCHC élimine les risques de verrouillage des fournisseurs et permet des investissements à l'épreuve du temps. Il répond spécifiquement aux besoins de l'écosystème IoT, et accélère le marché de l'IoT.

Perspectives

Internet est un ensemble de technologies qui ont permis de construire le plus grand réseau au monde et dont on ne connaît pas encore les limites. Sa simplicité fonctionnelle garantit une interopérabilité universelle des réseaux IP, leur assure une haute performance et permet d'innover au niveau applicatif pour porter un nombre croissant de services. Ces technologies répondent aussi de manière très pragmatique à des enjeux économiques et très opérationnels de délai d'accès au marché, de pérennité des solutions et de rentabilité des investissements. Mais surtout, IP est un standard ouvert, mature et omniprésent. Supporté par la plupart des systèmes d'exploitation (sinon tous), il offre une interopérabilité native avec les systèmes d'information et les infrastructures de réseau préexistantes. Simple, efficace et évolutif, IP est désormais prêt à connecter les prochains milliards d'objets communicants !

Bibliographie

AIOTI (2019), "IoT LSP standard framework concepts release 2.9 AIOTI WG03 – loT standardisation", https://aioti.eu/wp-content/uploads/2019/10/AIOTI-WG3-SDOs-Alliance-Landscape-IoT-LSP-standrad-framework-R2.9-Published.pdf

AKHSHABI S. & DOVROLIS C. (2011), "The evolution of layered protocol stacks leads to an hourglass-shaped architecture", *Actes* du colloque SIGCOMM'11.

RFC 8376, https://datatracker.ietf.org/doc/rfc8376/

RFC 8724, https://datatracker.ietf.org/doc/html/rfc8724

TOUTAIN L. (2018), « Une gouvernance pour l'Internet des Objets ? », *Enjeux numériques*, n°4, décembre, pp. 37-41.

TOUTAIN L., GIROD-GENET M. & SINGH K. (2021), « Programmer l'Internet des objets », MOOC de l'IMT Atlantique sur France Université Numérique : https://www.fun-mooc.fr/en/cours/programmer-linternet-des-objets/

WANG W. G., TOLK A. & WANG W. P. (2009), "The levels of conceptual interoperability model: Applying systems engineering principles to M&S", Spring Simulation Multiconference (SpringSim'09) *Proceedings*, San Diego, CA, USA.

Les enjeux de la 5G pour les objets connectés

Par **Cécile DUBARRY**
et **Anne-Lise THOUROUDE**
Arcep

De nombreuses technologies rendent possibles les objets connectés. Parmi celles-ci, les technologies mobiles grand public (4G, 5G…) sont largement mises en avant. Dans une acception large, les objets connectés vont de simples capteurs à des objets *high tech* : le téléphone n'est-il pas l'objet connecté le plus courant ?

Si différentes technologies (LoRa, Sigfox 4G …) permettent déjà la mise en place d'objets connectés, la 5G est souvent promue comme la technologie mobile qui entrainera un développement massif de ceux-ci. Cela s'explique par le cadre de mise au point de la 5G. En effet, la 5G, contrairement aux technologies précédentes, a été conçue dès le départ comme une technologie structurante pour l'Internet des objets (IoT). Actuellement en cours de déploiement, la 5G devrait s'enrichir au fur et à mesure de l'introduction des innovations sur les réseaux.

Les objets connectés : une connectivité déjà possible avec les technologies en place

Si on parle souvent de la 5G comme la technologie mobile rendant possible la généralisation des objets connectés, il existe depuis longtemps des solutions de connectivité LPWAN (Low Power Wide Area Network), bas débit, basse consommation, longue portée, non cellulaire telles que LoRa [(1)] et Sigfox [(2)]. Ces réseaux peuvent être déployés librement et sont optimisés pour connecter en grand nombre des objets très peu consommateurs d'énergie sur une moyenne et longue portée. Ils sont particulièrement adaptés à la supervision, dès lors que de nombreux points de mesure sont à contrôler sur un périmètre géographique étendu, pour générer des systèmes d'alerte ou du contrôle de processus.

En réponse à cette concurrence, les opérateurs de réseaux cellulaires ont mis au point des standards, le NB-IoT et le LTE-M [(3)], spécialement conçus pour développer l'Internet des objets (IoT) dans leurs réseaux mobiles. Ces deux normes ont d'ailleurs été conçues pour être compatibles avec la 5G.

NB-IoT et LTE-M ont plusieurs similarités et présentent sensiblement les mêmes avantages (comme celui de fonctionner avec peu d'énergie, permettant ainsi à des objets basse consommation de communiquer *via* le réseau cellulaire), mais ils diffèrent par leur débit et leur latence. Le LTE-M est le protocole qui propose le plus grand débit (quantité de données échangées pour un temps donné) et la plus faible latence. Ainsi, en termes d'usage, le NB-IOT sert principalement à l'utilisation de capteurs, pour effectuer des contrôles agricoles, pour le *smart grid*, pour la *smart*

(1) Les réseaux LoRa, qui utilisent les fréquences 868 MHz en Europe, sont basés sur un protocole de communication établi de manière coopérative au sein de la LoRa Alliance.
(2) Le réseau Sigfox, qui utilise également les fréquences 868 MHz en Europe, propose un modèle propriétaire, dans lequel Sigfox assure une couverture internationale en s'appuyant sur des déploiements propres ou sur des partenariats avec des opérateurs locaux.
(3) Sur le plan technique, le NB-IoT (Narrowband IoT) est une norme de communication à bande étroite : les canaux IoT peuvent prendre en charge un grand nombre de dispositifs terminaux sur seulement 200 MHz de spectre. Le LTE-M (ou eMTC), quant à lui, est une technologie de réseau étendu de faible puissance adaptée aux applications IoT à faible bande passante, caractérisé par une faible latence et une sécurité accrue.

city, pour la pénétration des bâtiments et la gestion des *pipelines*, etc. Tandis que le LTE-M est plus souvent utilisé dans le domaine de la sécurité (usage de caméras, surveillance…), du transport, du *tracking*, du suivi médical, etc.

Par ailleurs, au-delà de l'introduction de ces standards sur les réseaux grand public, certains acteurs industriels se dotent de réseaux privés qui permettent des cas d'usages ciblés, le plus souvent liés aux objets communicants. Pour répondre à une demande croissante des acteurs, l'Autorité de régulation des communications électronique, des postes et de la distribution de la presse (Arcep), qui est en France l'entité qui attribue les fréquences pour des réseaux mobiles, a d'ailleurs ouvert en 2019 un guichet d'attribution de fréquences pour des réseaux privés 4G. Ces réseaux devraient naturellement évoluer vers des réseaux 5G à l'avenir. La mise en place d'un réseau privé facilite notamment la maitrise, la résilience et la sécurité du réseau.

La 5G : un domaine d'innovation rendant possibles de nouveaux usages

La « 5G » est la cinquième génération de réseaux mobiles, qui succède aux technologies 2G, 3G et 4G. Si les premières technologies ne permettaient que les appels vocaux puis l'envoi de SMS, les générations suivantes de technologies mobiles ont permis de développer de nouveaux usages : se connecter à Internet, accéder à des applications, ou encore passer des appels en vidéo.

La 5G, quant à elle, est une technologie évolutive qui va s'enrichir progressivement, au gré de l'évolution des standards au niveau mondial : ses performances vont progresser (débit, réactivité, capacité à gérer les usages de beaucoup d'usagers en même temps) avec la maturité technologique. Ainsi, à l'instar des technologies précédentes, la 5G améliorera les services existants et favorisera le développement de nouveaux services.

La 5G, une rupture technologique

Lors de la préparation d'une nouvelle génération de réseaux mobiles, deux acteurs travaillent en parallèle pour la définir :

- dans le domaine public, l'UIT (Union internationale des télécommunications) qui définit les caractéristiques de la technologie, dans notre cas la 5G (IMT-2020) ;
- dans le secteur industriel, le 3GPP (3rd Generation Partnership Project) qui fournit les solutions techniques (« normalisation ») répondant aux objectifs définis par l'UIT.

Ainsi, l'UIT a défini la 5G par trois grandes catégories d'usages, avec leurs exigences respectives, potentiellement incompatibles entre elles :

- **mMTC – Massive Machine Type Communications,** qui regroupe principalement les usages liés à l'Internet des objets. Ces services nécessitent une couverture étendue, une consommation énergétique contenue et des débits relativement restreints ;
- **eMBB – Enhanced Mobile Broadband,** qui correspond aux applications et services qui nécessitent une connexion toujours plus rapide, pour permettre par exemple de visionner des vidéos en ultra haute définition (8K) ou d'utiliser des applications de réalité virtuelle ou augmentée. Cette famille représente l'évolution de la plupart des services proposés par les réseaux 4G ;
- **uRLLC – Ultra-Reliable and Low Latency Communications,** qui regroupe toutes les applications nécessitant une réactivité extrêmement importante ainsi qu'une garantie forte de transmission du message.

En complément des familles d'usages, huit indicateurs de performance (KPI) ont été établis par l'UIT pour préciser, quantifier et mesurer les caractéristiques de systèmes 5G. Le schéma ci-après compare la 4G et la 5G suivant ces huit KPI :

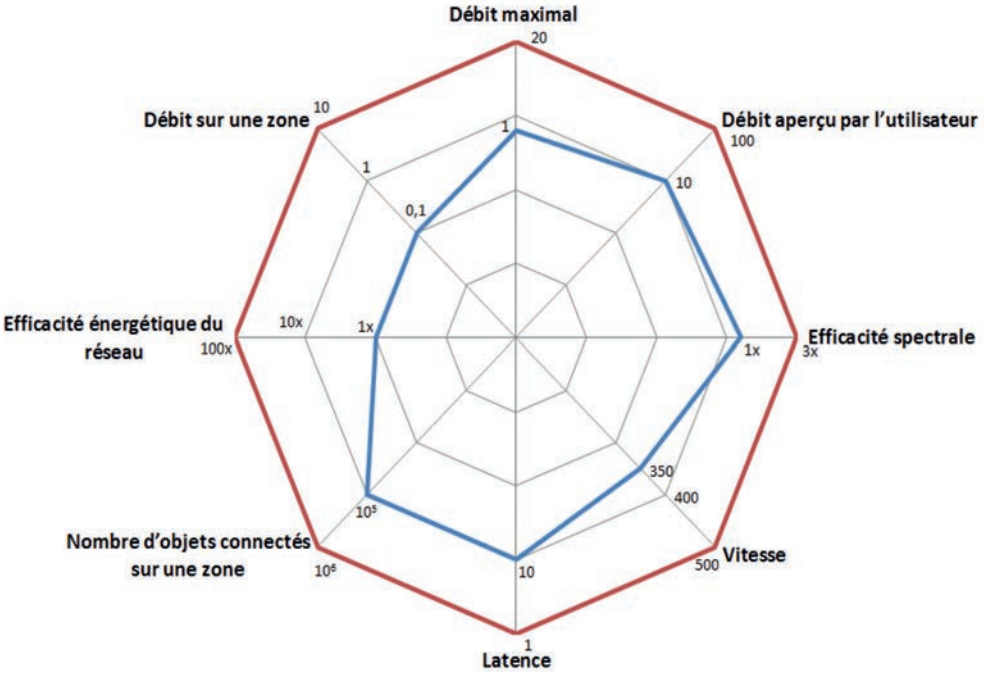


Figure 1 (Source : Arcep, issue de la Recommandation ITU-R M.2083-0 (09/2015) [4])

En résumé, la 5G a été spécifiée pour pouvoir offrir un débit maximal respectivement 10 fois supérieur à celui disponible actuellement, une densité maximale de connexions multipliée par 10 et une latence divisée par au moins 10 (la latence point à point cible est de 1 milliseconde, contre 30 à 40 millisecondes à ce jour).

Cependant, ces valeurs extrêmes ne pourront être atteintes simultanément pour tous les indicateurs : tous les cas d'usages ne sont pas compatibles entre eux, et un choix devra être réalisé pour définir des classes d'utilisation disposant chacune de son enveloppe de performances. À cet égard, la Figure 1 présente l'enveloppe des performances maximales de la 5G.

Le "*network slicing*" ou la possibilité d'usages variés de la 5G

Ainsi, chaque famille (mMTC, eMBB et uRLLC) est caractérisée par des usages qui lui sont propres et une enveloppe de performances appropriée. La Figure 2 ci-après en décrit quelques caractéristiques.

Comme vu précédemment, ces indicateurs ne pourront pas être tous satisfaits simultanément : les réseaux 5G seront configurés en « tranches » (*slices*), ils devront s'adapter dynamiquement à la demande, en fonction des usages, ce qui est réalisable grâce à la « virtualisation » logicielle des fonctions. Cette fonctionnalité, appelée "*network slicing*", est potentiellement la plus innovante de la 5G. Son introduction dans les réseaux est attendue à partir de 2023 en France.

(4) https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf)

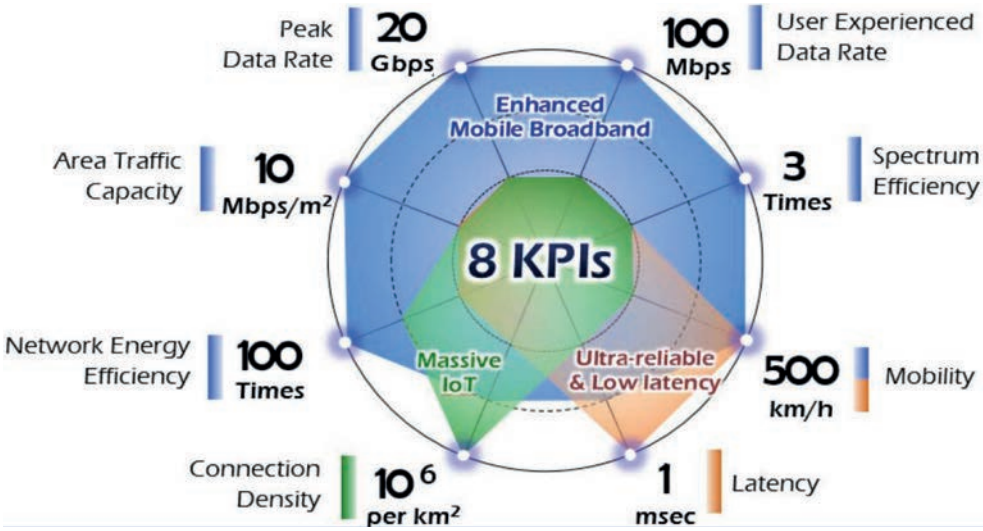


Figure 2 (Source : Dr. LEE, JunHwan - ETRI [5])

Pour les besoins d'ultra haut débit (eMBB), comme la vidéo 4K, 8K, 3D ou la réalité virtuelle, un certain nombre de performances, comme l'efficacité spectrale, le débit maximal et la capacité globale du réseau, peuvent être atteintes au détriment d'autres, comme la latence ou la densité de connexions simultanées. Actuellement, seul le eMBB est implémenté dans les déploiements des opérateurs mobiles.

À l'inverse, lorsqu'une connexion massive simultanée d'objets connectés (mMTC) doit être gérée, le réseau concentre ses ressources et utilise les technologies nécessaires à la résolution de cette tâche, mais il n'est pas en mesure, par exemple, d'utiliser aussi efficacement le spectre ou d'assurer une faible latence.

Enfin, lorsque des communications ultra fiables, avec une très faible latence sont nécessaires (uRLLC), le nombre de communications simultanées, le débit ou encore l'efficacité spectrale peuvent être réduits.

D'un point de vue technologique, cette flexibilité, ou capacité d'adaptation, qu'apporte le *network slicing* ne pourra être mise en place qu'avec la virtualisation d'un nombre important de composants du réseau ; on parle notamment de SDN (Software-Defined Networking) ou de NFV (Network Function Virtualisation). Derrière ces acronymes se cache une idée commune : utiliser le plus possible des composants génériques et reconfigurables, plutôt que des composants spécifiques dédiés *ad vitam* à des taches très particulières. Cette évolution vers le « logiciel » est envisagée depuis de nombreuses années, mais devient possible grâce à la montée en performances de tous ces composants reconfigurables, y compris ceux qui sont les plus proches des tâches élémentaires de la communication sans-fil (détection, codage en bande de base, gestion des trains binaires, changement de fréquences, traitement de signal, etc.).

L'attribution des fréquences 5G : vers un déploiement progressif

Pour le déploiement de la 5G, plusieurs bandes de fréquences ont été identifiées au niveau mondial, chacune présentant des priorités différentes et complémentaires. En France, les opérateurs utilisent à ce jour les bandes 700 MHz, 2,1 GHz et 3,6 GHz.

(5) https://5g-ppp.eu/wp-content/uploads/2016/11/06_10-Nov_Session-3_Lee-JunHwan.pdf

Les fréquences de la bande 3,5 GHz ont été attribuées aux opérateurs mobiles, le 12 novembre 2020, dans l'objectif de déployer la 5G. Avec au moins 70 MHz par opérateur, elles permettent notamment de répondre à la croissance du trafic dans les zones denses.

Les fréquences des bandes 700 MHz et 2,1 GHz ont été attribuées aux opérateurs mobiles en 2015 et 2001 par l'Arcep. Les autorisations étant technologiquement neutres, ces fréquences sont aujourd'hui utilisées pour des déploiements 4G et 5G. Avec une portée relativement conséquente, elles permettent d'assurer une couverture dans les zones plus rurales.

Le déploiement de la 5G sur le territoire n'en est qu'à ses débuts et sera progressif. Au 30 juin 2021, plus de 4 900 sites en bande 3,5 GHz sont ouverts commercialement. En prenant en compte l'ensemble des bandes de fréquences utilisées pour fournir un service 5G (3,5 GHz, 2,1 GHz et 700 MHz), ce sont plus de 16 800 sites qui sont ouverts en 5G aujourd'hui. Les opérateurs couvrent chacun entre 20 et 40 grandes agglomérations en bande 3,5 GHz.

La bande 26 GHz, qui a aussi été identifiée au niveau mondial pour la 5G, possède, quant à elle, des propriétés intrinsèquement différentes. En effet, avec une grande quantité de fréquences disponibles mais avec une faible portée, la bande 26 GHz permettra des débits très importants dans des cellules de petite taille. Ainsi, parmi les services envisagés figurent en premier lieu des services avec de très forts besoins en bandes passantes, comme des services de multimédia augmenté avec multiples prises de vues lors d'événements sportifs ou culturels ou encore la gestion d'outils industriels dans les usines.

L'Arcep, qui est l'entité qui attribue en France les fréquences aux opérateurs, conduit actuellement les travaux préparatoires à l'attribution de ces fréquences.

Les objets connectés, un cas d'usage majeur de la 5G ?

Les évolutions technologiques apportées par la 5G sont conçues pour tenir compte, entre autres, des objets communicants : connection d'un grand nombre d'objets ou augmentation des débits.

Sur un plan technique, les opérateurs ont à ce jour implémenté la 5G en eMBB, notamment pour faire face à la demande croissante en trafic. Avec l'introduction du *network slicing* vers 2023, il leur sera alors possible d'implémenter de la 5G en mMTC, catégorie la plus intéressante pour les objets communicants. Sur un plan commercial, il s'agira pour les opérateurs de proposer des offres BtoB (de l'anglais *business-to-business*) adaptés aux besoins des acteurs économiques (entreprises, collectivités, administrations...).

Face à ces évolutions, l'Arcep, consciente des enjeux pour la compétitivité de l'économie française s'est attachée à mettre en place lors de l'attribution des fréquences 3,5 GHz un cadre préparant la connectivité de demain. Ainsi, les autorisations d'utilisation de fréquences, outre des obligations de couverture du territoire ou de débit fourni, de natures assez classiques, comprennent aussi des obligations visant à faciliter les usages BtoB de la 5G. Parmi celles-ci, deux concernent particulièrement le développement du marché des objets communicants :

- celle d'activer au plus tard fin 2023 les fonctions les plus innovantes de la 5G (le "*slicing*" notamment) afin d'être en mesure d'offrir des « services différenciés », répondant à des besoins spécifiques ;
- celle, complémentaire et concomitante, « de faire droit aux demandes raisonnables » des acteurs économiques (entreprises, collectivités, administrations...) en leur proposant des offres spécifiques que ce soit en termes de couverture ou de performances (s'il le préfère, l'opérateur pourra leur confier localement ses fréquences).

Par ailleurs, afin d'accompagner les acteurs dans l'exploration des futurs usages de la 5G, différentes expérimentations ont été rendues possibles. En particulier, l'Arcep et le gouvernement ont ouvert en 2019 un appel à projets pour des plateformes 5G d' « innovation ouverte » dans la bande 26 GHz. Plusieurs usages ont pu être testés dans le cadre de ces plateformes, que ce soit dans les domaines du divertissement (*entertainment*), des transports, de la logistique ou encore dans le domaine industriel, avec notamment plusieurs cas d'usages impliquant des objets connectés (capteurs dans des bâtiments, capteurs dans des usines, etc.).

