

Internet des objets : pour une stratégie médiologique

Dominique Boullier

Pour la revue AOC 17 Octobre 2021

L'affaire semble entendue, l'internet des objets est non seulement annoncé comme inéluctable mais il est déjà là. Et tous les objets connectés que nous utilisons sans nous en rendre compte et tous les capteurs qui équipent nos villes nous le démontrent même s'ils ne sont pas connectés à Internet et utilisent des technologies WiFi ou Bluetooth ou des RFID en local : nous ne pouvons pas nous en passer. Pourtant, le saut que constitue cette nouvelle connectivité (des adresses IP pour tous les objets) mérite examen, et même plus, débat public. Car c'est d'un nouveau réseau qu'il s'agit, qu'il faut penser et discuter stratégiquement pour l'orienter selon des visées de bien commun et non seulement parce que le code court et que l'innovation n'attend pas. Trois questions (au moins) méritent d'être soulevées avant ce déploiement déjà bien avancé : l'architecture de réseau, la sécurité et notre couplage aux objets.

Avec l'internet des objets, l'étendue des possibles peut fasciner : de la voiture autonome, qui constitue le projet le plus ambitieux, au capteur de mouvement sur le lampadaire de la rue en passant par le jouet qui répond avec la voix des parents, il devient difficile de penser stratégiquement sans être pris dans cette avalanche de cas et d'innovations potentielles. Prenons ce dernier exemple, celui des jouets personnalisés connectés à internet. Il se trouve qu'il fut mobilisé le 12 Octobre 2016 dans l'attaque dite de Denial of Service (demandes de connexion tellement nombreuses que les serveurs tombent en panne) qui visait la société Dyn, qui gère l'orientation des requêtes à partir des noms de domaines. Ses serveurs de la côte Est des Etats-Unis ont été attaqués par des armées d'objets connectés qui, dotés d'une adresse IP et accessibles pour des hackers, ont été exploités pour lancer des requêtes en utilisant un programme (Mirai) mis à disposition sur le web par d'autres hackers. Ces caméras de surveillance, ces thermostats mais aussi ces jouets connectés (pour pouvoir simuler une interaction avec les enfants en utilisant des empreintes vocales des parents par exemple), sont devenus des brèches pour la sécurité car leurs concepteurs et les firmes qui les vendent n'ont jamais pris au sérieux ce risque et que la culture de la sécurité n'est pas diffusée dans cette industrie électronique proliférante. Comme le montre cet exemple, il devient impossible de penser objet par objet, application par application, fonction par fonction si l'on veut percevoir la transformation en cours. Les questions de sécurité sont un des enjeux essentiels de ce déploiement de l'internet des objets car elles révèlent les effets d'architecture de cette mise en réseau.

Médiologie de l'internet des objets

Penser les *architectures de réseau*, selon la terminologie de Lessig (1999), c'est penser en termes de *médiologie*, pour reprendre le concept de Régis Debray (1991). Car comme le disait Mc Luhan (1964), « the medium is the message », et cet aphorisme, souvent utilisé à tort et à travers, vaut comme algorithme d'une vision médiologique des architectures de réseau. Ce qu'il faut décrypter n'apparaît pas quand on fait la liste des objets eux-mêmes ni même quand on alerte sur les risques de telle ou telle application. Il nous faut comprendre cette capacité de l'architecture de réseau ainsi créée à nous faire agir d'une certaine façon, à programmer notre monde, notre vie. De même que la télévision, pour Mc Luhan, ne s'analyse pas en critiquant le contenu des journaux télévisés mais en pointant l'effet de synchronisation généralisée des esprits dans un pays donné au temps des journaux télévisés nationaux, un effet d'agenda setting de second degré pourrait-on dire. De même,

pour l'espace médiatique contemporain, j'ai montré (Boullier, 2020) que c'est le rythme attentionnel généré par la haute fréquence de réactivité sur les plates-formes de réseaux sociaux qui change tout et qui dicte sa loi à tout l'espace public, aux marques et aux interactions personnelles. Dans le cas de l'internet des objets, nous avons affaire à l'apparition d'un quatrième réseau et pour le percevoir, il faut repeupler la description de tout ce qui rend possible cette opération.