Conclusion

Si, à son lancement, la 5G va principalement améliorer l'accès aux services proposés par les réseaux existants en permettant notamment un meilleur débit et plus de capacité, elle devrait permettre par la suite le développement de nouveaux types de services pour les individus et surtout pour les entreprises. En particulier, la 5G viendra compléter la gamme de solutions disponibles pour le déploiement et la gestion des objets connectés. Ces nouvelles fonctionnalités pourront être proposées par les opérateurs au fur et à mesure de l'évolution de la 5G.

Pour tirer pleinement parti de ces nouvelles possibilités, les opérateurs devront mettre au point de nouvelles formes de services, répondant de manière plus ciblée aux besoins des différents utilisateurs et, notamment, des acteurs économiques. Parallèlement, ces utilisateurs devront explorer les nouvelles possibilités permises par la 5G. Et ce n'est que grâce un dialogue constructif et attentif entre fournisseurs et utilisateurs que la 5G pourra trouver tout son potentiel.

Use unlicensed LPWANs for cost-effective & secure massive industrial IoT

Par **Derek WALLACE**
VP of Marketing, LoRa Alliance

Introduction

The Internet of Things (IoT) allows us to collect and read data from sensors that have been added to industrial functions or measurable aspects of everyday life. Among its uses, this data can be leveraged to improve operational processes, enhance worker safety, and monitor maintenance requirements. Due to the diverse and multifaceted character of IoT technology, it can be extremely difficult to determine the right connectivity path for each usage. While established technologies, such as Wi-Fi, Bluetooth, and 4G have added IoT connectivity to their portfolios, the group of technologies that is quickly gaining traction in the massive industrial IoT segment is Low Power Wide Area Networks, or LPWANs. The reason this group of technologies, standards and smart devices has rapidly gained territory over the past several years is that they have been specifically designed to address the needs of the majority of IoT use cases to provide long-range communication on small, inexpensive batteries that often have a life of ten years or more. LPWANs can connect many types of sensors and offer a strong, cost-effective, secure and rapid, massive connectivity. In this article, we explore how LPWANs, and in particular unlicensed LPWANs and the LoRaWAN® standard, enable fast, reliable, and massive IoT through billions of connections.

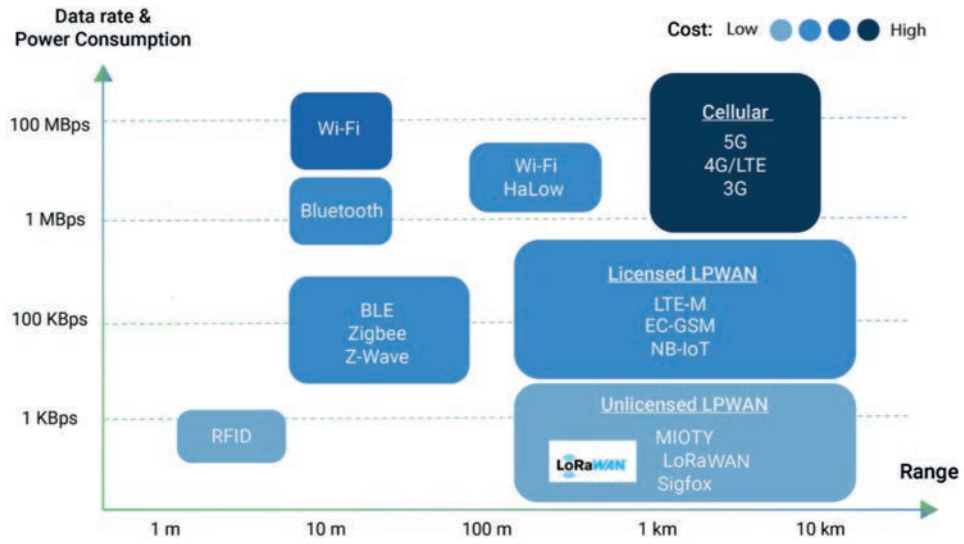
Building a smart future while limiting additional cost

Not all LPWAN's are created equally or within the same radio frequency. A key distinction is whether the spectrum is licensed or unlicensed. Each technology within these two categories offers different strengths and weaknesses, and delivers varying levels of performance depending on the requirements of an IoT use case. Factors, such as power consumption, quality of service, scalability, and standardization (for interoperability purposes) all play a role in choosing the right fit. There are benefits to operating within the licensed spectrum, yet it often involves a higher Total Cost of Ownership (TCO) compared to unlicensed LoRaWAN. One of the primary benefits of the unlicensed, open standard is flexibility and ease of deployment on either public, private, or hybrid networks. Other benefits include wide area connectivity, low-cost chipsets and networks, limited data usage, coverage in rural and non-cellular areas, and the ability to penetrate concrete and metal walls. To mitigate unwanted interference within the unlicensed band, standards bodies, such as the LoRa Alliance®, have ensured maintenance of secure connectivity *via* encryption and authentication protocols.

Various studies predict a prosperous future for LPWANs. For instance, the number of connected devices is expected to grow from 13.9 million in 2017 to 1,151 billion in 2023 [(1)].

(1) "Structural Health Monitoring Market by Solutions (Hardware: Sensors, Data Acquisition System; Software & Services), Technology (Wired and Wireless), End Users and Geography - Global Forecast to 2022", summary available at www.marketsandmarkets.com/Market-Reports/ structural-health-monitoring-market-101431220.html

The figure below shows the positioning of LPWANs, less recent, and legacy protocols when looking at power consumption & data rate against range.



Positioning of IoT Technologies (Source: Behr Technologies)

LoRaWAN is a nonproprietary, unlicensed technology for large-scale IoT

Within the unlicensed LPWANs, LoRaWAN uses the radio frequency spectrum that satisfies industrial IoT applications that require a long range, low bit-rate, low power consumption, and low throughput. This combination of long range and low power is better suited for frequencies lower than those used for Wi-Fi and Bluetooth. LoRaWAN operates in the sub-1 GHz license-free band, more specifically 868 MHz in Europe and 902-928 MHz in the US. It is accessible to anyone wishing to set up a network, whether it be a private, public, or hybrid one.

The goal of LoRaWAN is to connect millions of IoT devices in a secure and cost-effective manner. Where some other technologies require a data plan for every sensor deployed, LoRaWAN does not charge for spectrum use from the sensor to the gateway, and each gateway can support thousands of sensors. Network deployments consist of LoRaWAN end-point nodes connected wirelessly to gateways that in turn connect to a network server in the cloud or on premises, securely routing data to an application or business system.

Compared to licensed technologies, such as NB-IoT and LTE-M that are suited for critical IoT, LoRaWAN is ideally suited to serve the needs of non-critical and massive industrial IoT (*e.g.*, billions of sensors). Like all LPWANs, it does not facilitate transmission of large messages, and, when needed, can send short, fast ones at specific moments only, preserving battery life. Once a basic LoRaWAN network has been set up, any type of sensor serving any type of application can be very quickly connected in order to obtain valuable data.

A unique ecosystem promoting LoRaWAN

As the importance of global collaboration increases, solution providers, manufacturers, operators, and system integrators will continue to partner and face the challenge of returning positive ROI early in their projects. The group of IoT companies that strive for promotion of the LoRaWAN standard around the world is the LoRa Alliance®. The LoRa Alliance is a non-profit organization representing over 400 member companies developing and operating LoRaWAN equipment from silicon to solutions. Member companies are active across the entire LoRaWAN value chain, producing chipsets, modules, sensors, gateways, servers, and platforms that enable complete end-to-end LoRaWAN solutions for customers and enterprises. Thanks to numerous fruitful collaborations, LoRaWAN networks are currently available in 171 countries, and there are 156 LoRaWAN network operators, enabling thousands of use cases across cities, rural areas, and industries.

For more information, please visit lora-alliance.org.

La révolution du spatial ou la communication des objets partout dans le monde

Par **Alexandre TISSERANT**
Président de Kinéis

Quand on parle d'Internet des objets (IdO, ou IoT pour "Internet of Things"), on en vient rapidement à parler de milliards d'objets connectés. Beaucoup d'études de marchés, d'analyses prospectives promettent des dizaines de milliards d'objets connectés dans les cinq à dix ans.

Pour autant qu'elle se réalise effectivement, cette perspective recouvre des réalités technologiques et marchés très diverses. Les cas d'usages sont très variés, avec des besoins clients aux paramètres usuellement sources de discussions et de compromis : taille et forme de l'objet, nombre et nature des capteurs embarqués, niveau d'autonomie énergétique, fiabilité dans le temps, résistance physique (étanchéité, chocs, température…), volume de données à transmettre, intégration dans une chaîne de traitement de données plus large, et, bien sûr, prix de l'objet et sa connectivité.

Les paramètres de qualité et d'étendue de la couverture sont souvent passés sous silence, de même que la disponibilité de la même solution technologique sur l'entièreté de la surface du globe. Ou, plutôt, ils sont pris comme une donnée d'entrée avec laquelle il faut composer : tel réseau fonctionnera sur telle zone, sur telle fréquence, et les cas d'usages devront s'y adapter.

Désormais, les technologies spatiales permettent de révolutionner cette approche, et d'offrir une connectivité en tout point similaire sur le globe, d'un pôle à un autre, du milieu des océans à celui des déserts.

Et la plus-value est tout à fait considérable : aujourd'hui, seuls 15 % environ de la surface du globe sont couverts par des réseaux bas débit terrestres. Cela permet bien sûr de connecter beaucoup d'objets, de la *smart city* aux flux logistiques locaux par exemple. Mais de nombreux cas d'usages sont encore trop limités par cette faible couverture – qui, si elle continuera de s'améliorer, ne pourra jamais couvrir la totalité des territoires compte tenu des investissements nécessaires.

Cette couverture terrestre limitée concerne typiquement les applications maritimes, où, par définition, passé les zones côtières, la connectivité disparaît. C'est le cas également dans les grandes étendues très peu peuplées, en Amérique du Nord, du Sud, en Afrique, en Australie, ou même encore en Asie. Parfois même en Europe, des zones non connectées empêchent des cas d'usages d'émerger : la fiabilité requise pour le suivi quasi permanent de flux logistiques, d'actifs industriels stratégiques, sur route, rail ou mer, ne peut y être atteinte.. L'agriculture connectée est également très demandeuse de ces nouvelles solutions.

Ce qu'est et permet la connectivité satellitaire IoT – et ce qu'elle n'est pas

Le paysage de la connectivité satellitaire, si elle apporte son lot de simplicités attrayantes, n'échappe pas à la diversité des technologies et des offres :

- La couverture d'abord : usuellement 100 % globale pour les solutions spatiales vraiment dédiées à l'IoT, comme Kinéis ; certains réseaux, minoritaires cependant, peuvent ne pas couvrir les très hautes latitudes, de par la géométrie de la constellation en place. D'autres ont des autorisations

d'exploitation limitées sur certaines régions du globe. Il convient d'en avoir connaissance, car la couverture globale est pourtant souvent l'argument principal pour passer à la connectivité spatiale.

- L'autonomie ensuite : la différence majeure de la connectivité IoT par rapport aux autres solutions de connectivité reste sa très faible consommation d'énergie. C'est le cas aussi bien dans le domaine terrestre que satellitaire. Malgré tout, avec des satellites situés en orbite basse, entre 500 et 800 km d'altitude en général, la puissance nécessaire pour communiquer avec le satellite est légèrement supérieure. Ainsi, certains réseaux ne fonctionnent qu'avec des terminaux nécessitant une alimentation en énergie, qu'elle soit filaire externe (alimentation électrique), manuelle (piles) ou autonome (panneaux solaires, récupération d'énergie de chaleur ou de mouvement). À l'inverse, d'autres réseaux (comme celui de Kinéis) permettent d'avoir des terminaux qui, avec une simple batterie lithium, peuvent durer de plusieurs mois à plusieurs années.
- Puis la fréquence sur laquelle est opérée la connexion au satellite. Les réseaux terrestres IoT LPWAN (Low Power Wide Area Network) fonctionnent par exemple essentiellement sur les bandes dites ISM (industrielle, scientifique et médicale), aux alentours de 868 MHz (en Europe). Les réseaux satellitaires utilisent des fréquences plus variées, depuis le VHF (Very High Frequency) aux alentours de 156 MHz jusqu'à des bandes au-delà de 2 GHz. Ce point est crucial à plusieurs égards : d'abord, la fréquence détermine les autorisations à obtenir dans les différents pays (plus ou moins facilement, plus ou moins payantes) ; ensuite, à débit de données

Figure 1 : Connexion directe aux satellites (Source : Kinéis)

égal, plus la fréquence est élevée, plus l'énergie nécessaire pour transmettre est importante et moins le signal est robuste à l'environnement (intempéries, feuillages…) ; enfin, plus la fréquence est élevée, plus la taille de l'antenne nécessaire pour émettre est petite – ce qui parfois est un point important quand les exigences sur la forme et le volume de l'objet sont fortes.

- Également, la modalité de connexion au satellite : directe ou par l'intermédiaire d'un relais terrestre local (*gateway*). L'avantage d'une connectivité directe (le terminal dialogue de manière autonome directement avec les satellites) est bien sûr son indépendance et sa résilience (un terminal qui ne fonctionne plus n'affecte pas les autres). À l'inverse, une connexion *via* un relais terrestre peut favoriser une simplicité de déploiement dans certains cas : le relais va connecter des dizaines ou centaines de terminaux déjà déployés à l'aide d'une connectivité terrestre IoT existante (LoRa – pour Long Range – par exemple), et va ensuite transmettre ces données aux satellites. Cela permet d'utiliser des terminaux disponibles sur étagère, mais le relais, de par le trafic supporté, va nécessiter d'être alimenté en énergie, aura par définition un rayon de couverture limité et souvent fixe, et constituera un élément critique du dispositif (si le relais tombe, les centaines d'objets qui y sont connectés sont perdus).
- Enfin, le caractère uni ou bidirectionnel de la connectivité. Certains systèmes ne permettent que de la collecte de données pure et simple : un objet émet un signal que le satellite récupère et retransmet au sol pour livraison au client. D'autres, en revanche, permettent de communiquer en retour à l'objet, en *unicast* ou *multicast*, pour envoyer soit des informations métiers (une alerte météo pour un petit pêcheur isolé en haute mer, une commande d'ouverture de vanne pour un réseau d'eau ou de gaz), soit des informations techniques (éphémérides des satellites, statut de la constellation, commande de changement de stratégie d'émission…).

Plusieurs dimensions sont en revanche communes à tous les réseaux à constellations de satellites en orbite basse.

- Tout d'abord, le délai de revisite : les satellites en orbite basse sont des satellites dits défilants, c'est-à-dire qu'ils tournent autour de la Terre sur des orbites qui nécessitent une haute vitesse (sur des orbites polaires, ils font typiquement le tour de la Terre en 1 heure 30 environ). Cela signifie que, sur un point donné à la surface du globe, un satellite se lève à l'horizon, défile au-dessus du point et disparaît sous un autre horizon en 10 à 15 minutes environ. Le satellite suivant n'est pas toujours directement proche, et le délai moyen d'attente de ce satellite suivant, ce délai de revisite, constitue un paramètre à avoir en tête. Typiquement, certaines applications ont une tolérance forte à ce délai : un scientifique qui suivra une tortue marine ou un faucon sur une dizaine d'années se satisfera très bien de quelques points dans la journée. À l'inverse, une autorité de pêche voulant s'assurer que des bateaux immatriculés ne vont pas pêcher dans des zones interdites demandera un délai de revisite qui ne dépasse pas 15 minutes. Au bout du spectre, on trouvera des applications critiques de sûreté (alertes intrusion, explosion, etc.) qui demanderont du temps réel, et donc un temps de revisite nul. Évidemment, dans un réseau satellitaire où les satellites sont visibles par intermittence, l'objet connecté inclut (grâce au modem fourni par l'opérateur de ce réseau) une fonction de prévision de passage des satellites, afin de n'émettre que lorsque ceux-ci sont en visibilité.

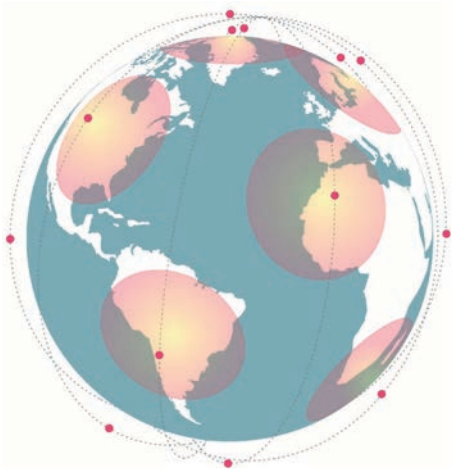


Figure 2 : Exemple de constellation satellitaire en orbite basse, avec successions des couvertures de chaque satellite (Source : Kinéis)

- Ensuite, la performance de transmission selon le point d'émission. Cela peut paraître évident, mais il peut être utile de rappeler que la connectivité satellitaire fonctionnera très bien dans des environnements en extérieur, dégagés, avec un accès au ciel le plus large possible et idéalement jusqu'à l'horizon. Ainsi, l'IoT par satellite fonctionnera très bien en mer, ou dans des zones avec peu de relief, qu'il soit naturel ou construit (campagnes, montagnes pas trop abruptes). La connectivité satellitaire ne sera en revanche pas un bon choix pour, entre autres, de la télé-relève de compteurs situés en sous-sol (à moins d'ajouter un relais externe), des objets situés à l'intérieur de bâtiments ou en plein centre-ville où des immeubles de grande hauteur empêcheront d'avoir un accès suffisamment large aux satellites.

C'est là que l'hybridation avec des réseaux terrestres devient tout à fait pertinente : encore à ses débuts en termes de déploiement, mais déjà technologiquement fonctionnelle, la technologie d'hybridation consiste à embarquer, dans un même terminal, un modem pour la connectivité terrestre (comme LoRaWAN) et un autre pour la connectivité satellitaire (comme Kinéis). Un algorithme relativement simple permettra de se connecter au réseau terrestre lorsque celui-ci est détecté à portée, typiquement en zone urbaine ou en intérieur, et de se connecter au réseau satellitaire dès que le terminal est hors de couverture terrestre. On crée alors la possibilité d'avoir des objets connectés qui fonctionnent de manière transparente quel que soit l'endroit où ils se trouvent sur le globe : cet objectif d'être une solution simple, ou "*no-brainer*", est très important d'un point de vue de l'adoption client.

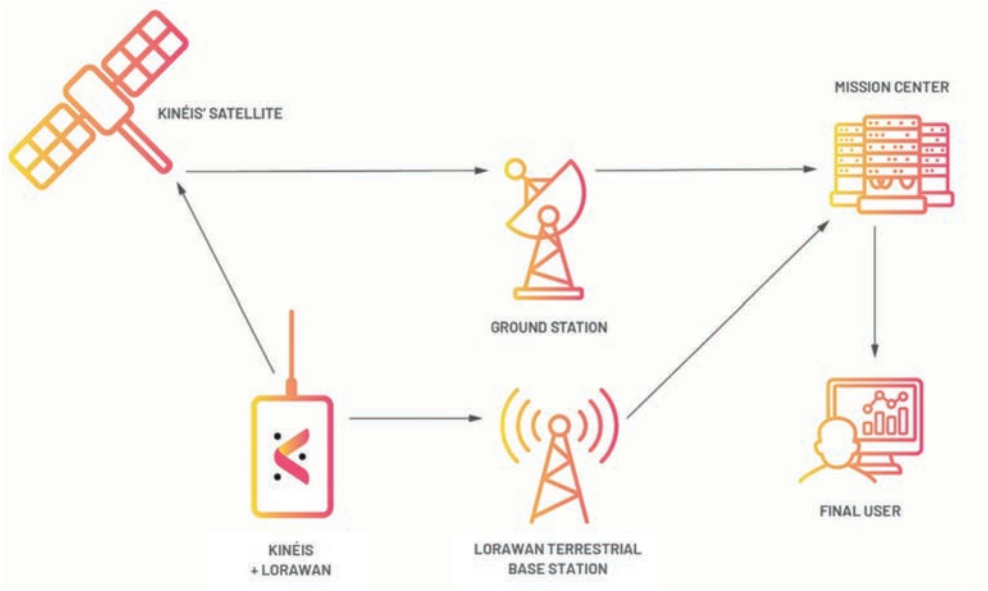


Figure 3 : Schéma de transmission des données avec une connectivité hybride LoRaWan + Kinéis (Source : Kinéis)

- Une dernière caractéristique intéressante avec les réseaux satellitaires en orbite basse est que, grâce précisément à leur caractère défilant très rapide, le signal perçu des terminaux induit un effet Doppler lorsque plusieurs messages sont envoyés d'affilée. Cet effet Doppler permet, à partir de 3 messages successifs, de calculer une position du terminal avec une précision de l'ordre de 150 mètres. Le point important est que ce calcul se fait sans avoir besoin de puce GNSS [(1)] dans le terminal, souvent très consommatrice en énergie. La précision de localisation est donc un compromis à faire avec l'autonomie du terminal. Là encore, cela dépend du cas d'usage :

(1) Géolocalisation et Navigation par un Système de Satellites, par exemple une puce GPS ou Galileo.

une précision de 150 mètres est largement suffisante pour suivre et étudier les migrations d'une cigogne sur 10 ans (et permettra de gagner de précieux milliwattheures d'énergie) ; à l'inverse, détecter sur quel quai a été déchargé un container peut requérir une position plus fine, et donc l'intégration d'une puce GNSS dans l'objet connecté au container.

Enjeux de l'IoT spatial

Au-delà des enjeux techniques et de ciblage pour le client, de nombreux enjeux traversent les réseaux satellitaires dédiés à l'IoT spatial.

Tout d'abord, celui du modèle économique. Malgré la baisse drastique des coûts d'accès à l'espace et la miniaturisation extrême des satellites (les plus petits satellites lancés pour l'IoT[2] font 10 cm x 10 xm x 2,5 cm…, on est très loin des satellites géostationnaires de la taille d'un bus), les investissements nécessaires à la construction d'un tel réseau sont considérables. Kinéis a par exemple dû lever 100 millions d'euros pour financer l'intégralité de sa constellation de 25 nano-satellites (d'une taille repliée de l'ordre de 20 cm x 20 cm x 40 cm pour 30 kg environ), qui fournira une couverture en quasi temps réel (délai de revisite en-dessous de 15 minutes). Les marchés sont importants, et la demande est forte, mais le cycle commercial est long : entre le premier contact prospect et le déploiement de quelques milliers d'unités sur le terrain s'écoule une période de 18 mois. En effet, il est rare qu'un objet connecté pour un cas d'usage donné puisse être réutilisé pour un autre ; ainsi, au-delà des nécessaires phases de conviction, de tests et de prototypage qu'il faut accompagner, l'industrialisation des objets adaptés au cas d'usage d'un client peut s'avérer longue. Il importe donc de bien maîtriser des verticales marchés particulières et les sujets de fabrication d'objets (avec l'aide de partenaires par exemple), de sorte de pouvoir reproduire au maximum un cas d'usage, et éviter de perdre trop de temps et de ressources à en développer d'autres.

Ensuite demeure toujours une question éthique, pour le coup pas forcément spécifique à l'IoT spatial : ces technologies permettent de suivre et surveiller des objets, mais techniquement rien n'empêche de suivre des personnes, avec ou sans leur consentement. Par ailleurs, des informations récoltées par les objets donnent souvent des renseignements sur des personnes (bracelet connecté de santé, données de consommation de fluides divers, déplacements, etc.). Dès lors, au-delà de la réglementation à respecter comme le RGPD (Règlement général sur la protection des données), il convient de vérifier l'éthique et l'utilité sociale de chaque projet pour en assurer son acceptabilité, et *in fine* sa rentabilité économique.

Dans le même ordre, la question écologique commence, à juste titre, à prendre de l'importance dans ce secteur. D'une part, la production et le lancement de satellites ainsi que le déploiement d'objets connectés induisent des émissions de GES (gaz à effet de serre) qu'il convient de quantifier, pour garantir ensuite qu'elles sont compensées au maximum par des projets d'IoT qui viendront réduire l'impact carbone d'un client (détection de fuites, optimisation des trajets, détection de feux de forêts…). D'autre part, la pollution spatiale deviendra rapidement problématique si aucune régulation internationale n'est établie. De la même manière qu'une organisation a dû être mise en oeuvre pour réguler le trafic aérien, et ainsi éviter les collisions et maîtriser les nuisances induites, nous n'échapperons pas à la mise en place d'une structure intergouvernementale pour éviter que l'orbite basse terrestre ne devienne un cimetière de débris spatiaux empêchant tout nouveau déploiement et toute observation astronomique. Sur ce dernier point, des acteurs privés

(2) Il s'agit des satellites de l'entreprise américaine Swarm, récemment rachetée par SpaceX.

commencent à affirmer qu'une régulation est nécessaire compte tenu des dizaines de milliers de satellites annoncés pour être lancés [3], et même des cabinets de conseil comme McKinsey se penchent sur la question [4].

Enfin, il ne faut pas oublier l'adage partagé par tous les ingénieurs du domaine spatial : "*Space is hard*". Malgré l'apparente facilité avec laquelle les nouveaux projets spatiaux se montent, nombre d'entre eux ne voient jamais le jour ou simplement ne sont pas au niveau des performances attendues [5]. Kinéis, avec son héritage spatial du CNES (Centre national d'études spatiales) et ses huit satellites déjà en orbite et fonctionnels, dispose pour le coup d'atouts importants et solides dans la compétition internationale des nouvelles entreprises du secteur spatial (*NewSpace*).

(3) https://www.spaceintelreport.com/viasat-spacex-starlink-threat-to-leo-sustainability-is-casus-belli-for-us-were-asking-spacefaring-nations-to-deny-market-access/?mc_cid=ff7baa4bd7&mc_eid=f929a87092
(4) https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/look-out-below-what-will-happen-to-the-space-debris-in-orbit
(5) https://spacenews.com/hiber-abandons-plans-for-iot-satellite-constellation/

Skywise, pour la maintenance prédictive et au-delà…

Par **François LE BOULCH, Frederic SUTTER** et **David MARTY**
Airbus

Airbus

Airbus est le pionnier d'une industrie aéronautique et spatiale durable, pour un monde sûr et uni. La société innove constamment pour fournir des solutions efficaces et technologiquement avancées dans l'aérospatial, la défense et les services connectés. Dans le domaine de l'aviation commerciale, Airbus propose des avions de ligne modernes et économes en carburant ainsi que des services associés. Airbus est également un *leader* européen dans le domaine de la défense et de la sécurité, ainsi qu'un acteur mondial de premier plan dans le spatial. Dans le domaine des hélicoptères civils et militaires, Airbus fournit les solutions et les services les plus performants au monde.

Par l'intermédiaire de ses prédécesseurs, Airbus a été le pionnier de nombreuses technologies qui ont contribué à conquérir le ciel et font désormais partie de la vie quotidienne. L'innovation a toujours été une force motrice chez Airbus, qui promeut les technologies de pointe et l'excellence scientifique pour contribuer au progrès mondial.

Le groupe encourage ses experts à toujours plus de disruption en inventant notamment de nouvelles possibilités pour l'avenir du vol : des véhicules habités sans pilote pour la mobilité urbaine, aux systèmes de propulsion hybrides et électriques.

Dans un environnement en évolution rapide où le *big data* soutient de plus en plus la prise de décision, où l'expérience utilisateur revêt une importance croissante et où les innovations sont rapidement mises en œuvre, Airbus a fait le choix d'investir dans la transformation digitale pour façonner l'avenir de l'industrie aéronautique 4.0.

Skywise

Chaque avion commercial dans le ciel rassemble aujourd'hui des informations provenant de milliers de points de données. L'Airbus A350, par exemple, compte plus de 250 000 capteurs à bord, qui génèrent plus de 10 Go de données à chaque heure de vol et fournissent des informations sur les performances, les besoins de maintenance, etc. En plus de transporter les passagers en toute sécurité d'un point A à un point B, l'avion moderne est un ordinateur dans le ciel.

Airbus a fait dès 2015 un choix stratégique en plaçant la donnée au cœur de son programme de transformation numérique.

L'approche retenue repose, d'une part, sur la mise en œuvre d'une plateforme de partage et d'analyse des données (*data platform*) et, d'autre part, sur l'acquisition et le renforcement des compétences internes en matière d'intelligence artificielle (IA), de science de la donnée, de gouvernance de la donnée, de cybersécurité, tous ces sujets étant considérés comme stratégiques.

Lancée au Salon du Bourget en juin 2017, la plateforme Skywise (développée avec la société américaine de logiciels et de services Palantir Technologies) est capable de mettre en commun et

d'analyser les données de l'ensemble de l'écosystème aéronautique. Skywise identifie des modèles, fait des prédictions et suggère des actions pour améliorer le fonctionnement des compagnies aériennes, et, au final, la façon dont les passagers vivent leur voyage en avion.

Au cœur du système, Skywise permet à ses utilisateurs d'accéder à la bonne information au bon moment. Elle exploite une importante quantité de données jusqu'alors enfermée dans les entreprises et les silos fonctionnels de l'industrie, générant ainsi de la valeur pour tous ses acteurs.

Airbus rend cette technologie disponible gratuitement à toute compagnie aérienne qui, en retour, partage avec le constructeur certaines des données de ses avions Airbus dans les domaines de l'*engineering* et de la maintenance. Ce partage renforce la collaboration et offre des bénéfices par nature très variés, depuis l'amélioration de la performance industrielle jusqu'au développement de nouveaux services en passant par la réduction des cycles de développement ou l'amélioration des produits.

Il est bon de rappeler que le premier cas d'utilisation a permis de supporter la montée en cadence du programme A350 avec une amélioration radicale de l'analyse de données, démontrant rapidement des gains à deux chiffres, notamment sur les problématiques de non-qualité ou de travaux restants.

Airbus started final assembly of the first A350-1000 on schedule at the A350 XWB final assembly line in Toulouse, France, beginning in February 2016 (Source: Airbus Media gallery)

L'écosystème Skywise

Skywise est le *leader* des plateformes de données d'entreprise pour l'industrie aéronautique.

Largement exploitée en interne chez Airbus, Skywise peut être utilisée par les compagnies aériennes, les fournisseurs, les partenaires certifiés, les développeurs d'applications, les autorités aériennes, les MRO (centres de maintenance, réparation et révision).

On parle d'écosystème Skywise, avec plus de 23 000 utilisateurs dans le monde qui contribuent à son développement au travers de projets comme le suivi et la résolution d'événements, l'analyse des temps de rotation, des opérations, de la régularité technique, ainsi que la maintenance prédictive, le *benchmarking* et l'aide à la décision de maintenance.

Source: Airbus

Avec la Skywise Academy, les utilisateurs peuvent construire leurs propres applications de façon autonome alors que pour des besoins plus génériques, Airbus a développé des applications prêtes à l'emploi disponibles sur une place de marché appelée Skywise Store.

Nombreux sont les cas d'usages où la collaboration entre les compagnies aériennes et Airbus crée de la valeur mutuelle. L'application "Wheel Bearing Inspection", par exemple, permet d'éviter certaines tâches de maintenance et réduit le nombre de remplacements des trains d'atterrissage grâce à l'analyse de données par les ingénieurs Airbus.

Un autre exemple : "Skywise Reliability Premium" où la collaboration avec Airbus aide les compagnies à cibler les problèmes techniques critiques sur l'ensemble de leur flotte avions, à identifier les meilleures solutions disponibles et à simuler leur efficacité. Cela est critique dans un contexte de reprise du trafic aérien où tout ce qui est évitable doit être évité.

Skywise comme plateforme de services aux clients

Avec l'expansion des flottes, les services aéronautiques généreront dans les vingt prochaines années quasiment autant de revenus que les produits eux-mêmes. De quoi bouleverser les modèles commerciaux et renforcer le pouvoir du *big data*.

Les interruptions d'exploitation et les AOG (Aircraft on Ground ou la traduction littérale d'avion au sol) sont le talon d'Achille des compagnies aériennes, et restent à l'origine d'énormes coûts de maintenance, d'une charge de travail non programmée et du mécontentement des passagers.

Au sein d'Airbus, les spécialistes données du plateau Zéro AOG créent des algorithmes qui scannent les données des avions des clients afin de détecter les signes avant-coureurs d'aléas techniques. On parle de maintenance prédictive (Skywise Predictive Maintenance). Elle anticipe la défaillance des composants en analysant les comportements anormaux grâce au calcul des données provenant des capteurs de l'avion. SPM est un ensemble d'algorithmes couvrant un large éventail de modes de défaillance parmi tous les chapitres de l'Air Transport Association (ATA). Cette solution aide les compagnies aériennes à réduire le nombre d'interruptions opérationnelles (retards, déroutements, retours en vol, etc.) et à anticiper les tâches de maintenance, pour passer d'une réparation majeure à une réparation mineure tout en optimisant la gestion des stocks de pièces détachées.

Les retours d'expérience positifs sont nombreux. Delta Airlines déclarait début 2019 un taux de réussite de plus de 95 % pour les prévisions de pannes en cours, soit 55 annulations liées à la maintenance contre 5 600 en 2010. En Europe, c'est Easyjet qui faisait figure de précurseur en signant début 2018 un contrat SPM d'une durée de cinq ans pour l'ensemble de sa flotte. Un choix gagnant puisque les retards ont été réduits de 70 % la première année, passant de dix à trois pour 1 000 vols sur les avions les plus récents de la compagnie.

Skywise Predictive Maintenance - Predictive events view (Source: Airbus)

Le plateau Zéro AOG n'est qu'un exemple de la transformation numérique opérée par Airbus pour devenir un prestataire de services à forte valeur ajoutée. Depuis trente ans, l'entreprise cherche à conquérir de nouvelles parts de marché. Le support client classique, essentiel au lancement de nouveaux programmes, a toujours prévalu sur le service après-vente payant.

Dans son rapport prévisionnel "Global Services Forecast 2018/2037", Airbus estimait qu'au cours des vingt prochaines années, le marché mondial des services de l'aviation commerciale représenterait quelque 4,6 milliards de dollars en valeur cumulée, contre 5,8 milliards de dollars pour les ventes d'avions commerciaux sur la même période. Compte tenu de ces perspectives, et pour répondre à la demande du marché, Airbus a accéléré le développement d'activités basées sur les données et centrées sur les clients.

Cette tendance s'expliquait non seulement par le changement de *business model* des compagnies aériennes, qui tendaient à externaliser les services coûteux de maintenance, réparation et révision (MRO), mais aussi par les progrès rapides du traitement de données dont profiteraient les exploitants aériens.

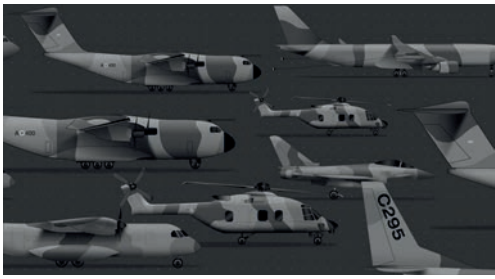
« Le secteur de l'aviation commence à se remettre de la crise du Covid-19 », déclarait Guillaume Faury, CEO d'Airbus. Un vent de reprise souffle sur l'aéronautique et les nouvelles technologies, incluant l'augmentation du nombre d'avions connectés, et conduira à la croissance des services digitaux.

Des possibilités infinies

Au salon 2018 de Farnborough, Airbus Helicopters et Airbus DS ont lancé conjointement SmartForce, une suite de services permettant aux opérateurs militaires d'exploiter les données pour optimiser la sécurité, la disponibilité opérationnelle et les coûts. Cette transformation a été engagée avec des initiatives structurantes dans les domaines des plateformes en ligne à base de *cloud* privé sur nos sites en Europe, mais aussi des "Analytics" avancés et des applications, de la cybersécurité et de la gouvernance des données, des nouveaux modèles économiques et des services, ou encore de la continuité numérique des produits.

SmartForce repose sur l'analyse de données, plus particulièrement adaptée aux avions et hélicoptères militaires. Parmi les clients figure Singapour, qui souhaite développer la maintenance prédictive en utilisant SmartForce pour sa flotte d'avions multirôles de ravitaillement en vol et de transport (A330 MRTT).

La proposition de valeur d'Airbus pourrait être résumée ainsi : « Concentrez-vous sur votre mission, nous nous occupons du reste ».



Source: Airbus Media gallery

The Royal Australian Air Force benefits from Airbus SmartForce digital services for the maintenance of their A330 MRTT Air Refueling Boom System (Source: Airbus Media gallery)

Les projets "Analytics" d'Airbus soutiennent de multiples plateformes comme l'A400M, l'A330 MRTT, l'Eurofighter Typhoon ou la flotte d'AWACS (pour Airborne Warning and Control System) de l'OTAN grâce à des centres implantés dans le monde entier. L'offre va des matériels à la maintenance, en passant par la révision-réparation, la formation et les opérations en vol, et couvre des sujets tels que : tris et analyses rapides de rapports de vols et d'essais, synthèses, support à l'analyse des causes racines avec isolation des *fault codes* et la maintenance prédictive. Elle permet par exemple de diviser par quatre le temps nécessaire à l'analyse des rapports de vol de l'A400M.

La partie militaire fonctionnera progressivement sous SmartForce et la partie civile sous Skywise. Les services connectés aident les opérateurs dans trois domaines : sécurité, disponibilité et optimisation des coûts. Les avantages de ces services vont de la prévision du besoin en pièces de rechange à une maintenance et un support plus efficaces.

À toute allure

Quel que soit le challenge, Airbus possède l'expertise nécessaire et les moyens d'y faire face. Par exemple, lorsqu'Airbus a repris la maintenance des A330 de Singapore Airlines, la compagnie a augmenté la disponibilité de sa flotte de 8 %, générant autant de profits supplémentaires pour la compagnie aérienne.

Les services sont un domaine ultra concurrentiel, où fournisseurs et maintenanciers défendent ardemment leur pré carré, tandis que les constructeurs misent sur le digital pour accroître leur sphère d'influence.

Sur ce terrain, la collecte et l'analyse des données au service de la maintenance prédictive et préventive permettent à Skywise de marquer son époque.

Si la plateforme améliore la régularité technique et opérationnelle des flottes en service, livre des analyses rapides des causes racines des problèmes opérationnels, optimise la performance de chaque appareil, suit l'efficacité de la maintenance dans le temps et fournit des processus de *reporting* en un clic, le numérique, lui, redéfinit notre industrie à toute allure.

Références

Skywise :
https://skywise.airbus.com/ ; https://skywise.airbus.com/en/about-skywise.html

Delta airlines :
https://news.delta.com/delta-techops-expanding-predictive-maintenance-capabilities-new-airbus-partnership

Easyjet :
http://www.predictiveaircraftmaintenance.com/airbus-skywise/

Airbus :
https://www.airbus.com/company/history/airbus50/day21.html ;
https://www.airbus.com/public-affairs/brussels/our-topics/innovation/data-revolution-in-aviation.html ; https://www.airbus.com/newsroom/press-releases/en/2018/07/airbus-forecasts--4-6-trillion-worldwide-market-for-commercial-a.html ;
https://www.airbus.com/newsroom/press-releases/en/2018/03/easyjet-signs-skywise-predictive-maintenance-agreement-with-airb.html ;
https://www.airbus.com/search.document.html?q=salon+du+bourget+2019&newsroom=true#searchresult-document-all-12 ;
https://www.airbus.com/newsroom/press-releases/en/2019/06/airbus-launches-seven-new-smartforce-services-for-military-customers.html ;
https://www.airbus.com/newsroom/news/en/2021/05/Tanking-goes-automatic.html
https://www.airbus.com/newsroom/press-releases/en/2021/05/airbus-provides-suppliers-with-an-update-on-production-plans.html#media-list-document-document-all_ml_0-2

SUTTER F. & BOUREAU L. (2018), « Le digital, un déploiement déjà fructueux », *Le Magazine des Ingénieurs de l'armement*, n°116.

Où vont nos données ? L'exemple des assistants vocaux

Par **Martin BIERI**
Chargé d'études au Laboratoire d'innovation numérique de la Commission nationale de l'informatique et des libertés (CNIL)

La voix est l'un – si ce n'est le premier – de nos principaux outils de communication : nous l'utilisons quotidiennement, pour toutes sortes d'interactions. Si elle est restée longtemps le vecteur d'échanges entre les humains (et aussi, dans une moindre mesure, avec les animaux), elle devient une nouvelle interface dans la relation homme-machine, incarnée par les assistants vocaux. Désormais, chacun peut échanger directement avec des systèmes informatiques en utilisant le langage de tous les jours, le « langage naturel [1] ». Ce qui signifie que la machine possède des capacités allant de la compréhension à la formalisation d'une réponse, vocale également. Tout ce processus induit un traitement de notre voix et de nos paroles par l'objet communicant. Alors, comment fonctionne réellement un assistant vocal ? Et que fait-il de notre voix ?

Le rapport à la voix : une donnée à géométrie variable

Une histoire pas si récente

Avant de regarder sous le capot de ces « nouveaux majordomes », analysons la voix et la parole comme « données à interpréter ». Historiquement, la voix était une donnée volatile : selon le proverbe, les paroles s'envolent, et les écrits restent. Toutefois, depuis l'invention du phonographe par Thomas Edison et Charles Cros (chacun de son côté), à la fin des années 1870, permettant d'enregistrer les sons – et donc la voix –, cet adage semble de plus en plus obsolète. Son développement entraîne une nouvelle perception de ce moyen de communication, notamment sur le plan juridique. En effet, quelques années après, en 1890, dans un texte autour de la protection des données et de la vie privée (sur la notion du « droit d'être laissé tranquille »), les juristes américains Warren et Brandeis pointent les risques associés à ces nouvelles technologies d'enregistrement, y incluant « le possesseur de tout autre dispositif moderne de reformulation ou de reproduction de scènes ou de sons [2] ». En France, le code pénal actuel précise notamment dans son article 226-1 la protection contre la captation, l'enregistrement ou la transmission « des paroles prononcées à titre privé ou confidentiel [3]».