Un quatrième réseau

Trois réseaux, toujours opérationnels, ont été décrits par Tim Berners-Lee en 2006 en étapes historiques et en entités connectées : le réseau des machines, Internet (1974), le réseau des documents (1990), le réseau des personnes (les réseaux sociaux, 2004). Notons que chacun de ces réseaux, comme je l'ai montré (Boullier, 2021), ont tous été conçus de façon distribuée, selon la philosophie de départ d'internet, mais se sont trouvés tous centralisés progressivement : internet et ses machines, autour de Amazon Web Services qui fait 30% du marché de tous les services du cloud, le web autour de Google avec 90 % des parts de marché dans le monde, les réseaux sociaux autour de Facebook avec ses 2,8 milliards de comptes (extensibles via Instagram et WhatsApp). L'internet des objets constitue ainsi un quatrième réseau, très convoité, dont la centralisation risque rapidement d'émerger là aussi pour des raisons financières, quand bien même les parties prenantes restent encore nombreuses pour l'instant.

Tous les projets déjà lancés de *smart cities* vont bénéficier de ces services pour un pilotage supposé plus intelligent mais rien ne dit qui va finalement prendre la main et gagner en expertise dans cette connectivité généralisée : les opérateurs, les fournisseurs de service urbains, les équipementiers, les développeurs d'applications nourries à l'intelligence artificielle et pourquoi pas, les collectivités territoriales ou les services publics ? Dans tous les cas, un enjeu de responsabilité légale sur toute la chaîne de valeur et la chaîne technique devra être soulevé rapidement car il n'est pas possible de clairement délimiter les frontières de cette mise en réseau : le producteur du capteur, l'équipement qui le supporte, le service qui l'exploite, le développeur de l'IA qui le contrôle, l'utilisateur qui en bénéficie, etc. Ces débats ont déjà lieu à propos de la voiture autonome car les enjeux de sécurité et de responsabilité apparaissent d'emblée énormes mais on oublie de dire que ce doit être la même chose pour tous les objets connectés à internet.

Encastrer l'internet des objets dans un design organisationnel

Il est très risqué de développer et de réglementer des objets sans les « encastrent dans un design organisationnel » précis. Les encastrent, selon le terme de Polanyi (embeddedness), pour éviter que le calcul ne rende plus de comptes qu'à lui-même (et même pas à ses concepteurs qui ne savent plus l'interpréter à partir d'un certain nombre de couches de neurones). Les encastrent dans un « design organisationnel », qui oblige à décrire précisément les conditions d'utilisation et les parties prenantes, pour vérifier qu'on assure les conditions d'une appropriation par les personnes concernées (qui peuvent être des utilisateurs ordinaires aussi). Or toute la conception actuelle de ce réseau vise à engendrer une vitesse et une invisibilité maximale qui, de ce fait, rend plus difficile toute reprise de contrôle par les utilisateurs, j'y reviendrai. Première vision systémique, donc : les organisations et les parties prenantes qui contribuent au réseau ainsi dessiné. Mais il faut revenir sur le réseau lui-même et ses propriétés techniques.

Où l'on reparle de la 5G, condition d'existence de l'internet des objets

C'est ici que la 5G intervient, impossible à dissocier de l'internet des objets. On peut même dire que l'internet des objets est la principale démonstration de son intérêt. Je précise qu'il s'agit plutôt de la 5G 26Ghz qui sera déployée en France, nous dit-on, à partir de 2023, et non de la 3,5 Ghz dont les

fréquences viennent d'être attribuées par l'Arcep à la fin de l'année 2020. La 5G 26Ghz permettra en effet de proposer des temps de latence d'un ordre inférieur à 10ms avec tous ces objets comme avec tous les terminaux, ce qui produit un effet d'immédiateté complet pour l'utilisateur final. A condition que de nombreuses antennes soient déployées puisque leur portée descend en dessous des 500 mètres et que les serveurs soient aussi localisés au plus près des activités. Ce sera le cas grâce à ce qu'on appelle le « edge computing », version relocalisée du cloud si l'on peut dire, contre sa centralisation excessive qui place les serveurs trop loin du lieu de fourniture de services et qui ralentit la réactivité des objets connectés.