Des données multiples et complexes

La voix n'est pas qu'un son à interpréter, mais une donnée à géométrie variable. Tout d'abord, il faut distinguer l'information verbale, c'est-à-dire le message en lui-même que nous voulons transmettre, et les informations non verbales, dites « paralinguistiques » : l'intonation, les silences, les gestes, etc.

(1) En opposition au « langage formel », codifié pour être non ambigu et qui est utilisé pour les programmes informatiques.
(2) WARREN S. & BRANDEIS L. (1890), "The right to privacy", *Harvard Law Review*, 4(5), December 15.
(3) Version en vigueur au 1er août 2020.

Sans pour autant entrer dans la théorie entre « signifiant » (l'image acoustique associée à un mot) et « signifié » (le concept de ce mot) [4], la parole peut véhiculer un ou plusieurs sens [5]. Et selon ce qui est dit, l'information que l'on en retire sera différente : une phrase anodine n'aura pas la même notion de sensibilité qu'une phrase délivrant un secret, ou faisant état d'une opinion politique, d'une appartenance syndicale, d'une orientation sexuelle, etc.

Par ailleurs, hors du sens propre de ce qui est dit, la voix renferme également d'autres éléments, la part non verbale. En effet, nous sommes en capacité de reconnaître ou d'en déduire d'autres informations : âge, genre, état émotionnel, état de santé (par exemple, des maladies dégénératives comme Parkinson [6]), condition physique, origine géographique, accent, etc.

Et ce jusqu'à l'identité du locuteur [7]. La voix possède des caractéristiques qui sont propres à chaque individu : des attributs biométriques « comportementaux [8] » qui permettent d'en authentifier l'identité, à travers la création d'un modèle de voix ou gabarit. La voix est d'ailleurs comprise dans le droit à l'image, en tant qu'« attribut de la personnalité, une sorte d'image sonore ». Puisqu'elle permet l'identification d'une personne physique, de manière directe ou indirecte, la voix est de fait une donnée personnelle au sens du Règlement général sur la protection des données (RGPD). Les données biométriques, à l'instar des données de santé, sont donc considérées comme « sensibles » dans le RGPD, c'est-à-dire des données dont l'utilisation est particulièrement encadrée : l'article 9 prévoit ainsi une interdiction à leur traitement, en permettant des exceptions. Le traitement de la voix n'est donc pas un processus anodin…

La voie des données

Fonctionnement d'un assistant vocal et circulation des données

Il faut d'abord préciser ce qu'est un assistant vocal, à commencer par ce qu'il n'est pas : une enceinte connectée n'est pas forcément un assistant vocal, mais peut en être équipée. Ce que l'on considère être un assistant, c'est la part logicielle offrant des capacités de dialogue oral en langage naturel avec l'utilisateur de l'objet l'embarquant. De manière plus pratique, nous pouvons définir trois grandes entités entrant dans la composition d'un assistant vocal [9] :

- **l'instance physique** : tout élément matériel dans lequel va prendre forme l'assistant, et qui se concrétise aussi par la présence de microphones, haut-parleurs et capacités de calcul ;
- **l'instance logicielle** : c'est la partie qui met en œuvre l'interaction homme-machine (à travers les modules de transcription automatique de la parole, de compréhension et génération du langage naturel, de dialogue et de synthèse vocale) ; elle peut être opérée au sein de l'objet, mais, de façon générale, est réalisée de manière distante ;
- **les ressources** : toutes les données externes, bases de connaissances et applications qui fournissent la réponse à la question posée ou permettent de déclencher l'action demandée par l'utilisateur.

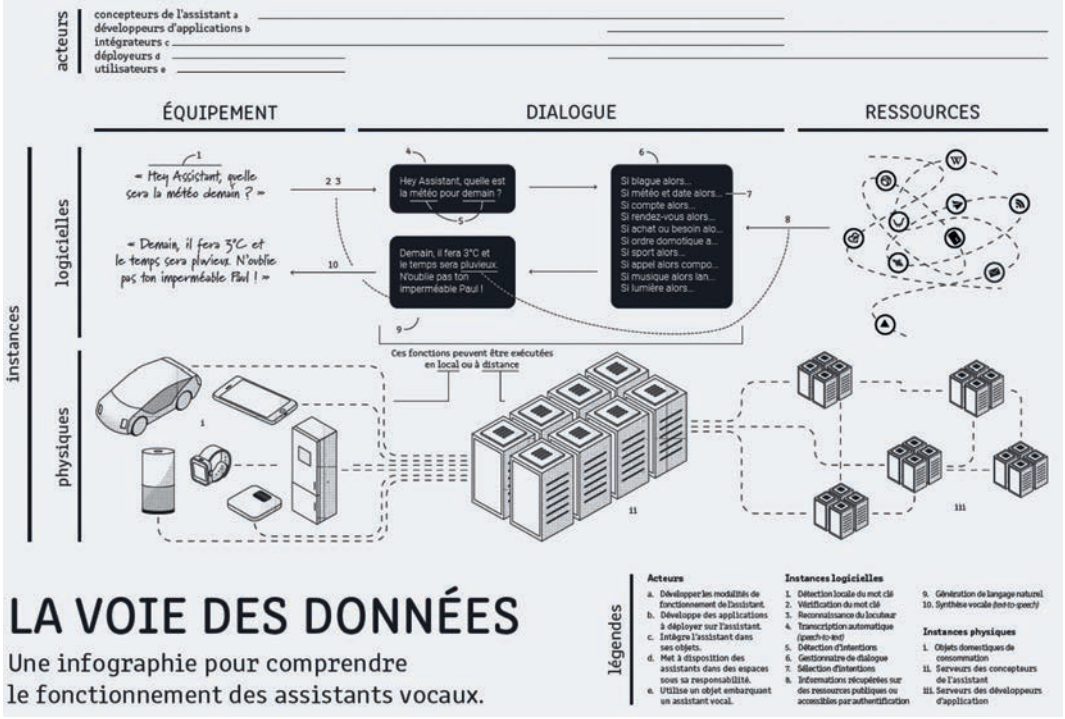
Un assistant vocal n'enregistre pas en continu tout ce qui est à portée de microphone : il est nécessaire d'utiliser un mot-clé pour « réveiller » l'assistant, qui sinon reste en veille. Il n'utilise

(4) DE SAUSSURE F. (1916), *Cours de linguistique générale*, Payot.
(5) REVIS J. (2018), « Notre voix porte en elle toutes les intentions qui sont les nôtres », *Linc.cnil.fr*, entretien, mars.
(6) JEANCOLAS L. *et al.* (2016), « L'analyse de la voix comme outil de diagnostic précoce de la maladie de Parkinson : état de l'art », *Compressions et Représentation des Signaux audiovisuel*, mai.
(7) BONASTRE J.-F. (2017), « La voix n'est pas une biométrie classique », *Linc.cnil.fr*, entretien, février, https://linc.cnil.fr/jean-francois-bonastre-la-voix-nest-pas-une-biometrie-classique
(8) BONASTRE J.-F., *Ibid.*
(9) CNIL (2020), « À votre écoute – Exploration des enjeux éthiques, techniques et juridiques des assistants vocaux ».

alors qu'une mémoire tampon qui n'a pour but que de vérifier si ce mot de réveil a bien été prononcé. Cette vérification est faite localement au sein du dispositif, mais, pour les cas où les traitements sont faits à distance, il peut y avoir une deuxième passe effectuée sur des serveurs, afin de déceler un faux positif (un mot qui aurait été pris pour le mot-clé par erreur). Il peut y avoir à ce moment une vérification de l'identité du locuteur, si ce dernier s'est enrôlé, c'est-à-dire s'il a préalablement partagé ses caractéristiques vocales à l'assistant. Une fois réveillé, l'assistant va recevoir la requête de l'utilisateur qui sera traitée localement ou à distance (sur le modèle « mot de réveil, quel temps fera-t-il demain ? »). L'audio est alors transcrit en texte (*speech to text*), et le texte va être interprété par les algorithmes de traitement automatique du langage : seront alors identifiées les intentions du message ainsi que les variables d'informations. Concrètement, dans l'exemple de l'interrogation de l'assistant sur la météo pour demain, l'intention est la demande du temps, et la variable est donc « demain », la temporalité. À partir de cette identification, un gestionnaire de dialogue va pouvoir construire le scénario de la réponse à apporter. Si nécessaire, les bases d'informations distantes (ici, la base de données météorologiques) seront interrogées pour préciser la réponse selon les variables identifiées. La phrase de réponse est ainsi générée – et/ou l'action, si c'était l'objet de la requête (comme « monter le chauffage »). Elle est alors synthétisée (*text to speech*) et est donc ensuite mise en œuvre par l'objet embarquant l'assistant, et l'assistant repasse en veille !

Les acteurs en présence

Pour faire fonctionner un assistant, plusieurs acteurs sont nécessaires. Ils interviennent à différents moments dans la chaîne de valeur, à commencer par le **concepteur** de l'assistant. C'est celui qui va mettre au point l'assistant, en choisir le fonctionnement et les paramètres (techniques, matériels, etc.). Interviennent également les **développeurs d'application** : ce sont eux qui vont élaborer les applications utilisables *via* l'assistant, à l'image de ce qui est fait pour les *smartphones*. Bien qu'ils



doivent respecter le cadre instauré par le concepteur, ils ont une responsabilité également puisque, généralement, ce sont eux qui vont définir les finalités de l'application et le traitement des données (voir le cas d'usage n°2 dans le livre blanc « À votre écoute »). Il y a ensuite les **intégrateurs**, ceux qui vont implémenter dans leurs objets et équipements l'assistant vocal avant que les **déployeurs** (même si le terme n'est pas très élégant) n'installent l'assistant dans des endroits partagés, des endroits de passage, des environnements de travail, etc. Enfin, il ne reste plus que **l'utilisateur** lui-même, qui va interagir avec l'assistant vocal (et éventuellement être lui-même « déployeur » s'il installe chez lui des équipements embarquant l'assistant vocal).

Les grands enjeux

Des stratégies économiques, notamment fondées sur la récupération des données

La plupart des assistants vocaux font peu de traitement des données embarqué directement dans les dispositifs, mais plutôt sur des serveurs distants. Ce qui implique que le transfert des données vocales ainsi que le traitement se passent directement chez le concepteur de l'assistant. Ceci est parfois justifié par le fait qu'il faudrait embarquer directement dans l'objet connecté des capacités de calcul plus importantes que ce qui est fait majoritairement aujourd'hui, et qu'il est plus facile et moins coûteux de tout centraliser.

Cependant, il y a aussi – et surtout – des enjeux économiques dans ce mode de fonctionnement : les modèles d'affaires des grands constructeurs occidentaux (à commencer par les deux firmes qui dominent ce marché, Google et Amazon) reposent sur une stratégie classique de récupération des données à des fins publicitaires. Si la technologie vocale est « nouvelle » dans nos usages, son modèle économique reste celui de la publicité classique sur Internet : l'assistant vocal n'est qu'un avatar, un point d'entrée de plus pour récupérer des données d'utilisation, afin de pouvoir enrichir un profil qui sera ensuite utilisé pour du ciblage publicitaire. Par ailleurs, pour pouvoir utiliser l'assistant à 100 %, il est souvent nécessaire de créer un compte ou de le synchroniser avec un compte déjà existant (par exemple, un compte Gmail pour Google ou Amazon pour Alexa).

Le fait de n'embarquer que peu de puissance de calcul directement dans l'objet est aussi un moyen pour baisser son coût : le but est ainsi la pollinisation du marché par une forte production d'équipements à moindre frais, permettant une assise certaine sur le marché. Les grands constructeurs ont aussi fait en sorte qu'il soit aisé de mettre au point une application (pour la déployer dans un assistant) comme de l'intégrer dans un équipement tiers (montre, frigo, aspirateur, etc.).

Quels enjeux concernant les données pour les assistants vocaux ?

Les enjeux posés par les assistants vocaux et les assistants tout court par ailleurs, comme en témoignent les travaux du Comité national pilote d'éthique du numérique (CNPEN) sur les *chatbots* [10], sont nombreux, et n'ont pas tous trait à l'utilisation des données (et notamment les données personnelles [11]) : relation homme-machine, genre et identité de l'assistant, anthropomorphisation, l'implémentation d'IA et la question des biais qui lui est souvent associée, en passant par des problématiques liées au fait que les noms utilisés pour les assistants soient déjà existants [12], etc.

(10) CNPEN (2020), « Les enjeux éthiques des agents conversationnels », https://www.ccne-ethique.fr/fr/actualites/cnpen-les-enjeux-ethiques-des-agents-conversationnels, 26 juin.
(11) CNIL (2020), « À votre écoute – Exploration des enjeux éthiques, techniques et juridiques des assistants vocaux ».
(12) PINSKER J. (2021), "Amazon killed the name Alexa", *The Atlantic*, 18 août.

La question de la circulation des données se pose : la chaîne de valeur d'un assistant vocal comprend un certain nombre d'acteurs, dont plusieurs sont directement destinataires des données ou les voient transiter sur leurs serveurs. Qui est alors responsable du traitement de données ? La question du stockage de certains types de données a soulevé des interrogations, notamment le fait de proposer un enrôlement à l'utilisateur. Ce processus implique de garder quelque part un gabarit biométrique (modèle de voix) propre à l'utilisateur – la plupart des assistants donnent désormais la possibilité de stocker cette partie directement en local, au sein de l'objet connecté embarquant l'assistant.

De la même manière, la sensibilité des données – dans le sens de ce qu'elles peuvent révéler sur l'intimité des individus – a été au cœur d'un scandale à l'été 2019. Comme pour tout système d'apprentissage automatique, il est nécessaire d'avoir une supervision humaine et un contrôle du fonctionnement. Pour les assistants vocaux, cela veut dire améliorer les performances par la réécoute d'interactions (par exemple, en vérifiant ce qui avait déclenché un faux positif dans le réveil de l'assistant, ou pourquoi l'assistant avait mal compris). L'information apportée aux personnes ne contenait pas de précision sur « cette amélioration à des fins de service », et la base légale d'un tel traitement posait question – l'autorité de protection des données d'Hambourg [13] avait alors demandé à Google de suspendre ces écoutes le temps de clarifier le fondement juridique de ce type de traitement. Par ailleurs, ces écoutes pouvaient contenir des éléments intimes (voire des scènes violentes), et ces données pouvaient être traitées par des prestataires externes aux entreprises conceptrices, jetant encore un peu plus de flou sur qui avait accès à ces données. Les grands concepteurs ont alors revu leurs pratiques, arrêtant cette manière de faire pour certains ou permettant une option de retrait (ou *opt-out*) de ce système associée à une meilleure information des utilisateurs. Cette question est d'autant plus problématique lorsque les enregistrements proviennent de personnes n'ayant pas été informées de ce traitement ou n'ayant pas donné leur consentement. En réveillant l'assistant vocal sans avoir connaissance qu'il est dans la pièce (en prononçant un mot-clé proche par exemple), la personne ignore que l'assistant va traiter l'extrait comme étant une requête.

L'assistant vocal et son incarnation physique (enceinte, véhicule, montre, etc.) sont donc un nouveau point d'entrée pour les concepteurs, leur permettant de récolter des données, de la même manière que pour une navigation sur le *web*. C'est aussi une porte d'entrée vers les comptes et les données des utilisateurs. De nombreuses publications ont montré que les assistants vocaux (notamment à travers les enceintes communicantes) étaient sensibles à des attaques plus ou moins sophistiquées. Les angles sont multiples pour accéder à cette porte d'entrée vers nos données : à travers des sons inaudibles par l'homme (*dolphin attack* [14]), à travers un laser pointé vers l'assistant (à une centaine de mètres de distance ! [15]), ou tout simplement se trouver dans son rayon d'action (environ 5 mètres). Des enjeux qui ont amené un cabinet d'avocats irlandais à bannir leur utilisation dans ses locaux – notamment pour préserver le secret professionnel et se prémunir d'éventuelles écoutes intempestives.

(13) The Hamburg Commissioner for Data Protection and Freedom of Information (2019), "Speech assistance systems put to the test - Data protection authority opens administrative proceedings against Google", août.
(14) ZHANG G. *et al.* (2017), "DolphinAttack: Inaudible voice commands", *ACM Conference on Computer and Communications Security*, novembre.
(15) SUGAWARA T. e*t al.* (2019), "Light commands: Laser-based audio injection on voice-controllable systems", novembre, https://lightcommands.com/

Conclusion

Il y a déjà eu de multiples changements depuis l'arrivée du premier assistant vocal grand public, Siri, en 2011. Encore récemment, au printemps 2021, Apple a annoncé des modifications : l'assistant deviendra « un peu plus privé [16] », faisant en sorte qu'aucun contenu ne soit enregistré par défaut, et que le maximum de traitement de la voix se fasse localement. D'autres concepteurs ont engagé des travaux pour permettre une meilleure gestion des données, ont corrigé également la sensibilité aux mots de réveil, etc. La CNIL, dans son livre blanc, avait alors listé plusieurs pistes d'amélioration, selon les problématiques et les acteurs concernés [17], à travers quatre grands principes cardinaux : entretenir les frictions désirables (profiter des moments de choix et de paramétrage pour présenter la réalité des traitements), privilégier le local au distant, assurer les moyens de contrôle par l'utilisateur et s'adapter au média vocal (présentation de l'information, recueil du consentement, etc.).

(16) HERMANN V. (2021), « Vie privée et sécurité : Apple monte d'un cran », *NextInpact.com*, 23 juillet.
(17) CNIL (2020), *Ibid.*, voir pp. 66 à 84.

Le mythe de la *smart city* écologique

Par **Philippe BIHOUIX**
Directeur général du groupe AREP

Le poids environnemental des villes, tant par leur « fabrication » (artificialisation des sols, consommation de matières premières, énergie grise et émissions de CO_2 à la production des matériaux de construction, en particulier le ciment et l'acier) que par leur « métabolisme » (flux d'énergie, de matières et de déchets, besoins de mobilité des personnes et des marchandises…), n'est plus à démontrer. Les rendre « écologiques » ou « durables », sans même parler de neutralité carbone, est un défi énorme, alors que la population mondiale continue à se concentrer – le taux d'urbanisation mondial pourrait passer de 55 % actuellement à 68 % en 2050 (1).

À suivre les discours convenus, les technologies numériques permettraient d'optimiser le fonctionnement futur des villes et de les rendre plus efficaces, mais aussi plus transparentes, « inclusives » et démocratiques, grâce au déploiement d'objets connectés – permettant de récolter des données, de surveiller et d'agir sur la ville (caméras, capteurs, contrôle d'équipements…) – et à l'analyse et l'exploitation de ces données par des logiciels, notamment basés sur les techniques d'intelligence artificielle (IA). Il y aurait là un « vivier extraordinaire d'usages potentiels que ce soit pour la gestion de l'énergie, de la mobilité, de l'eau ou encore des déchets » (2).

Le déploiement de tout un arsenal technologique urbain s'avèrerait même incontournable, certes pas forcément suffisant à la conversion écologique des villes, mais nécessaire. Stéphane Richard, patron de l'opérateur Orange, soutenait ainsi le déploiement de la cinquième génération de téléphonie mobile (5G), au plus fort du débat à l'automne 2020 : « La 5G, c'est aussi une promesse de développement des objets connectés, indispensables pour les *smart cities* : les municipalités auront besoin de la 5G pour réaliser leur transition écologique » (3).

La *smart city*, concept émergent ou mort-né ?

La notion de *smart city* (ou ville intelligente) émerge sous l'égide de quelques grandes sociétés technologiques : en 2005, Cisco lance le programme de recherche "Connected Urban Development Program", dont le but est de rendre les villes « durables grâce à l'innovation » (4), tandis qu'IBM lance sa "Smarter Planet Initiative" fin 2008, puis le "Smarter Cities Challenge" pour « aider les grandes villes à fonctionner plus efficacement, à économiser de l'argent et des ressources et à améliorer la qualité de vie des habitants » (5).

L'expression fait rapidement florès ; colloques, études, articles, livres, intentions affichées et projets se multiplient un peu partout. Après la crise financière de 2008, beaucoup d'acteurs privés voient alors dans l'Internet des objets et la fourniture de nouveaux services numériques un relais de croissance de leurs activités ; tandis que les décideurs publics sont à la recherche d'économies – donc d'efficacité des opérations urbaines –, mais y voient aussi matière à développement économique local et à attractivité territoriale, indispensable dans une économie toujours plus

(1) NATIONS UNIES (2018), « 2,5 milliards de personnes de plus habiteront dans les villes d'ici 2050 », 16 mai.
(2) RENALDO P. & VAQUERO G. (2019), « 5G : une nouvelle génération technologique, des usages à inventer », Wavestone.
(3) Stéphane Richard, PDG d'Orange, interview dans *Les Échos*, 22 septembre 2020.
(4) "Connecting cities : achieving sustainability through innovation".
(5) en.wikipedia.org/wiki/Smarter_Planet

mondialisée. La création de Sidewalk Labs en 2015 par Alphabet, la maison-mère de Google, achève de convaincre les plus indécis qu'il y a là matière à marchés juteux, et que les villes et leurs services publics pourraient bien être le nouveau terrain de jeu de la « disruption ».

La définition de la *smart city* reste floue. Selon la CNIL (Commission nationale de l'informatique et des libertés), la « ville intelligente est un nouveau concept de développement urbain. Il s'agit d'améliorer la qualité de vie des citadins en rendant la ville plus adaptative et efficace, à l'aide de nouvelles technologies qui s'appuient sur un écosystème d'objets et de services », concept qui concerne « les infrastructures publiques (bâtiments, mobiliers urbains, domotique, etc.), [les] réseaux (eau, électricité, gaz, télécoms) ; [les] transports (transports publics, routes et voitures intelligentes, covoiturage, mobilités dites douces – à vélo, à pied, etc.) ; les *e*-services et *e*-administrations » [(6)].

Ces dernières années cependant, la protection des données individuelles est devenue une question de plus en plus sensible, qui pourrait remettre en cause la vision idyllique d'une gestion technologique et ultra-optimisée des villes, surtout si celle-ci est confiée à des acteurs privés, voire au petit cercle des géants du numérique. Sérieusement asticoté à Toronto, où il devait participer au développement de la friche industrielle de Quayside, Google a finalement jeté l'éponge en mai 2020 – officiellement pour cause d'incertitude économique liée à la crise sanitaire.

Bienvenue à « écoloville »

Mais la promesse de *smart cities* écologiques se heurte à bien d'autres obstacles. Certes, sur le papier, on peut trouver des « cas d'usages » pertinents, même si de nombreuses fonctionnalités, comme la vidéosurveillance, la cybersécurité ou les services publics numériques, n'ont pas grand-chose à voir avec l'environnement. Les plus importants concernent la gestion énergétique et les transports, auxquels on peut ajouter la sobriété de certains réseaux (détection des fuites d'eau, éclairage public réduit *via* la détection de présence…) ou une meilleure gestion des déchets – comme des poubelles connectées aidant au geste de tri ou à l'optimisation des tournées de ramassage.

Pour l'énergie, il s'agirait de construire, à toutes les échelles (logements, bâtiments, quartiers…) un réseau de production, de distribution et de consommation, une sorte « d'Internet de l'énergie » [(7)] articulant productions renouvelables, dispositifs de stockage, réseaux intelligents (*smart grids*) et pilotage fin de la demande (« effacement », fonctionnement en horaires décalés, etc.). Dans les transports, les systèmes améliorés (information voyageurs, plateformes d'agrégation d'offres de service…) favoriseraient l'intermodalité, l'utilisation des transports en commun, le développement du partage et des modes doux, tandis que l'autonomie des véhicules viendrait généraliser le covoiturage et fluidifier le trafic.

Mais face à ces « bénéfices » environnementaux escomptés, projetés dans un futur encore à « inventer », il convient de comptabiliser également les « coûts », qui risquent d'être bien réels et plus immédiats.

Consommation de ressources

Le premier écueil concerne le besoin de ressources engendré par la multiplication des objets connectés qui viendront « enrichir » habitations, infrastructures et espaces publics – mais aussi par le développement des équipements numériques (pour le stockage et le traitement des données) situés en arrière-plan.

(6) cnil.fr/fr/definition/smart-city
(7) RIFKIN J. (2012), *La troisième révolution industrielle*, Éditions Les liens qui libèrent.

Les progrès technologiques des dernières décennies, en matière de miniaturisation des circuits électroniques et de chimie des batteries notamment, permettent aujourd'hui de déployer, à moindre coût, des – ou d'envisager le déploiement de – milliards d'objets connectés. Or ceux-ci sont paradigmatiques des difficultés rencontrées par le secteur numérique dans le recyclage. La complexité et la variété des objets électroniques, la multiplicité des composants et des matières incorporées [8], les quantités très faibles utilisées (et ce d'autant plus que l'objet est petit), les alliages rendent les processus de recyclage cauchemardesques, et très imparfaits : actuellement, plus d'une trentaine de métaux (sur une soixantaine au total), souvent emblématiques des *high-tech* – comme l'indium, le gallium et le germanium, les terres rares, le tantale – sont recyclés à… moins de 1 % au niveau mondial [9].

Évidemment, tous les objets connectés embarquent différentes ressources en quantités variables, selon les technologies employées, les modes de communication (RFID, Wi-Fi, Bluetooth, GSM…), leur mode d'alimentation, leur autonomie… Les quantités globales en jeu sembleront peut-être limitées face à d'autres besoins, comme les énergies renouvelables de forte puissance ou les voitures électriques ; mais à l'inverse, les objets connectés favorisent les usages jetables (faible coût, batterie conçue pour une durée de vie de l'objet de quelques années…), et leur « invisibilité » pourrait également être un frein à leur collecte pour un recyclage dans les conditions les plus optimales possibles.

Il est en tout cas certain que plus nous « technologiserons » nos objets, nos services, nos villes, plus nous piocherons dans le stock limité de ressources, souvent plus rares, et plus nous nous éloignerons d'une économie circulaire, accélérant, au lieu de freiner, la logique « extractiviste » actuelle.

Effet et inertie « systémiques »

Le deuxième écueil vient de la nécessité de raisonner à une échelle « systémique », de prendre en compte l'ensemble de la chaîne de valeur et des effets induits. Sans doute, les voitures autonomes et les *smart cities* pourraient optimiser les consommations futures, par kilomètre-passager parcouru, par mètre-carré de logement occupé, etc. Mais quels systèmes de traitement des données et de télécommunications seront nécessaires pour les faire « tourner », et avec quel impact environnemental ? Le secteur numérique exerce déjà une pression énorme sur les ressources et les besoins électriques [10].

Il est difficile d'estimer, à ce stade, ce que consommeront les réseaux 5G, nécessaires aux applications nécessitant un temps de latence très faible (comme les véhicules autonomes) ou si la densité d'objets connectés dépasse un certain seuil [11]. Cela dépendra de la stratégie de déploiement de chaque opérateur, des configurations adoptées, du trafic effectif… Selon le Haut conseil pour le climat (HCC), cela pourrait représenter une augmentation de 5 à 13 % de la consommation d'électricité finale du pays [12] en 2030.

Une voiture autonome pourrait générer plusieurs milliers de gigaoctets (Go) par jour – ainsi une flotte d'un milliard de voitures roulant quelques heures par jour multiplierait par 1 000 au moins le trafic de données actuel – ; un habitant de *smart city* plusieurs centaines de Go par jour. Nul ne sait la proportion de ces données qui devra être archivée (à des fins sécuritaires, assurantielles,

(8) De l'ordre de 40 métaux dans un *smartphone*, par exemple.
(9) *Cf.* les travaux de l'International Resource Panel / United Nations Environment Program.
(10) Le système numérique consomme plus de 10 % de l'électricité mondiale et émet environ 1 milliard de tonnes de CO_2 par an. Voir par exemple les travaux du Shift Project.
(11) La 5G permet d'augmenter fortement cette densité, jusqu'à un million d'objets communicants par km^2.
(12) Soit 16 à 40 térawattheures : HCC (2020), « Maîtriser l'impact carbone de la 5G », décembre.

marketing…), et pour quelle durée ; mais l'impact sur les centres de données pourrait être massif – à titre comparatif, la quantité stockée actuellement dans le *cloud* ne représente encore « que » 5 000 Go par Terrien environ [13] (chiffre qui serait donc atteint en quelques semaines si le Terrien devenait habitant d'une ville intelligente).

Rappelons enfin que les coûts environnementaux associés au déploiement des infrastructures interviendront nécessairement avant le moindre bénéfice des nouveaux usages. Sans compter l'inertie inhérente à la nécessité de « faire système » pour délivrer les résultats espérés. Ainsi, l'exemple des voitures autonomes, pour lesquelles il faudra attendre le renouvellement quasi intégral du parc automobile – soit dix ou quinze ans « après leur généralisation » [14] – pour voir disparaître accidents ou embouteillages. Ainsi, sans doute, de l'articulation à trouver entre énergies renouvelables, bâtiments et véhicules électriques, complexe à déployer et à généraliser – y compris dans son modèle économique.

Effet rebond

Reste l'écueil le plus épineux, lié aux usages. Certes, le déploiement technologique pourrait offrir des gains d'efficacité, des « économies unitaires » substantielles, pour chaque service ou acte de consommation, en énergie et/ou en ressources. Mais toute la trajectoire technologique de l'humanité, depuis deux siècles, montre que cette efficacité technologique, rapidement convertie en « efficacité économique » (baisse des prix), fait augmenter les volumes consommés, et donc la facture environnementale totale. L'offre, plus efficace et plus compétitive, crée sa propre demande : cet « effet rebond » [15] a été montré dès les années 1860 par l'économiste Stanley Jevons pour les machines à vapeur.

Un effet toujours d'actualité et qui concerne tous les secteurs : le covoiturage longue distance n'a pas réduit la consommation de carburant mais développé les opportunités de transport ; les voitures ont des motorisations plus efficaces, mais deviennent plus lourdes et plus performantes ; dans les bâtiments rénovés et mieux isolés, la température de confort des habitants augmente, et tout ou partie des gains théoriques sont perdus ; et dans le numérique, les progrès unitaires sont phénoménaux, mais l'augmentation des besoins l'est encore plus, conduisant à une empreinte environnementale croissante.

Il est à craindre qu'il en sera de même pour une grande partie des applications de la *smart city* : la voiture autonome sera-t-elle un outil au service du covoiturage du quotidien, ou un « bureau mobile » permettant d'habiter encore plus loin de son travail ?

Vers une résilience technique et sociale

Sans accompagnement réglementaire ou fiscal, l'efficacité technologique ne fera donc pas de miracle, au contraire sans doute ; et il n'y a certainement pas bijection entre *smart*, numérique et transition environnementale. Même bardées d'objets communicants, les métropoles ne seront jamais « vertes », restant vulnérables du fait d'une concentration humaine trop grande, aujourd'hui face aux crises sanitaires, demain sans doute face aux enjeux climatiques.

Se pose également la question de la résilience, face à un monde au devenir plus incertain : est-il raisonnable de confier, pour des raisons d'efficacité ou de praticité, notre destin (la distribution d'eau potable, d'énergie, les systèmes de transports, etc.) à des dispositifs technologiques toujours plus nombreux, toujours plus interconnectés et complexes, dépendant de réseaux de production

(13) De l'ordre de 40 zettaoctets pour un peu moins de 8 milliards de Terriens.
(14) Si tant est que cela soit possible économiquement, ce qui fait largement débat ; voir la position de Carlos Tavares, PDG de Stellantis, par exemple.
(15) r.wikipedia.org/wiki/Effet_rebond_(économie)

ultra segmentés et mondialisés, de se retrouver ainsi plus exposés aux risques de cybersécurité, de ruptures d'approvisionnement, de contrôle par des puissances étrangères ?

Au lieu de rester fascinés devant les perspectives de l'innovation *high-tech*, l'idée pourrait être d'amorcer une démarche plus "*low-tech*", visant à l'économie de ressources, à la sobriété à la source, aux réflexions sur le juste besoin. Il ne s'agirait pas de revenir à la bougie, bien sûr, mais de faire preuve de « techno-discernement », de faire le tri pour n'utiliser les technologies – et donc les précieuses ressources qu'elles mobilisent – que là où elles sont indispensables ou là où elles apportent un avantage indiscutable.

Qu'est-ce qu'un besoin ou un service « indispensable » ou essentiel – sachant que les normes sociales, les référentiels évoluent profondément et en permanence ? Évidemment, il y aura là matière à débats, dans l'opportunité et la manière de « trier ». Pourtant, on sent bien, intuitivement, que certains usages relèvent plus du gadget que d'autres (le réfrigérateur qui fait les courses tout seul, les interrupteurs qui obéissent à la voix…), ou consistent à remplacer du travail humain (le bâtiment bardé d'automatismes, ce qui permet de se passer du concierge) ou du lien social (bracelets d'alerte pour personnes âgées à domicile ou distributeur connecté de croquettes pour chat, qui évitent d'avoir à tisser des relations de bon voisinage)… Dans d'autres cas, lorsqu'il y a des enjeux de surveillance d'installations et de sécurité des personnes par exemple, il sera difficile de nier la véritable « utilité sociale » d'objets connectés en permanence.

C'est donc une réflexion profonde qu'il faudra mener, sur nos besoins, nos usages, nos modes d'organisation, de production et de consommation, nos normes sociales et culturelles, nos exigences aussi (rapidité de livraison ou de téléchargement… acceptation d'absence d'information, de fonctionnement perturbé…). Et plutôt que miser sur l'enrichissement technologique de nos vies et de nos métropoles, amorcer dès à présent un programme de relocalisation (de ce qui peut l'être) au profit d'une plus grande maîtrise locale ; de « démétropolisation » et de décentralisation au profit d'une plus grande résilience, d'une proximité et d'une reconnexion aux processus naturels ; de ralentissement au profit de rythmes de vie plus apaisés ; de simplification au profit d'une plus grande autonomie personnelle et collective.

Une piste chaotique, mais potentiellement enthousiasmante, qui demandera bien plus d'intelligence que pour concevoir et installer des capteurs partout, explorer les arcanes du *machine learning* et sonder les abîmes du *big data*.

Les enjeux éthiques des objets communicants personnels

Par **Christine BALAGUÉ**
Professeur en sciences de gestion à Institut Mines-Télécom Business School,
Co-titulaire de la Chaire Good in Tech (www.goodintech.org)

L'année 2017 constitue une période charnière durant laquelle le nombre d'objets connectés dans le monde a dépassé le nombre d'humains sur notre planète. Cette évolution vers un monde du « tout connecté », souvent fondé sur une vision de solutionnisme technologique, pose plusieurs enjeux environnementaux et sociétaux majeurs.

Une taxonomie nécessaire des objets communicants et de leurs usages

Le marché de l'Internet des objets regroupe les appareils physiques qui sont connectés à Internet et capables de communiquer entre eux. Selon l'entreprise américaine de conseil Gartner, il existera 25 milliards d'objets connectés dans le monde fin 2021, le marché connaissant une forte croissance. D'ici à 2025, la prédiction du marché global de l'Internet des objets, selon le Market Data Forecast, est de 875 milliards de dollars, avec une progression annuelle de 26,9 %. Cependant, une analyse plus précise des chiffres du marché de l'Internet des objets permet d'effectuer deux remarques.

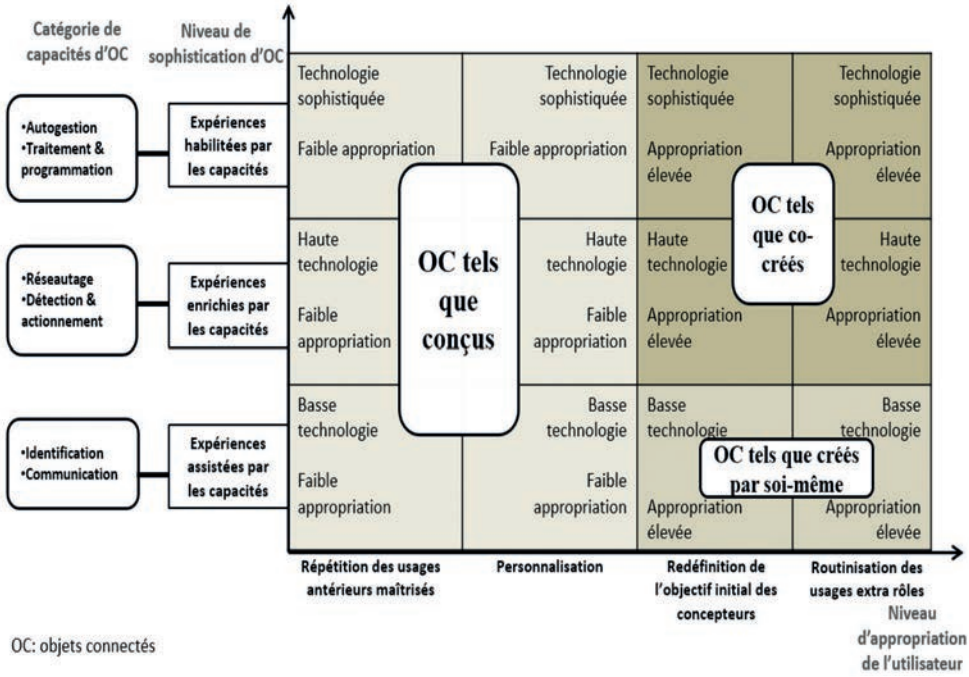
La première porte sur les prévisions de marché, qui diffèrent d'un institut à l'autre (les prédictions pour 2020 variaient entre 18 milliards et 78 milliards d'objets connectés…), et qui ne génèrent pas de consensus, excepté sur le constat d'une forte croissance. De même, en ce qui concerne le type d'« objets », la place des dispositifs mobiles (*smartphones* ou tablettes) n'est pas homogène selon les études. Ceux-ci sont exclus dans certaines définitions de l'objet connecté (McKinsey Global Institute, 2015 ; Oberländer, 2018), et inclus dans d'autres (Benghozi, Bureau & Massit-Folléa, 2015), même si la tendance est à la distinction entre objets connectés et téléphonie mobile par exemple.

La deuxième remarque porte sur le paradoxe entre données de marché et usages. L'étude 2021 de l'Arcep (Autorité de régulation des communications électroniques, des postes et de la distribution de la presse) sur la diffusion des technologies de l'information et de la communication dans la société française, qui s'appuie sur une enquête du Credoc (Centre de recherche pour l'étude et l'observation des conditions de vie), montre que 37 % des Français (chiffre relativement faible encore) sont équipés dans leur foyer d'au moins un objet connecté, avec des usages divers : 23 % déclarent posséder un objet connecté relatif à la santé, 17 % un objet connecté dans l'électro-ménager, 15 % un objet connecté pour la sécurité, et 15 % un objet connecté de domotique.

Ces deux constats montrent qu'on doit distinguer les différents types d'objets connectés de leurs usages pour bien en comprendre les enjeux. Pour cela, nous avons élaboré une taxonomie des objets connectés publiée en 2021 [(1)], fondée sur un état de l'art pluridisciplinaire. Une première dimension distingue les objets connectés suivant six caractéristiques fonctionnelles : autogestion (capacité à apprendre à partir d'expériences antérieures pour optimiser son fonctionnement) ; traitement et programmation (capacité à exécuter des instructions et à programmer des tâches) ;

(1) ZHONG Z. & BALAGUÉ C. (2021), « Comprendre les objets connectés grand public : proposition d'une taxonomie centrée sur l'utilisateur », *Vie et Sciences de l'entreprise*, n° 211-212, pp. 72-89, https://www.cairn.info/revue-vie-et-sciences-de-l-entreprise-2021-1-page-70.htm

détection (capacité à la collecte de données) et actionnement (capacité à provoquer un changement sur sa propre structure) ; réseautage (capacité à échanger des données grâce à la mise en réseau d'objets) ; communication (capacité à signaler son état ou son environnement) ; identification (capacité à s'identifier aux autres systèmes grâce à une identité unique). Une deuxième dimension de la taxonomie distingue trois niveaux d'expériences utilisateurs : les expériences assistées (interactions limitées avec l'objet qui est souvent simple), les expériences enrichies (les utilisateurs interagissent avec l'objet et tirent parti de ses capacités technologiques pour façonner leur expérience) et les expériences habilitées par les capacités de l'objet (niveau d'expérience le plus sophistiqué, les utilisateurs participent activement à la co-création d'expériences). Une troisième dimension de la taxonomie distingue cinq niveaux d'appropriation (répétition d'usages antérieurs maîtrisés, personnalisation, redéfinition de l'objectif initial des concepteurs, routinisation et stabilisation des usages).



Taxonomie des objets connectés (Source : Zhong et Balagué, 2021)

Cette taxonomie multicritères, croisant capacités techniques et usages, montre qu'on ne peut parler d'objets connectés ou communicants en général, mais qu'on doit les distinguer sur des critères à la fois fonctionnels et d'usage. Il est également nécessaire d'intégrer les utilisateurs autrement que par des scenarios d'usages prédéfinis (Balagué, 2018), afin de bien comprendre les différentes dimensions du marché des objets connectés et ses enjeux.

Les risques liés à la captation massive de données

L'Internet des objets personnels permet de collecter des données à partir des capteurs présents dans ces objets. Ces données peuvent être aussi analysées localement ou dans un *cloud*, voire partagées avec d'autres objets connectés. Le volume des données créées par les connexions des objets connectés devrait, selon le cabinet IDC, s'élever, en 2025, à 90 zettaoctets (1 zettaoctet équivaut à 1 milliard de téraoctets), ce qui est considérable. On parle alors de données massives.