Des ressources modulaires et monétisables pour les opérateurs de télécommunications

Mais, même en décrivant ainsi le réseau, on manque encore ce qui constitue sa radicale nouveauté. La technologie 5G permet en effet de distribuer les ressources de réseau (débit et bande passante) de façon ciblée en direction d'un terminal ou d'un objet précis et non plus, comme le fait la 4G, en arrosant tout le voisinage. Cela s'appelle le « network slicing ». Cette avancée technologique est présentée avant tout comme un progrès sur le plan environnemental puisqu'ainsi la consommation d'énergie est optimisée. On oublie de dire qu'il faudra du coup beaucoup plus d'antennes et que ce nouveau réseau doit permettre de déployer tous ces objets connectés par milliards avant 2025. Mais on oublie surtout de dire que cela permettra une tarification personnalisée, différenciée, modulaire selon les types de terminaux et le consentement à payer des utilisateurs. Or, cette avancée sera surtout l'occasion aux opérateurs de télécommunications de profiter à leur tour des revenus considérables engendrés par internet.

Car, et cela paraît peut-être étonnant, les opérateurs de télécommunications prétendent, à juste titre, qu'ils ont déployé des ressources de connexion (la fibre optique principalement) pour le bénéfice principal des GAFAM et des plates-formes de streaming, alors que leurs tentatives pour devenir eux aussi des plates-formes ont toutes échoué. C'est notamment pour cette raison que les opérateurs voulaient en finir avec la neutralité d'internet qui oblige à servir tous les demandeurs de capacités de réseau sur un pied d'égalité (best effort) alors que les YouTube, Facebook, Netflix et autres sites porno occupent toute la bande passante à leur seul profit sans avoir à payer pour leurs investissements de réseau.

Avec la 5G et l'internet des objets, il n'est pas question pour les opérateurs que cela se reproduise. Et l'interactivité à haute fréquence exigée par les services qu'on anticipe grâce à la connexion internet avec tous ces objets, exige des investissements qui pourront être monétisés grâce à ce *slicing* et à ce calcul de proximité équipé d'IA qui déterminera des tarifications très granulaires. Pour les usages déjà existants, voir Netflix en streaming 8K pourra donc être possible en mobilité selon les abonnements que l'on aura payés auprès des opérateurs télécoms et non plus seulement en fonction des offres commerciales de Netflix. Et pour les services de l'internet des objets, la même tarification fine pourra être appliquée. De même que pour le métavers de Mark Zuckerberg qui repose sur la réalité virtuelle et la réalité augmentée, très gourmandes en bande passante. L'objectif de l'architecture de la 5G est bien de générer des revenus pour les opérateurs télécoms et non plus seulement pour les plates-formes. La réactivité des objets, la latence réduite doivent être interprétées à cette lumière pour comprendre comment l'on peine parfois pour trouver des justifications d'usage pour le grand public, au point d'inventer des scénarios invraisemblables comme la chirurgie à distance en situation de mobilité.

L'internet des objets à domicile

Pour parachever ce projet, il existe deux faiblesses de la 5G 26Ghz qu'il faut surmonter : les obstacles physiques et les zones blanches. Ses ondes de courte portée ne peuvent franchir les obstacles et

donc ne peuvent desservir l'intérieur des domiciles, des bureaux, des commerces, des lieux publics fermés. Il suffit cependant d'implanter plus d'antennes en intérieur pour assurer la continuité technique du service en 5G 26Ghz pour que les usages de l'internet des objets ne soient pas interrompus, pensons à Pokemon Go par exemple (cas nettement plus réaliste que la chirurgie mais justification moins noble des investissements) ou encore aux jeux du métavers de Méta (ex Facebook), aux hologrammes qui demanderont tous une persistance. Pourtant, il existe déjà le Wifi, qui plus est gratuit, sans parler de Bluetooth ou d'autres protocoles d'objets qui ne sont pas reliés à internet comme le protocole SigFox. Mais tout cela a pourtant deux inconvénients : il n'offre pas de réactivité suffisante, la latence est trop grande, et plus encore, il est gratuit. Les opérateurs vont ainsi implanter des antennes en intérieur (c'est déjà le cas en Suisse mais pas pour l'usage d'objets connectés) qui permettront de générer des revenus en raison de la fourniture de services très fins et adaptés aux usages. Voici donc un autre volet de l'architecture de l'internet des objets qu'il faut prendre en compte.

Et maintenant les satellites pour l'internet des objets

Un troisième volet, plus connu, est constitué par les flottes de satellites qui sont en cours d'installation en orbite basse tout autour du globe. Or, l'internet des objets, qui par définition doit être mobile (sinon la fibre peut y suffire), souffre de limitations dans certaines zones du monde, zones blanches parfois très vastes. Les compagnies de satellite comme Starlink (Elon Musk) ou OneWeb ou même Facebook ont anticipé ce marché potentiel et, en dehors de toute planification internationale, voire sans réelle réglementation, se lancent dans cette course aux satellites. Maintenant que le projet de métavers de Facebook a été dévoilé, on comprend mieux l'intérêt de développer un réseau satellite qui lui soit propre. Mieux même, on peut dire que le point central de la stratégie de Facebook avec son métavers est de devenir le système d'exploitation de ce quatrième réseau, non seulement pour les satellites mais pour toute cette nouvelle version de l'internet mobile, alternatif ainsi à iOS et à Android. Le pilotage des objets via internet est un objectif essentiel même si pour l'instant, la latence pour les orbites les plus basses ne descend pas en dessous de 30 ms ce qui est insuffisant pour piloter certains objets avec la réactivité nécessaire, notamment les véhicules autonomes.

A cette occasion, on peut ainsi observer qu'un autre type d'acteurs entre dans la compétition, les compagnies de satellites, qui visent à obtenir une rente sur l'accès à cette connectivité à la place des opérateurs traditionnels et sont prêtes pour cela à des investissements considérables (Elon Musk lance 60 satellites de 1,5 kg tous les 15 jours pour atteindre 42000 satellites en 2025). Facebook semble ainsi largement distancé sur créneau mais se réserve le système d'exploitation (OS). L'encombrement spatial, la régulation des déchets, de la perturbation des observations, la sécurité, les risques de monopole, etc., tout cela semble de peu d'importance pour les agences qui gèrent l'espace ou les fréquences, puisqu'il convient avant tout de laisser faire les innovateurs.

Un réseau parallèle pour l'internet des objets !

Voici donc le tableau complet du nouveau réseau, le réseau de l'internet des objets et ce tableau n'a plus rien à voir avec l'imagerie Bisounours des objets à service personnalisé qui nous est souvent présenté. L'architecture de tous ces objets une fois connectés dépasse ces objets et nous dépasse. Elle n'est pas décidée stratégiquement par les pouvoirs publics ni aucune autre assemblée, elle se constitue par dérive progressive depuis la compétition féroce entre acteurs anciens et nouveaux. Or, tous ces investissements, aussi privés soient-ils, usent d'un bien commun (les fréquences, l'espace), de ressources rares (l'énergie mais aussi les matériaux), sans oublier notre attention, et organisent ainsi une infrastructure nouvelle qui concurrence directement les investissements lourds qui ont été

consentis avec la fibre optique notamment et souvent avec l'appui de financements publics. Nous aurons donc ainsi des réseaux concurrents, sous prétexte d'adopter le point de vue stratégique de la mobilité généralisée, voire du métavers, alors que la plupart de ces services pourraient être opérables à travers une combinaison de fibre optique et de Wifi, au prix, certes, d'un ralentissement et donc d'un frein pour l'usage de l'internet des objets tel qu'il est projeté actuellement.