L'un des catalyseurs de la collecte massive de données *via* des objets connectés est le déploiement actuel de la 5G dans la plupart des pays développés. Cette technologie permet en effet de connecter en temps réel plusieurs millions d'objets connectés simultanément, dont les données sont envoyées et stockées dans un *cloud* pour être ensuite traitées par des programmes informatiques. D'un point de vue utilisateur, l'un des risques majeurs liés aux objets connectés combinés au réseau 5G est donc la collecte et le stockage en temps réel dans un *cloud* de l'ensemble de ses activités, avec ainsi l'apparition de *data-clones* d'individus dans le *cloud*. Dans ce contexte technologique, l'enjeu du respect des données personnelles (*privacy* ou vie privée des utilisateurs) devient majeur. Quelles garanties auront les utilisateurs sur les traitements de données qui seront menés ? Comment s'assurer du bon respect du Règlement général sur la protection des données (RGPD) mis en place en Europe en 2018, en particulier le consentement explicite concernant la collecte, le stockage et l'accès aux données ? Quelles seront les protections dans d'autres pays qu'en Europe, où le RGPD n'existe pas ? Ces questions sont d'autant plus importantes que les objets connectés s'implantent, notamment, dans des lieux de la vie personnelle, comme la maison (avec le concept de maison connectée, regroupant des appareils électroménagers, informatiques, compteurs d'énergie, ou encore de domotique, pouvant être connectés entre eux ou reliés à une enceinte connectée) ou encore la voiture (véhicule connecté). Les chercheurs Meyer-Waarden et Cloarec (2021) ont de plus montré que les préoccupations des utilisateurs au sujet de la *privacy* affectent négativement leur confiance dans la technologie et sa sécurité, ainsi que leur intention d'usage.

La sécurité des objets connectés est également un enjeu éthique primordial, notamment pour certaines applications de données sensibles comme c'est le cas dans la santé. La fonctionnalité de connexion, caractéristique principale des objets connectés, les rend vulnérables à des failles de sécurité, générant un risque de *hacking* des données et/ou de réutilisation de celles-ci à des fins malveillantes, comme la revente de ces données sur le *dark web*. Plusieurs secteurs spécifiques présentent des risques plus élevés pour les utilisateurs, tels le transport (par exemple, si un hackeur prend le contrôle du véhicule connecté) ou encore la santé (piratage des données de patients diabétiques ou cardiaques possédant des dispositifs connectés par exemple). En France, le règlement sur les dispositifs médicaux oblige les fabricants à mettre au point des niveaux de sécurité forte. Cependant, les enjeux de sécurité des objets connectés constituent encore des verrous techniques sur lesquels de nombreux chercheurs travaillent aujourd'hui.

Enfin, la fiabilité des données représente toujours sur certains marchés un enjeu important, des capteurs de plusieurs marques ou fabricants d'objets connectés pouvant fournir des chiffres différents (par exemple sur la mesure de la fréquence cardiaque de l'utilisateur) ou les capteurs pouvant à un moment donné devenir défaillants. Une analyse de la qualité des données issues d'objets connectés est donc nécessaire pour développer la confiance des utilisateurs et la pérennité du marché, comme le proposent Byabazaire *et al.* (2020).

Des données pour quels traitements ? Les enjeux éthiques des algorithmes

Les traitements des données collectées *via* des objets connectés reposent généralement sur des algorithmes plus ou moins complexes, selon l'application visée. Dans le cadre d'objets communicants personnels (généralement dans la maison, dans son véhicule, sur ou avec soi), les données nourrissent par exemple des algorithmes de recommandations de services (ainsi, la détection de produits manquants dans un frigidaire connecté peut générer une recommandation de listes de courses sur un site de *e*-commerce ; l'analyse des données issues des capteurs de consommation d'énergie au sein du domicile peut générer des algorithmes de recommandations de baisse de dépenses énergétiques). Lorsque les données comportent un historique important et/ou portent sur un nombre important d'utilisateurs, des algorithmes d'intelligence artificielle,

utilisant le *machine learning*, sont utilisés (par exemple, les algorithmes de traitement automatique du langage utilisés pour apporter des réponses aux requêtes des utilisateurs sur une enceinte connectée, de type Google Home ou Alexa). Ces traitements algorithmiques présentent plusieurs enjeux éthiques. Le premier concerne les risques liés aux biais des données nourrissant l'algorithme d'apprentissage, qui peuvent entraîner des résultats peu fiables des algorithmes. Une deuxième conséquence préjudiciable aux utilisateurs est le risque de discrimination de certaines populations *via* le traitement algorithmique, générant des injustices. Le troisième enjeu porte sur les risques liés à l'opacité des systèmes. Du point de vue de l'utilisateur, la collecte de données d'objets connectés, la manière dont ces données sont traitées par l'algorithme, le type de traitement effectué, n'est pas transparent. À l'ère de la 5G et des données massives collectées, les potentiels croisements de données sont infinis, et les risques d'atteinte à la vie personnelle sont réels. Pour répondre à cet enjeu, il est nécessaire de mettre au point des algorithmes « auditables » par les autorités compétentes (souvent de régulation) et explicables aux utilisateurs, qui doivent pouvoir comprendre leur fonctionnement. La multiplicité des objets connectés au sein de la maison, combinée à des enceintes connectées de type Google Home (ou Alexa) et aux différents services de Google (ou d'Amazon), rend cette explicabilité indispensable pour garantir une limite aux effets potentiels négatifs sur les utilisateurs. Cet enjeu est aujourd'hui la thématique d'un courant de recherche pluridisciplinaire très actif sur l'éthique de l'intelligence artificielle. Enfin, les traitements de données algorithmiques utilisant des données d'objets connectés peuvent contenir parfois les opinions de leurs concepteurs (par exemple, les seuils et les critères pour déclencher une recommandation), qui peuvent porter préjudice.

La valeur d'usage : un concept souvent oublié

Le marché des objets connectés grand public a débuté avec de nombreux produits de bien-être (entre autres, la montre connectée captant le nombre de pas effectués par jour, ou la fréquence cardiaque). Dans cet univers, de nombreux gadgets électroniques sont apparus ces dernières années, en France et dans le monde, apportant plus ou moins de valeur à l'utilisateur. La faible prise en compte par les fabricants de ce critère de valeur d'usage, pourtant bien connu depuis longtemps sur les marchés de consommation, est probablement l'un des facteurs explicatifs du retard de l'adoption des objets connectés, face à une prolifération de l'offre. Ainsi, l'un des enjeux est d'avoir une réelle proposition d'offre de valeur avec des objets connectés, en apportant un réel bénéfice à l'utilisateur, ce qui va être source d'une meilleure appropriation. Dans un article publié en 2020 [(2)], nous avons montré que cette appropriation des objets connectés est un processus dynamique qui s'appuie sur différents types d'interaction entre l'utilisateur et l'objet (sensitif, cognitif, fonctionnel, passif, expressif), s'intensifiant en fonction de la valeur perçue par l'utilisateur (au départ, l'utilisateur n'a qu'une perception de la valeur de l'objet connecté, puis se crée une valeur d'usage en fonction de l'utilisation, s'ensuit une phase de co-production de valeur et enfin une valeur transformative qui génère une appropriation finale de l'objet connecté, celui-ci devenant dans une étape de stabilisation un objet de la vie quotidienne de l'utilisateur). En conséquence, l'un des enjeux éthiques du marché de l'Internet des objets est de déployer des offres de services et de produits à réelle valeur ajoutée pour l'utilisateur, et d'éviter le développement de gadgets électroniques.

Sur certains marchés, la valeur d'usage des objets connectés peut être cependant très forte. Par exemple, les dispositifs connectés pour diabétiques (qui vont jusqu'à des pompes connectées) permettent aux patients de mesurer automatiquement leur glycémie et d'avoir des messages

(2) BENAMAR L., BALAGUÉ C. & ZHONG Z. (2020), "Internet of Things devices appropriation process: The Dynamic Interactions Value Appropriation (DIVA) framework", *Technovation*, Volume 89, January, 102082, https://doi.org/10.1016/j.technovation.2019.06.001

d'alerte, voire de s'injecter directement de l'insuline par la pompe connectée. Ce type de dispositifs est perçu par certains patients comme améliorant nettement leur vie quotidienne.

Développer une innovation numérique responsable des objets connectés en mesurant l'impact environnemental et sociétal

L'impact environnemental du numérique, selon Green IT en 2019, représente 3,8 % des émissions de gaz à effets de serre au niveau mondial (si le numérique était un pays, il aurait deux à trois fois l'empreinte de la France). En 2020, les objets connectés ont représenté 1 % des émissions contre 18 à 23 % estimés en 2025, en raison de la croissance prévue très forte du nombre de ces objets, ainsi que du déploiement de la 5G facilitant leurs usages. En conséquence, un enjeu éthique majeur lié aux objets connectés est de préserver la planète et de limiter l'empreinte carbone liée à la fois à l'élaboration et à l'usage de ces technologies. Plus largement, pour faire face à cet enjeu, il est nécessaire aujourd'hui de développer une innovation éthique et responsable, en élaborant des outils de mesure d'impact sur l'environnement des objets communicants et de leurs usages. En parallèle, des critères d'impact sur la société de ces objets connectés devraient être intégrés dans la Responsabilité sociale des entreprises (RSE), ainsi que des actions à mettre en place afin de limiter les effets négatifs de ces objets.

Bibliographie

BALAGUÉ C. (2018), « Santé : pourquoi certains objets connectés sont un succès et d'autres font un flop », *The Conversation*, février, https://theconversation.com/sante-pourquoi-certains-objets-connectes-sont-un-succes-et-dautres-font-un-flop-87452

BALAGUÉ C. (2018), « Objets connectés, gadgets ou véritables innovations », *L'Abécédaire des institutions*, cahier 116 sur l'e-santé, https://www.labecedaire.fr/editions/labecedaire-institutions-cahier-n116/;https://cloud.flippad.com/flipbook/43953b178a0d143d07a6b28825db38ee31c346cb#Publication/page-5

BENAMAR L., BALAGUÉ C. & ZHONG Z. (2020), "Internet of Things devices appropriation process: The Dynamic Interactions Value Appropriation (DIVA) framework", *Technovation*, Volume 89, January, 102082 https://doi.org/10.1016/j.technovation.2019.06.001

BENGHOZI P. J., BUREAU S. & MASSIT-FOLLÉA F. (2015), *L'Internet des objets/The Internet of Things: Quels enjeux pour l'Europe ?/What Challenges for Europe?*, Éditions MSH.

BYABAZAIRE J., O'HARE G. & DELANEY D. (2020), "Data quality and trust: A perception from shared data in IoT", *IEEE*, 978-1-7281-7440-2/20/$31.00

MEYER-WAARDEN L. & CLOAREC J. (2021), "'Baby, you can drive my car': Psychological antecedents that drive consumers' adoption of AI-powered autonomous vehicles", *Technovation*, https://doi.org/10.1016/j.technovation.2021.102348

OBERLÄNDER A. M., RÖGLINGER M., ROSEMANN M. & KEES A. (2018), "Conceptualizing business-to-thing interactions – A sociomaterial perspective on the Internet of Things", *European Journal of Information Systems*, 27(4), pp. 486-502.

VANSIMAEYS C., BENAMAR L. & BALAGUÉ C. (2021), "Digital health and management of chronic disease: A multimodal technologies typology", *International Journal of Health Planning and Management*, pp. 1-19, https://doi.org/10.1002/hpm.3161

ZHONG Z. & BALAGUÉ C. (2021), « Comprendre les objets connectés grand public : proposition d'une taxonomie centrée sur l'utilisateur », *Vie et Sciences de l'entreprise*, 211-212, pp. 72-89, https://www.cairn.info/revue-vie-et-sciences-de-l-entreprise-2021-1-page-70.htm

Le traçage cyberphysique des personnes et la vie privée

Par **Mathieu CUNCHE**
Maître de conférences à l'INSA-Lyon

Depuis l'apparition de l'iPhone en 2007, une grande partie de la population porte en permanence sur elle un « ordiphone », qui a été récemment rejoint dans notre sphère physique personnelle par d'autres appareils connectés (écouteurs, bracelets, capteurs de sport ou de santé, etc.). Ces appareils ont en commun d'inclure une ou plusieurs technologies sans-fil : Wi-Fi, Bluetooth et sa variante basse consommation, le Bluetooth Low Energy (BLE).

Depuis le début des années 2010, on a vu apparaître des systèmes traçant les utilisateurs dans le monde physique *via* la collecte des signaux radio émis par ces appareils sans-fil compagnons. Initié aux États-Unis par l'entreprise Euclid Analytics [(1)], le concept de traçage cyberphysique s'est rapidement développé au point de déclencher des réactions des autorités de contrôle, du législateur et des fabricants d'appareils.

Ce traçage cyberphysique, souvent pratiqué à l'insu des individus concernés, est particulièrement intrusif, et est une menace évidente pour la vie privée. Cette problématique de protection des données personnelles peut être abordée suivant deux axes : premièrement, une approche légale et réglementaire, avec une évolution des règles pour encadrer ces nouvelles techniques de collecte de données personnelles ; et deuxièmement, une approche technologique, avec une réflexion sur l'évolution des standards et la mise en œuvre de contre-mesures.

Traçage cyberphysique : fonctionnement et applications

Le traçage cyberphysique tel qu'on l'entend ici repose sur les technologies sans-fil (Wi-Fi et Bluetooth) intégrées dans nos appareils portables (ordiphones, bracelets connectés, écouteurs, etc.). Ces appareils se comportent comme des balises radio en émettant régulièrement des courts messages qui contiennent un identifiant unique et propre à chaque appareil (on parle d'adresse MAC). Cette diffusion de message est continue, et est présente même quand l'appareil n'est pas connecté ; en effet, l'émission de ces messages fait partie d'un mécanisme qui permet à notre appareil de découvrir les réseaux ou équipements à portée, auxquels il pourrait éventuellement se connecter.

Ces messages de découverte sont émis en clair (*i.e.,* non protégés par un chiffrement), et leur contenu, en particulier l'identifiant propre à l'appareil, peut être capté à distance (parfois à plusieurs dizaines de mètres) par un appareil dédié appelé *sniffer.* En collectant les signaux émis par nos appareils, ces *sniffers* sont en mesure de détecter la présence de personnes et de suivre leurs déplacements (voir Figure 1).

(1) https://archive.thinkprogress.org/meet-the-real-life-tracking-database-that-could-include-you-ddba626eb210/

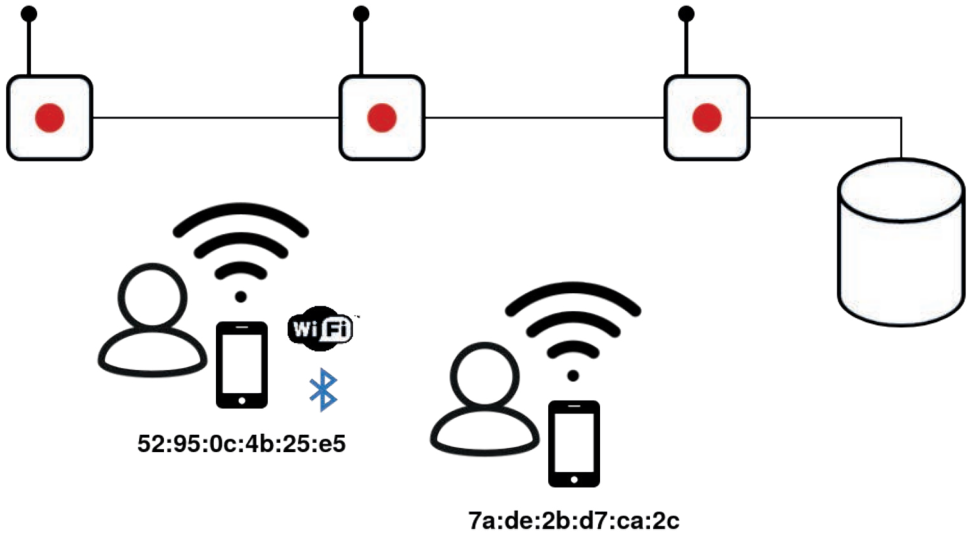


Figure 1 : Système de traçage cyberphysique basé sur le Wi-Fi et/ou le Bluetooth. Les signaux émis par les ordiphones sont captés par des *sniffers*, permettant un suivi des porteurs de ces appareils (Source : D. R.)

Ces systèmes de traçage cyberphysique ont trouvé une diversité d'applications. Par exemple dans le domaine des transports avec l'observation des flux sur les axes routiers [2], ou encore dans les transports en commun comme dans le métro londonien [3]. Un autre domaine d'application est les enseignes commerciales qui utilisent ces systèmes dans le cadre d'applications dites d'*analytics*, donnant lieu à des mesures de la clientèle (nombre de visiteurs, durée et fréquence des visites, etc.). Sur le modèle du traçage en ligne, le traçage cyberphysique permet de profiler les personnes et de leur soumettre de la publicité ciblée sur leurs ordiphones [4] ou dans le monde physique *via* des écrans publicitaires [5].

Enjeux légaux et réglementaires

Le traçage cyberphysique et la collecte de données qui en découle sont soumis à un ensemble de règles, et en particulier au Règlement général sur la protection des données (RGPD), entré en application en 2018. Les données captées par ces systèmes, et notamment les identifiants d'appareils, sont des données à caractère personnel au sens du RGPD. Ainsi, il découle de cette qualification un ensemble d'interdictions et d'obligations liées à leurs collectes et leurs traitements. Ces obligations peuvent être levées si les données sont rendues anonymes, cependant cette tâche s'avère difficile à mettre en œuvre sur ce type de données.

La CNIL (Commission nationale de l'informatique et des libertés) a proposé une liste de règles [6] applicables aux systèmes de « mesure d'audience et de fréquentation dans des espaces accessibles au public ». Elle y rappelle en particulier les exigences en termes d'information des personnes et d'exercice du droit d'opposition et de rectification. Elle précise également l'importance de l'anonymisation et de la pseudonymisation des données, et rappelle les bonnes pratiques en la

(2) https://www.mobilite-intelligente.com/ressources/technologies/localisation/captures-dadresses-bluetooth
(3) https://techcrunch.com/2019/05/22/mind-the-privacy-gap/
(4) https://info.haas-avocats.com/droit-digital/smartphone-et-g%C3%A9olocalisation-un-dispositif-sous-haute-surveillance-de-la-cnil
(5) https://qz.com/112873/this-recycling-bin-is-following-you/
(6) https://www.cnil.fr/fr/dispositifs-de-mesure-daudience-et-de-frequentation-dans-des-espaces-accessibles-au-public-la-cnil

matière. En ce qui concerne la base légale, l'invocation de l'intérêt légitime est considéré comme valable si l'anonymisation intervient à court terme ; ce qui implique que les données pourront être collectées sans le consentement des personnes. Par contre, en l'absence d'une anonymisation à court terme, l'intérêt légitime n'est plus acceptable, et un consentement informé, libre et spécifique est alors nécessaire.

Plusieurs autorités de protection européennes, dont la CNIL, ont pris des décisions au sujet de systèmes de traçage cyberphysique. Ces décisions illustrent les motivations des « traceurs » et présentent ce qui n'est pas acceptable pour les autorités en l'état actuel de la législation. En 2015, la CNIL a refusé un projet d'estimation de flux piétons porté par JCDecaux et Fidzup [7] à cause d'insuffisances au niveau de l'anonymisation des données et de l'information des personnes. En 2018, cette même entreprise Fidzup a été mise en demeure par la CNIL [8] pour son système de profilage et de ciblage publicitaire mobile basé sur des systèmes de traçage cyberphysique déployés chez des commerçants. Cette mise en demeure repose sur l'absence de base légale pour ce traitement de données, et en particulier l'absence de consentement. Aux Pays-Bas, la ville d'Enschede s'est vu infliger une amende de 600 000 euros pour avoir mis en place un système qui permettait de tracer, et non pas seulement de compter, les passants dans le centre-ville [9]. On voit donc que l'absence d'anonymisation à court terme et la base légale sont les motifs principaux de ces interdictions et sanction (dans le cas des Pays-Bas) de la part des autorités de protection.

Un nouveau règlement européen, baptisé *ePrivacy*, pourrait bientôt changer cette situation. Ce règlement vient compléter le RGPD sur le cas particulier des communications électroniques. La problématique des systèmes de traçage cyberphysique *via* des signaux sans-fil y est abordée dans l'article 8 intitulé « Protection des informations stockées dans les équipements terminaux des utilisateurs finaux ou liées à ces équipements », où l'on peut lire :

« 2- La collecte d'informations émises par l'équipement terminal pour permettre sa connexion à un autre dispositif ou à un équipement de réseau est interdite, sauf si :

(cc) elle est pratiquée exclusivement dans le but d'établir une connexion et pendant la durée nécessaire à cette fin ; ou

(dd) un message clair et bien visible est affiché, indiquant les modalités et la finalité de la collecte et la personne qui en est responsable, fournissant les autres informations requises en vertu de l'article 13 du règlement (UE) 2016/679 lorsque la collecte porte sur des données à caractère personnel, et précisant les mesures éventuelles que peut prendre l'utilisateur final de l'équipement terminal pour réduire au minimum la collecte ou la faire cesser ».