L'internet des objets nous fait passer dans le tout mobile, au détriment des réseaux existants

Il faut donc récupérer la main sur cette possible duplication des réseaux sans tomber sous le charme de l'argument de l'internet des objets. C'est ce que j'appelle une stratégie médiologique, qui prend en compte l'effet systémique, les dimensions techniques et socio-économiques plurielles qui sont ainsi affectées. Le modèle culturel qui est ainsi diffusé ne dépend pas d'un objet (un thermostat), d'une application (Pokemon Go) ou d'un service précis. C'est toute notre vie ordinaire qui se voit sommée de basculer dans la « mobilité par défaut », puisque tout ce que nous faisons actuellement en ligne en utilisant de la fibre et du wifi devra désormais être possible en utilisant uniquement la 5G 26Ghz, et bien plus puisque ce sera l'occasion de nous proposer encore plus de services, jusqu'aux hologrammes généralisés qui semblent le Graal des projets de 6G déjà en cours de spécification et dont la portée apparaît stratégique avec le projet de métavers.

La sécurité, parent pauvre des choix d'architecture de réseaux

Les enjeux de sécurité évoqués en début d'articles prennent dès lors tout leur sens car un équipement d'un réseau aussi intense en objets nécessiterait de sécuriser le réseau (et pas seulement la 5G, mais tout internet, puisque cela reste l'architecture commune). Or, lorsque l'on se focalise sur la latence, on privilégie encore et toujours la vitesse, au détriment de la sécurité. Les craintes de hack et de surveillance que l'administration Trump a diffusée à propos de l'équipementier Huawei, leader sur la 5G, ne sont pas seulement gesticulations anti chinoises. Elles sont tout à fait crédibles à condition de les étendre à tous les équipementiers (dont les européens comme Erikson ou Nokia) et de souligner que les *backdoors*, les portes dérobées qui demeurent dans la plupart des équipements (dont les terminaux), sont en fait encouragées par toutes les agences de renseignements qui ne supporteraient pas d'avoir à faire à un réseau trop sûr, qui ne leur permettrait plus de prélever des données et d'effectuer leur activité de surveillance. Les failles de sécurité ne sont pas dues seulement à des entités malveillantes, ni à la faiblesse des protocoles à l'origine d'internet. Ces failles sont créées et maintenues « by design » par une alliance fabricants, opérateurs et agences de renseignement, ce qui rend très difficile tout progrès substantiel en matière de sécurité.

Une IA présente partout dans l'internet des objets et de plus en plus opaque

D'autant plus que tous ces systèmes dépendront des algorithmes de Machine Learning qui y seront implémentés, car cette vitesse de réaction, avec des objets et des serveurs aussi distribués, exige de tels degrés de complexité que seule l'IA permettra de les gérer. Or, le développement actuel de l'IA est hors de contrôle. Les performances des algorithmes dépendent dans le *deep learning* notamment d'une telle quantité de couches de neurones que ces boîtes noires ne sont même plus interprétables par les informaticiens qui les ont développées. Du point de vue de la sécurité, lancer l'internet des objets, c'est nécessairement donner les clés de la gestion du réseau, dans toutes ses couches, à des IA toujours plus puissantes et toujours plus opaques.