Ainsi, en l'état actuel de ce règlement, un affichage informant sur le traçage et les moyens de s'opposer ou de limiter la collecte de données serait suffisant. On note que cette position est beaucoup plus libérale que celle de la CNIL qui exige pour le moment une anonymisation à court terme ou un consentement.

Enjeux technologiques

Si les protections réglementaires ne sont plus suffisantes, la technologie à la source du problème peut nous fournir des solutions pour échapper à ce traçage.

(7) https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000031159401/
(8) https://www.frenchweb.fr/la-cnil-met-en-demeure-deux-startups-de-ciblage-publicitaire/332384
https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000037217124/
(9) https://datanews.levif.be/ict/actualite/la-ville-neerlandaise-d-enschede-se-voit-infliger-une-amende-gdpr-pour-du-tracage-wifi/article-news-1420015.html?cookie_check=1626181080

Adresses aléatoires

Face à cette menace de traçage accentuée par la généralisation des objets portables intégrant Wi-Fi ou Bluetooth, une solution a été proposée. Cette solution, appelée « adresse aléatoire », repose sur la substitution de l'identifiant permanent présent dans les signaux par un identifiant aléatoire et temporaire. Ainsi, l'appareil utilise consécutivement des pseudonymes indépendants qui rendent inopérants les systèmes de traçage cyberphysique.

Fabricants et développeurs d'OS

L'intégration des mécanismes anti-traçage tels que les adresses aléatoires est la responsabilité des fabricants de systèmes d'exploitation (OS) mobiles, comme Apple pour iOS et Google pour Android. De plus, les fabricants sont souvent amenés à adapter le système d'exploitation, et il est de leur responsabilité de veiller à ce que les modifications qu'ils apportent au système n'affectent pas les protections anti-traçage. Ces mécanismes de protection sont aujourd'hui intégrés dans une majorité des appareils récents. Néanmoins, il a pu être observé des failles qui remettaient en cause l'efficacité de ces protections. En effet, l'utilisation d'une adresse aléatoire n'est pas suffisante à elle seule, et son intégration est loin d'être évidente.

Au-delà des mécanismes de protection, il est nécessaire de fournir à l'utilisateur des moyens de contrôle clairs et efficaces. Dans le cadre du traçage *via* Wi-Fi et Bluetooth, il est parfois suggéré d'éteindre les fonctionnalités sans-fil de l'appareil pour échapper au traçage. Cependant, cette opération ne désactive que partiellement les fonctionnalités sans-fil et n'empêche pas le traçage [(10)]. Des efforts sont donc nécessaires pour informer les utilisateurs de cette collecte de données et pour leur fournir les moyens de s'y opposer.

Standardisation

Les technologies telles que le Wi-Fi et le Bluetooth sont définies par des standards techniques sur lesquels les fabricants se basent pour développer leurs produits. Ces documents déterminent donc les exigences sur les fonctionnalités auxquelles doivent satisfaire les appareils voulant apparaître comme conformes à ces normes. Ainsi, ces standards techniques sont en capacité d'imposer la mise en place de mesures de protection à une très large échelle.

Au sein de ces standards, la sécurité des communications est un enjeu qui a été considéré dès leur genèse, et une large part des spécifications est dédiée à la description de mécanismes de sécurité (par exemple WPA – Wi-Fi Protected Access). Comparativement, on retrouve peu d'éléments liés aux problématiques de vie privée telles que les protections contre le traçage cyberphysique. Si l'on s'intéresse au cas de l'adresse aléatoire, son introduction dans le Bluetooth coïncide avec l'introduction du BLE en 2010, tandis que son introduction dans le 802.11 (Wi-Fi) s'est faite beaucoup plus tardivement, en 2018 [(11)]. Depuis peu, les enjeux de protection des données personnelles commencent à prendre de l'importance au sein de ces standards, avec notamment la constitution de groupes de travail [(12)] sur le sujet et la publication d'un document de l'IEEE 802 sur les considérations en matière de protection de la vie privée dans ces standards [(13)].

(10) https://linc.cnil.fr/fr/desactiver-le-wi-fi-android-ne-nous-preserve-pas-du-tracage
(11) https://standards.ieee.org/standard/802_11aq-2018.html
(12) "IEEE P802.11 - Randomized and Changing MAC address (RCM) Study Group (SG)", https://www.ieee802.org/11/Reports/rcmtig_update.htm
(13) "IEEE 802E-2020 - IEEE Recommended Practice for Privacy Considerations for IEEE 802® Technologies", https://standards.ieee.org/standard/802E-2020.html

Conclusions & perspectives

Le traçage des personnes est rendu possible par une adoption croissante d'appareils équipés de technologies sans-fil. Les problématiques de vie privée associées font apparaître des enjeux technologiques, mais aussi légaux et réglementaires. Il est essentiel de considérer ces problématiques le plus tôt possible pour mettre en place des protections adéquates. Ceci est particulièrement important pour les aspects technologiques, car, une fois définis, les standards sont difficilement modifiables et demeurent en vigueur pendant de longues périodes.

Au-delà du Wi-Fi et du Bluetooth, dont il a principalement été question dans cet article, une meilleure prise en compte de problématiques de vie privée est nécessaire dans le développement des futures technologies sans-fil. En effet, Wi-Fi et Bluetooth sont progressivement rejoints par d'autres technologies qui pourraient être à la source de nouvelles menaces pour la vie privée. Par exemple, l'Ultra Wide Band (UWB), qui permet d'estimer les distances entre appareils avec une précision de quelques centimètres, est progressivement intégrée dans les appareils mobiles. L'UWB pourrait donc favoriser un traçage beaucoup plus fin que ce qui est réalisé actuellement par les technologies Wi-Fi et Bluetooth.

Bibliographie

CELOSIA G. (2020), *Privacy challenges in wireless communications of the Internet of Things,* thèse de doctorat, Université de Lyon, INSA-Lyon.

DEMIR L., CUNCHE M. & LAURADOUX C. (2014), "Analysing the privacy policies of Wifi Trackers", *Proceedings of the 2014 Workshop on Physical Analytics*, New York, NY, USA, pp. 39-44.

MATTE C. (2017), *Traçage Wi-Fi : Attaques par prise d'empreinte et contre-mesures*, thèse de doctorat, Université de Lyon, INSA-Lyon.

MATTE C. & CUNCHE M. (2016), « Traçage Wi-Fi : applications et contre-mesures », *GNU/Linux Magazine*, n°84, hors série.

MAVROUDIS V. & VEALE M. (2018), "Eavesdropping whilst you're shopping: Balancing personalisation and privacy in connected retail spaces", *Living in the Internet of Things: Cybersecurity of the IoT – 2018,* pp. 1-10.

Les enjeux de souveraineté des objets communicants

Par **Didier DANET**
Maître de conférences en sciences de gestion, détaché de l'Université Rennes 1 auprès de l'Académie militaire de Saint-Cyr
Et **Alix DESFORGES**
Chercheuse en postdoctorat à l'Université Paris 8 au sein du projet GEODE (géopolitique de la datasphère)

Introduction

Depuis une dizaine d'année, les débats sur les enjeux de souveraineté à l'ère numérique prolifèrent autant au sein des milieux politiques, stratégiques et académiques. Historiquement, l'expression « souveraineté numérique » a été largement mobilisée en France principalement pour dénoncer la suprématie des entreprises américaines en matière numérique. Toutefois, cette expression en apparence simple cache un concept aux multiples facettes (Danet et Desforges, 2020). Or les enjeux majeurs soulevés par l'irruption et la généralisation des outils et des données numériques pour l'exercice de la souveraineté des États requièrent clarté et précision pour en comprendre les mécanismes et dynamiques. Les objets communicants visent principalement à simplifier et à faciliter un grand nombre de processus et démarches. En apparence souvent anodins, ils bouleversent davantage qu'il n'y parait la vie quotidienne des citoyens, mais aussi des organisations et des États. Ils posent des questions en termes de sécurité et de confidentialité pour les consommateurs et les usagers, mais au-delà soulèvent des enjeux de souveraineté en raison de leur massification et de leur pénétration dans tous les aspects de la vie quotidienne.

Pour cet article, nous avons choisi de nous interroger sur les enjeux soulevés par les objets communicants dans le cadre de la souveraineté dans son sens le plus strict, c'est-à-dire la défense des intérêts de la nation et l'exercice de compétences de l'État (Norodom, 2020a). En quoi l'irruption des objets communicants va-t-elle véritablement changer la manière dont la question de la souveraineté se pose aujourd'hui ? Le changement quantitatif d'échelle est en soi préoccupant : plusieurs milliards d'objets captant et transmettant des données de toutes sortes ne sont pas sans conséquences sur la capacité de l'État à exercer ses prérogatives régaliennes internes et externes.

L'article présentera dans un premier temps une analyse des principaux enjeux de souveraineté soulevés par les objets communicants. Nous y verrons que, loin de générer de nouvelles problématiques, la prolifération en cours des objets communicants vient en réalité accélérer et consolider des dynamiques déjà à l'œuvre dans le processus de numérisation des sociétés humaines, par exemple dans les rapports entre États et entreprises du numérique. Nous reviendrons dans un second temps sur l'exemple de la sonnette connectée d'Amazon, qui illustre parfaitement ces dynamiques.

Objets communicants : l'accélération et le renforcement de dynamiques existantes

La massification des objets communicants et leur utilisation dans tous les pans de la vie quotidienne soulèvent trois principaux enjeux de souveraineté pour les États : la sécurité, la maîtrise des données

et la place d'acteurs privés, au premier rang desquels les grandes entreprises du numérique pour l'exercice des pouvoirs régaliens.

La sécurité des objets communicants

Le premier enjeu soulevé par les objets communicants et leur prolifération est celui de leur cybersécurité. En effet, ces objets, principalement conçus pour la vie quotidienne, le sont souvent bien loin de toute préoccupation de sécurité. Décrits comme le « maillon faible de la cybersécurité » (Benhamou, 2021), les objets communicants constituent autant de nouveaux vecteurs d'attaques pour des acteurs malveillants. De plus en plus d'attaques informatiques, notamment des attaques par déni de service, exploitent la très faible, voire souvent inexistante sécurité des objets communicants. En 2016, l'attaque contre la société de gestion DNS Dyn a rendu inaccessibles un grand nombre de sites Internet tels que Twitter, eBay, Netflix, GitHub ou PayPal [(1)]. L'attaque a mobilisé le *botnet* Mirai, dont l'une des spécificités est d'utiliser les objets communicants non sécurisés pour procéder à des attaques en déni de service. Mirai a compté jusqu'à 600 000 objets connectés (Antonakakis *et al*., 2017).

Ainsi, de par leur vulnérabilité aux attaques informatiques, les objets communicants sont devenus une véritable menace en termes de cybersécurité. Or la combinaison de ces dispositifs aux techniques d'attaques existantes participe à l'élévation générale du niveau de menace affectant la sécurité et la stabilité de l'espace numérique dans son ensemble, et plus largement la sécurité nationale (Douzet et Géry, 2020).

La maîtrise des données mise au défi de la massification des objets communicants

La prolifération d'objets communicants conduit à la massification de la production de données de tous types. Cette massification soulève des questions de sécurité pour les consommateurs et les usagers, mais interroge surtout la maîtrise de ces données. En effet, si certaines de ces données peuvent ne pas être sensibles en apparence (contenu d'un réfrigérateur, kilométrage et heure d'utilisation d'une trottinette, etc.), d'autres sont à l'évidence beaucoup plus sensibles (données de santé ou liées à la sécurité du domicile par exemple). Ces données, générées sans même que nous en ayons conscience, peuvent révéler pourtant beaucoup d'informations, que ce soit sur un individu en particulier, offrant d'énormes opportunités de ciblage à des fins commerciales ou d'espionnage, que sur le fonctionnement général d'une organisation quelle que soit son envergure. Elles participent ainsi pleinement au processus de « datafication généralisée » (Cattaruzza, 2019).

En effet, les données (générées par les objets communicants ou non) reflètent les modes d'organisation sociaux et bouleversent les modes de gouvernement des sociétés, avec l'émergence de « nouvelles formes d'expression du pouvoir qui se développent par le biais des outils numériques » (Cattaruzza, 2019). Parmi ces outils, les objets communicants prennent une place de plus en plus importante, par exemple en matière de contrôle des frontières.

Des acteurs privés aux pouvoirs inédits

Le point commun des données générées par les objets communicants est qu'elles sont quasi exclusivement détenues par des acteurs privés, générant ainsi une situation de dépendance des États dans l'exercice d'un certain nombre de leurs compétences régaliennes, par exemple dans la mise en œuvre de leur droit dans l'espace numérique. Perçue comme un réel risque géopolitique, notamment, en France (Danet et Desforges, 2020), cette dépendance est d'autant plus problématique qu'elle intervient à la faveur d'entreprises souvent étrangères qui sont déjà

(1) *HackRead* (2016), "DDoS attack on DNS; Major sites including GitHub PSN, Twitter suffering outage", 21 octobre, https://www.hackread.com/ddos-attack-dns-sites-suffer-outage/

en situation de quasi-monopole sur le marché du numérique. Ces entreprises, que l'on présente trop souvent sous le simple acronyme GAFAM (Google, Apple, Facebook, Amazon et Microsoft), sont perçues comme déjà aussi puissantes que les États (Nocetti, 2019). Les objets communicants et leur massification viennent de fait alimenter des problématiques déjà bien connues sur les questions numériques et sur la façon dont les États exercent leur souveraineté dans bien des domaines (levée de l'impôt, création de la monnaie, gestion des populations, sécurité nationale, etc.) (Norodom, 2020b). Les objets communicants peuvent renforcer la position d'acteurs privés déjà puissants ; des acteurs majeurs du numérique ne manqueront pas de mettre au point des stratégies en vue d'occuper une place centrale dans ces différents domaines, traditionnellement de la responsabilité des États. Mais le changement d'échelle généré par le volume croissant des objets communicants ouvrira des perspectives inédites en termes de services et de compétences, comme l'illustre l'exemple de la sonnette connectée d'Amazon.

L'exemple d'Amazon et de sa sonnette connectée Ring

Cette évolution est déjà largement engagée, notamment aux États-Unis, comme le montre l'exemple de la sonnette connectée Ring d'Amazon. En lui-même, l'objet est assez simple : une sonnette vidéo raccordée avec système audio bidirectionnel et détection de mouvements, cette dernière fonctionnant également de nuit. L'occupant de l'habitation est informé de la présence de visiteurs, de livreurs ou d'intrus grâce à une application dédiée qu'il peut consulter en étant présent chez lui ou à distance. Moyennant un abonnement spécifique très peu coûteux, la sonnette peut réaliser un enregistrement vidéo qui peut être partagé avec le voisinage sur un site dédié, intitulé précisément "Neighbors".

À partir de ce capteur finalement assez commun, Amazon a développé une stratégie qui la place aujourd'hui au cœur du système policier chargé d'assurer la sécurité des citoyens.

L'interconnexion automatique des sonnettes et les échanges de données qui en résultent (les vidéos enregistrées notamment) contribuent à cristalliser des communautés de citoyens vigilants, le périmètre couvert devenant une sorte de "*gated community*" virtuelle, dont Amazon est l'initiateur et l'architecte. Les données qui remontent de ces dizaines de milliers de capteurs sont utilisées de multiples manières. Prosaïquement, elles permettent à Amazon de contrôler la qualité de ses opérations de livraison (à quelle heure le paquet a-t-il été livré ? L'employé l'a-t-il jeté ou l'a-t-il déposé avec précaution ?). Elles sont également cédées à des "*data brokers*" ou à des sociétés partenaires (Facebook par exemple). Elles peuvent surtout permettre à Amazon de se placer comme un prestataire obligé des services de police.

Ce dernier point est bien évidemment le plus lourd de conséquences pour la mise en œuvre des politiques publiques en matière policière.

Centralisant les vidéos captées par les sonnettes dès lors qu'elles perçoivent un mouvement, Amazon dispose de données très anodines (le chat du voisin est passé devant la maison), mais aussi de données plus importantes pour la prévention et la résolution des délits et des crimes. Telle personne inconnue est passée à plusieurs reprises devant un groupe de maisons qui ont été cambriolées. Elle a suivi tel itinéraire, était présente à telle heure à tel endroit… Tous ces indices sont évidemment précieux pour la police chargée de retrouver et de confondre les auteurs des délits et crimes. Il n'est donc pas étonnant que les partenariats se soient multipliés très rapidement entre Amazon et des services de police, couvrant l'ensemble du territoire des États-Unis. En 2018, 40 partenariats avaient été mis en place ; il en existait plus de 2 000 au début de l'année 2021, avec un taux de progression de l'ordre du doublement chaque année. Seuls deux États américains, le Wyoming et le Montana, États ruraux s'il en est, n'avaient pas encore de liens avec Amazon.

La nature et les modalités de ces liens montrent la position centrale de l'entreprise par rapport aux autorités policières.

Tout d'abord, l'entreprise qui collecte les données, en particulier les vidéos, exerce un contrôle de l'accès des services de police à la base qui les contient. Ces derniers peuvent demander à les consulter dans un cadre extrajudiciaire et dans des conditions définies par Amazon. Récemment, l'entreprise a décidé d'instituer des règles de « transparence », la police devant solliciter la consultation par une demande écrite motivée qui sera communiquée aux utilisateurs concernés. Les consultations peuvent également intervenir dans un cadre judiciaire, les modalités étant alors définies par les règles de la procédure pénale, les fameux "*subpoenas*" (ordre d'un juge pour la production d'une pièce ou d'un témoignage). Mais, même dans ce cas, Amazon semble se montrer soucieuse du contrôle de ses bases de données puisqu'elle n'aurait satisfait qu'à moins de 60 % des requêtes judiciaires en 2020.

Surtout, cette maîtrise des données s'accompagne du monopole des outils permettant de les exploiter. Amazon a en effet conçu un logiciel de reconnaissance d'images, Rekognition, qui fonctionne comme un service en nuage ("*cloud-based software as a service*"). Ce service propose nombre de fonctions parmi lesquelles la détection et l'analyse de visages (sexe, tranche d'âge, port de lunettes, émotions…), ou la reconnaissance et l'identification de visages sur des photos ou des vidéos. L'utilité de ce type de logiciel couplé avec les bases de données rassemblées grâce aux sonnettes Ring n'est guère difficile à saisir. Elle n'a d'ailleurs pas échappé aux services de police qui ont été jusqu'à 2020 des clients importants d'Amazon. Mais, l'utilisation du service pour identifier des manifestants du mouvement Black Lives Matter enregistrés par des sonnettes connectées associées à des biais manifestes dans le traitement des images des Noirs américains a conduit l'entreprise à un moratoire renouvelé en mai 2021. Ce moratoire a été suivi par les concurrents d'Amazon, en particulier Microsoft.

Cela revient à dire qu'une entreprise privée, Amazon, se trouve en situation de monopoliser des bases de données immenses, alimentées par des dizaines de milliers de caméras installées à la porte des habitations sur tout le territoire des États-Unis, et elle se réserve l'usage exclusif des logiciels de reconnaissance faciale permettant d'identifier et de tracer toute personne « suspectée » d'avoir commis un « délit », pouvant aller de la livraison non conforme d'un colis à la participation à une manifestation non autorisée ou à un cambriolage nocturne avec violence sur personnes. Mieux équipée et mieux informée que les services de police, elle ne peut qu'en devenir le partenaire obligé, et un partenaire en position de force.

On retrouverait des dynamiques comparables dans d'autres fonctions régaliennes où des acteurs privés pourraient, dans les années qui viennent, chercher à asseoir sur leur capacité d'innovation dans les objets communicants des stratégies visant à occuper une position centrale par rapport aux acteurs publics, qui avaient traditionnellement la maîtrise de la conception et de la mise en œuvre des politiques de l'État. Que l'on songe par exemple à Apple et aux données transmises par les 100 millions de porteurs d'iWatch sur leur activité physique, leur rythme cardiaque ou leur taux d'oxygène dans le sang. Compte tenu du rythme de progression des ventes et de la part d'Apple sur le marché (plus de 50 %, soit cinq fois plus que le deuxième), on peut prédire sans grande difficulté que l'entreprise disposera très rapidement d'un volume de données de santé sans équivalent, et de la capacité à les analyser pour concevoir des services de santé publique.

Conclusion

Au-delà de son aspect quantitatif, l'augmentation brutale du volume des données captées et transmises, la massification à venir des objets communicants devrait s'accompagner de stratégies d'acteurs privés, les entreprises géantes du numérique, pour intervenir dans la conception et

la conduite des politiques publiques, notamment des politiques régaliennes comme la défense et la sécurité, la monnaie ou la santé. On peut penser que ces entreprises chercheront moins à s'approprier la souveraineté des États qu'à se poser en partenaires incontournables des évolutions possibles de ces politiques. Les situations conflictuelles ne sont pas à exclure, comme l'a montré le cas de l'application TousAntiCovid, mais les relations entre acteurs publics et privés seront probablement plutôt de nature partenariale, les États ayant besoin des bases de données et des compétences analytiques des entreprises pour définir les politiques adaptées.

Bibliographie

ANTONAKAKIS M. *et al.* (2017), "Understanding the Mirai Botnet", *Proceedings of the 26th USENIX Security Symposium*, pp. 1093-1110.

BENHAMOU B. (dir.) (2021), *Internet des objets & souveraineté numérique*, Paris, Institut de la souveraineté numérique et AFNIC.

CATTRUZZA A. (2019), *Géopolitique des données numériques,* Paris, Le Cavalier Bleu.

DANET D. & DESFORGES A. (2020), « Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques », *Hérodote*, n°177-178, pp. 179-195.

DOUZET F. & GERY A. (2020), « Le cyberespace, ça sert, d'abord, à faire la guerre. Prolifération, sécurité et stabilité du cyberespace », *Hérodote*, n°177-178, pp. 329-349.

NOCETTI J. (2020), « Les Gafam sont-ils trop puissants ? », *Les Grands dossiers de diplomatie*, n°50, pp. 88-89.

NORODOM A-T. (2020a), « Être ou ne pas être souverain, en droit, à l'ère numérique », *in* CASTET-RENARD *et al.* (éd.), *Enjeux internationaux des activités numériques,* Larcier, pp. 21-41.

NORODOM A-T. (2020b), « La souveraineté au défi des plateformes numériques », *in* RAPP L. (éd.), *Le droit international : entre espaces et territoires*, Institut francophone pour la justice et la démocratie, pp. 181-198.

kinéis

Brisez les barrières de l'IoT
grâce aux satellites Kinéis !

Avec l'IoT satellitaire, il est possible de connecter des objets partout dans le monde, soit environ 85 % de la surface du globe.

Gardez le contact avec vos objets : où qu'ils se trouvent, vos données continuent d'arriver régulièrement. Affranchissez-vous des zones blanches et des contraintes de roaming avec une connectivité vraiment globale.

Avec 7 satellites déjà en orbite et 25 supplémentaires en 2023, ce sont déjà des milliers d'objets connectés depuis plus de 40 ans par la technologie Kinéis.

Quelle que soit votre activité (loisirs d'extérieur, transport et logistique, agriculture, sciences et environnement, industrie, énergie…) retrouvez l'IoT que vous connaissez : miniaturisation, basse consommation, plug and play… Partout !

Résumés

données, etc. Ces enjeux sont communs aux enjeux de souveraineté posés par l'ensemble des processus de la numérisation de nos sociétés humaines. Toutefois, le changement quantitatif d'échelle et l'insertion des objets communicants dans tous les aspects de la vie quotidienne viennent renforcer considérablement ces enjeux, mais aussi les dynamiques en cours, notamment la dépendance des États vis-à-vis d'acteurs privés. L'article prend l'exemple de la sonnette connectée de la société Amazon.

Abstracts

Ont contribué à ce numéro

Vincent AUDEBERT est diplômé de Télécom Paris en 1991. Depuis plus de vingt-huit ans, il travaille pour le groupe EDF où il a occupé différents postes à la R&D, dans la distribution électrique, dans une filiale télécom utilisant les courants porteurs hauts débits et dans une filiale de services énergétiques. Depuis 2011, il est de retour à la R&D où il travaille sur l'application de l'Internet des objets et de la 5G aux besoins du groupe. Il est le représentant d'EDF à l'Alliance LoRa, au 3GPP et à EUTC. Il est co-auteur de 3 brevets et a reçu l'EPRI Technology Transfer Award en 2015.
→ ***L'usage des objets communicants dans le monde des entreprises électriques***

Christine BALAGUÉ est professeur et titulaire de la Chaire Good in Tech (www.goodintech.org) sur les technologies responsables à l'Institut Mines-Télécom Business School. Ses recherches portent sur la modélisation du comportement des individus connectés (réseaux sociaux, algorithmes d'intelligence artificielle, objets connectés), sur l'éthique des technologies et de l'intelligence artificielle ainsi que sur l'impact sociétal des technologies. Christine Balagué est également membre de plusieurs instances nationales : comité d'experts du CSA sur la désinformation en ligne, comité d'éthique de la Défense, commission impact des recommandations de la Haute autorité de santé. En tant que vice-présidente du Conseil national du numérique de 2013 à 2016, elle a participé à différents travaux remis au gouvernement français sur les grands enjeux du numérique (Neutralité du Net, Neutralité des plateformes, *E*-inclusion, *E*-éducation, *E*-santé, Ambition Numérique). Elle est également l'auteur de plus de 90 publications dans des journaux et conférences scientifiques internationaux, ainsi que de plusieurs ouvrages sur numérique et société.
Habilitée à diriger des recherches, Christine Balagué est docteur en sciences de gestion à HEC, diplômée de l'ESSEC et d'un master d'économétrie à l'ENSAE. Elle est aussi Chevalier de l'ordre national du Mérite.
→ ***Les enjeux éthiques des objets communicants personnels***

Martin BIÉRI est chargé d'études à la CNIL (Commission nationale de l'informatiques et des libertés) au sein du service du LINC, le Laboratoire d'innovation numérique de la CNIL. Diplômé de géographie de la santé et d'intelligence économique, il a rejoint l'équipe du LINC en 2019, après quelques expériences dans les études et la veille dans l'écosystème numérique. Il a participé aux différentes productions et études du LINC (sur le site : https://linc.cnil.fr), notamment des Cahiers Innovation et Prospective (Cahier IP7 sur les *civic techs* ; Cahier IP8 sur le rapport quotidien à la protection de la vie privée) et le livre blanc « À votre écoute » sur les assistants vocaux, paru en septembre 2020. Il s'intéresse particulièrement aux enjeux numériques de la santé.
→ ***Où vont nos données ? L'exemple des assistants vocaux***

Ingénieur centralien, **Philippe BIHOUIX** a travaillé comme ingénieur-conseil ou dirigeant dans différents secteurs industriels, en particulier les transports et la construction, avant de rejoindre le groupe AREP, agence d'architecture pluridisciplinaire et filiale de la SNCF (www.arep.fr), comme directeur général. Il est l'auteur de plusieurs ouvrages sur la question des ressources non renouvelables et des enjeux technologiques associés, en particulier *L'âge des low tech. Vers une civilisation techniquement soutenable* (Seuil, 2014) et *Le bonheur était pour demain. Les rêveries d'un ingénieur solitaire* (Seuil, 2019).
→ ***Le mythe de la* smart city *écologique***

Capitaine de gendarmerie, **François BOUCHAUD** dirige le département coordination opérationnelle cyber (DCOC) du Centre de lutte contre les criminalités numériques (C3N) au

sein du Commandement de la gendarmerie dans le cyberespace (ComCyberGend). Titulaire de plusieurs masters (Systèmes embarqués, Génie industriel et Management de la sécurité), il détient un doctorat en informatique et applications (sujet relatif à l'investigation criminelle dans l'Internet des objets).
→ ***Les objets connectés dans les missions judiciaires***

Jean-Pierre CORNIOU, économiste, ancien élève de l'ENA, a accumulé une expérience singulière dans le monde des organisations complexes – administrations, grandes entreprises – en devenant en 1990 directeur des systèmes d'informations dans la sidérurgie, puis chez Renault. Président du CIGREF entre 2000 et 2006, auteur, enseignant et consultant depuis 2006, il a été acteur et observateur de la révolution numérique dès l'origine, et accompagne la mutation de notre société par une réflexion stratégique comme par des interventions opérationnelles. Comme président de l'enjeu « industries et services » du pôle de compétitivité Systematic Paris Région, il met directement cette expérience multiple au service de la compétitivité des entreprises.
→ ***L'histoire des objets connectés***

Mathieu CUNCHE est maître de conférences à l'INSA-Lyon, membre du laboratoire CITI et de l'équipe Inria Privatics. Sa recherche porte sur les problématiques de vie privée et de sécurité associées aux objets communicants et aux réseaux informatiques (réseaux sans-fil, Internet, etc.). À l'INSA-Lyon, il enseigne les fondamentaux de l'informatique, la sécurité informatique, et la protection de la vie privée. Il a participé à des activités de standardisation à l'IETF ainsi qu'à l'IEEE 802. Avant de rejoindre l'INSA-Lyon en 2012, il a été chercheur post-doctorant au NICTA (actuel Data61-CSIRO) à Sydney, Australie. Il a obtenu son doctorat de l'Université de Grenoble en 2010 pour sa thèse sur les codes correcteurs LDPC.
→ ***Le traçage cyberphysique des personnes et la vie privée***

Didier DANET est maître de conférences en sciences de gestion, détaché de l'Université Rennes 1 auprès de l'Académie militaire de Saint-Cyr. Ses activités de recherche portent sur la mutation de la conflictualité contemporaine avec un intérêt particulier pour l'impact des nouvelles technologies sur les structures et l'action des forces armées : conflits dans l'espace numérique, robotisation du champ de bataille… Il a notamment codirigé, avec Stéphane Taillat et Amaël Cattaruzza, *Cyberdéfense*, aux éditions Armand Colin (collection U), ouvrage couronné par le Prix Cyberdéfense du Forum international sur la cybersécurité (FIC) en 2019. Il est responsable du mastère spécialisé « Opérations et gestion des crises en cyber défense » de l'Académie militaire de Saint-Cyr. Il est membre du groupement GEODE (Géopolitique de la Datasphère) piloté par Frederick Douzet (Université Paris 8).
→ ***Les enjeux de souveraineté des objets communicants***

Alix DESFORGES est chercheuse en post-doctorat à l'Université Paris 8 au sein du projet GEODE (Géopolitique de la Datasphère) depuis septembre 2018. Elle est diplômée d'un doctorat de géographie mention géopolitique de l'Institut Français de Géopolitique (Université Paris 8). Sa thèse porte sur les enjeux géopolitiques de défense et de sécurité nationale du cyberespace au travers l'exemple de la France. Ses travaux actuels portent sur les discours sur la souveraineté numérique et l'autonomie stratégique dans le domaine numérique en France et au sein de l'Union européenne.
→ ***Les enjeux de souveraineté des objets communicants***

Cécile DUBARRY a été nommée directrice générale de l'Arcep le 27 février 2017.
Ingénieure générale des mines, Cécile Dubarry a débuté sa carrière en 1994 à la direction générale des postes et télécommunications, puis, de 1997 à 2002, à l'Autorité de régulation des télécommunications.

En 2002, elle fut nommée sous-directrice, puis en 2005 cheffe de service, adjointe au directeur, à la direction du développement des médias.
Entre 2009 et 2017, elle a occupé les fonctions de cheffe du service de l'Économie numérique à la Direction générale des entreprises (DGE) du ministère de l'Économie et des Finances.
→ ***Les enjeux de la 5G pour les objets connectés***

Matthieu HUG est co-fondateur et CEO de Tilkal, plateforme de traçabilité 4.0 et de transparence pour les *supply chains*. Serial entrepreneur passionné par les technologies numériques, Matthieu siège au conseil de plusieurs *start-up* innovantes, ainsi que de l'ALCCI (Association de lutte contre le commerce illicite).
Entre 2007 et 2016, Matthieu a cofondé et dirigé RunMyProcess, une plateforme *cloud B2B* acquise en 2013 par le groupe Fujitsu. Auparavant, il a exercé plusieurs fonctions opérationnelles et de conseil autour des technologies numériques.
Matthieu est ingénieur CentraleSupélec et détenteur d'un Master of Science du Georgia Institute of Technology.
→ ***La traçabilité***

Marianne LAURENT est directrice marketing au sein de la *start-up* Acklio. Elle est titulaire d'un double diplôme Grenoble École de Management et ingénieur Télécom Bretagne en 2007, et d'une thèse dans le domaine des assistants vocaux avec Orange Labs en 2011. Avant de rejoindre Acklio, Marianne Laurent pilotait l'incubateur de l'IMT Atlantique à Rennes, avec pour mission d'accompagner la valorisation des résultats de recherche en création d'entreprise ou en partenariats industriels.
→ ***Les protocoles de l'Internet au service de l'interopérabilité de l'Internet des objets***

François LE BOULCH a débuté sa carrière chez Alcatel Space en 2005 (Thales Alenia Space depuis 2006) comme ingénieur aux affaires réglementaires. En 2011, il prend la direction du département avant-vente d'une ETI spécialisée dans les services télécoms, pour laquelle il remporte la réalisation de la première enquête nationale de qualité de service avec quatre opérateurs mobiles en France métropolitaine, pour le compte de l'Arcep. En 2013, il rejoint un opérateur mobile au Maroc, filiale du groupe mobile international Zain basé au Moyen Orient. Il y dirige le département Budget, Planification et Performance, avec pour objectif principal le lancement du 1er réseau mobile 4G du Royaume, réalisé en 2015. En 2017, il rejoint Airbus Defence and Space pour y développer l'activité relative aux licences et à la politique du spectre ; fonction qu'il occupe toujours actuellement. En 2019, il participe à la Conférence mondiale des radiocommunications de l'Union internationale des télécommunications (UIT) – institution spécialisée des Nations unies pour les technologies de l'information et de la communication – afin d'y promouvoir les intérêts d'Airbus, et suivre plus globalement l'évolution du sujet 5G. François Le Boulch a coordonné la réponse du groupe Airbus à la consultation de l'Arcep sur la 5G en France et mené l'audition du groupe aéronautique qui s'en est suivie par le collège de l'Arcep. En 2021, il est élu président de la Commission fréquences (radio) du GIFAS pour un mandat de deux ans.
François Le Boulch est diplômé de l'école d'ingénieurs Télécom Bretagne (IMT Atlantique) et de l'IE Business School of Madrid (MBA).
→ ***Skywise, pour la maintenance prédictive et au-delà…***

David MARTY is father of two marvelous kids and graduated with a Master in Aeronautics. He started his career at Airbus in 2001 within the Technical publication department. Originally a specialist of engines-related subjects, David Marty had various positions from 2006 to 2014 in the Airbus Customer services as Maintenance engineer, Planning specialist, Project leader, ...
In 2014, David Marty was appointed as Head of scheduled maintenance services developing

tailored solutions for airlines to optimize maintenance cost and increase aircraft availability. David Marty has also developed a center of competence in Malaysia to support Asian pacific operators.
Since April 2020, David Marty has joined the Airbus commercial team and he is in charge of Sales & Marketing for Digital Solutions. Digital Solutions include softwares developed by the Airbus Digital services team, but also the Skywise platform and its associated premium features.
In constant relation with airlines all along his career, David Marty has developed a passion for art, cultures, people, and he always seeks for new opportunities to learn.
→ ***Skywise, pour la maintenance prédictive et au-delà…***

Pierre MUSSO, philosophe de formation, est professeur de sciences de l'information et de la communication à l'Université de Rennes 2 et associé à Télécom Paris où il a créé la Chaire « Modélisations des imaginaires, innovation et création ». Il a été *fellow associate* et il est membre du conseil scientifique de l'Institut d'Études Avancées de Nantes. Il est l'auteur de nombreux ouvrages sur Saint-Simon et la philosophie des réseaux. Il a codirigé *Édition critique des Œuvres Complètes de Henri Saint-Simon* (quatre volumes, PUF, collection Quadrige, 2013). Sur l'imaginaire industriel, il a publié : *L'imaginaire industriel* (Manucius, 2013) et a dirigé l'ouvrage *Imaginaire, industrie et innovation. Colloque de Cerisy* (Manucius, 2016). Il a publié récemment *La religion industrielle. Monastère. Manufacture, Usine. Une généalogie de l'entreprise* (Fayard, collection Poids et mesures du monde, 2017) et *Le temps de l'Etat-Entreprise* (Fayard, 2019).
→ ***L'imaginaire de l'Internet des objets***

Alexander PELOV est le président et cofondateur d'Acklio. Il est co-chair du groupe de travail LPWAN au sein de l'organisme de standardisation IETF, membre de l'IETF IoT Directorate. Alexander Pelov a obtenu sa thèse en informatique à l'Université de Strasbourg en 2009. Il a été maître de conférences à Télécom Bretagne de 2010 à 2016. Ses travaux portaient sur l'efficacité énergétique dans les réseaux sans-fil et l'utilisation des *smart grids* dans le cadre des compteurs intelligents et les véhicules électriques. Alexander Pelov est co-auteur de plus de 30 ouvrages scientifiques dans des conférences et journaux internationaux à comité de sélection.
→ ***Les protocoles de l'Internet au service de l'interopérabilité de l'Internet des objets***

Frederic SUTTER is the Head of Skywise program at Airbus. Skywise is the first-of-its-kind open data platform developed by Airbus for the aviation industry. In addition, he is Airbus representative in GAIA-X AISBL and coordinates the Aerospace Dataspace regrouping industrial players from the GIFAS and BDLi.
Previously, Frederic Sutter was appointed as Airbus Group Digital Transformation Program Director in May 2015 and then became Airbus Digital Transformation Leader in June 2016, reporting to Group Digital Transformation Officer. In this role, he focused on multiple projects covering digital workplace, data governance, as well as Skywise ecosystem expansion towards third parties and other aviation stakeholders, including public institutions in order to facilitate industry-wide collaboration around data.
Prior to his role, Frederic Sutter joined Airbus Group in June 2012 as VP, Services Development and Strategy. Before joining Airbus Group, he had various responsibilities within Alcatel-Lucent as services channel sales manager, Director corporate strategy, VP in the managed services division and finally Head of the defense segment. Frederic Sutter started his career at Sema Group as systems architect in the IT industry.
Frederic Sutter is Auditor of the French Institute for National Defense Studies (IHEDN) and is also colonel of the civilian reserve of the French Air Force. He has a Master of International Business (EM Lyon) and a telecommunications engineering degree (ENST Bretagne). He has three children.
→ ***Skywise, pour la maintenance prédictive et au-delà…***

Anne-Lise THOUROUDE est une ancienne élève de l'École polytechnique et de l'école nationale supérieure des télécommunications, et ingénieur en chef des Mines. Après un début de carrière en 2006 à la Direction générale des entreprises au sein du ministère de l'Économie, des Finances et de l'Industrie, elle rejoint le Secrétariat Général du ministère de l'Économie, des Finances et de la Relance, en 2014 sur des fonctions de transformation des systèmes d'information puis de transformation numérique du ministère. Actuellement à l'Arcep depuis 2019, elle est en charge de la prospective en matière de fréquences et de planification de celles-ci.

→ ***Introduction***

→ ***Les enjeux de la 5G pour les objets connectés***

Alexandre TISSERANT est président de Kinéis, un nouvel opérateur satellitaire fournisseur de connectivité dédiée aux objets connectés, après avoir été directeur des projets stratégiques à CLS (Collecte localisation satellites). Diplômé de l'École polytechnique et de Télécom Paris, il a été le directeur adjoint du cabinet de la secrétaire d'État au Numérique et à l'Innovation de 2015 à 2017, où il avait notamment en charge le projet devenu loi pour une République numérique. Il a également occupé plusieurs postes à la direction du Budget du ministère des Finances, dont la gestion du budget du secteur des médias et du numérique en France, et a agi pendant deux ans comme directeur des opérations chez Always Innovating, une *start-up* de développement de matériel informatique à San Francisco.

→ ***La révolution du spatial ou la communication des objets partout dans le monde***

Laurent TOUTAIN est professeur associé au département Systèmes réseaux, cybersécurité et droit du numérique de l'IMT-Atlantique. Il a travaillé pendant plusieurs années sur le protocole IPv6 et a participé à la création du groupe G6 qui regroupe, depuis 1995, chercheurs et industriels autour du protocole IPv6. Actuellement, ses recherches concernent les protocoles et les architectures spécifiques aux besoins de l'IoT. Il est l'auteur de plusieurs ouvrages sur les réseaux. Laurent est cofondateur et conseiller scientifique d'Acklio.

→ ***Les protocoles de l'Internet au service de l'interopérabilité de l'Internet des objets***

Thomas VANTROYS est maître de conférences à l'Université de Lille et membre du laboratoire CRIStAL (UMR 9189) et de l'IRCICA (USR 3380). Ses travaux de recherche portent sur les systèmes embarqués et leur sécurité.

→ ***Les objets connectés dans les missions judiciaires***

Derek WALLACE, VP of Marketing, LoRa Alliance.

Derek Wallace leads the fantastic marketing team at the LoRa Alliance and brings over 25 years of experience marketing technology, Industrial IT and communication products and services globally. Most recently, he was Director of Product Management and Marketing for MultiTech, responsible for the increasing revenue and profitability for the entire IoT/M2M portfolio, including one of the largest suite of LoRaWAN products in the industry. He has worked across multiple parts of the value chain and around the world, with stops at Ericsson in Copenhagen, Orange Business Services in London, StrategyMix in Sydney and US West in Minneapolis. An active volunteer, Derek Wallace spent many years coaching ultimate frisbee teams around the world and is very involved with his Alma Mater, Carleton College, as part of the Alumni Council and leader of the Engagement Work Group. When not working, Derek Wallace enjoys traveling, reading and ultimate frisbee.

→ ***Use unlicensed LPWANs for cost-effective & secure massive industrial IoT***