Là encore, l'objet n'est rien sans le calcul qui lui permet de fonctionner, et ce calcul à base d'IA est désormais en train de se désencastrer des règles et des organisations qui l'ont vu naître, au point que certains comme Rahimi craignent de n'être pas plus crédibles que des alchimistes. Dès lors, les peurs

et les fantasmes véhiculés par la littérature comme la gelée grise des objets nanotechnologiques qui s'autoprogramment de Michael Crichton (La proie, 2002) ou encore d'un épisode de Black Mirror (Hated in the nation, 2016) qui donne à voir l'action coordonnée d'essaims d'abeilles artificielles, ne peuvent plus être disqualifiées. Que sommes-nous en train de produire avec cette connectivité généralisée des objets qui pourront se passer d'un contrôle humain ?

L'internet des objets est-il habitable ?

C'est la dernière dimension qu'il convient d'évoquer pour dépeindre dans son ensemble le tableau du monde qui se prépare en adoptant -sans débat- une architecture comme l'internet des objets. Car si cette perspective reste pourtant attractive auprès des humains, des consommateurs, des citoyens, c'est que le modèle d'adhésion à ses principes sont déjà en place. Lorsque la vitesse, obsession des concepteurs, se transforme en immédiateté des services exigée par les consommateurs, on sait qu'un allié de poids a été gagné, le public, et qu'une défaite du consentement éclairé doit être actée. En effet, le monde qui est le nôtre est gouverné, à partir des plateformes par le triple impératif suivant : « *one click, one tweet, it's a match* ». *One click* est la promesse réalisée par Amazon pour tout le commerce, *one tweet* est ce qui résume au mieux l'état des arguments et des débats publics et *it's a match* décrit la réussite des promesses des sites de rencontre (Pidoux, 2021) comme des recommandations (livres, vidéos, services) et tous les effets de plateforme d'intermédiation qui semblent s'annuler elles-mêmes tant la vitesse engendre l'invisibilité de la médiation. L'idéal du marketing one-to-one déjà ancien et de tous les économistes libéraux était de favoriser des transactions sans friction (*frictionless transactions*). L'internet des objets et son architecture vont tout entiers dans ce sens, et cela pour notre bien et pour notre plus grande satisfaction.

Une ergonomie de la transparence et ses pièges

Lorsque je travaillais avec mes collègues sciences cognitives et d'ergonomie à inventer des tests pour s'assurer que l'objet ou le service pouvait être approprié par divers publics, je pensais contribuer à un couplage plus étroit avec les objets, à une égalité d'accès à ces services, à une pénibilité moindre. En fait, tout ce que nous (et beaucoup d'autres) avons développé dans les laboratoires des usages que j'ai contribué à créer en France (Lutin, Cité des Sciences), a été repris par les plateformes et par les designers pour engendrer une disparition telle des frontières que la question de l'appropriation (qui est toujours conflictuelle et donc pleine de frictions) ne se pose même plus. L'internet des objets vise en fait un idéal « d'être-connecté », ce mutant qu'on aurait lobotomisé, dont on aurait ôté toute la compétence de libre arbitre tant il jouit de voir ses supposés désirs devancés par l'immédiateté des réponses des services, par les plateformes et les opérateurs. Le droit est sans doute la première victime dans cette affaire, tant il génère par définition des frictions, qui entravent l'immédiateté des pulsions au profit de la décision éclairée.

La médiologie de l'internet des objets impose donc d'en venir aussi à ces sujets de droit que l'on disqualifie, pour leur bien cela va sans dire, et les sujets consommateurs-à-réaction seront les premiers à défendre les objets connectés apparemment esclaves mais pourtant autonomes pour rendre immédiatement des services que l'on ne savait pas vraiment vouloir. Les questions légales de données personnelles, de traces de comportement introduisent là aussi des frictions et les firmes feront tout pour les contourner, alors qu'au contraire au moment de cette extension infinie des êtres connectés, il faudrait reconsidérer et renforcer encore les politiques de contrôle des traces et données personnelles. Notre anthropologie naïve ou savante sur nos identités et nos frontières personnelles est désormais à reconsidérer de même que nos ontologies : quels seront les statuts légaux et existentiels de ces objets qui sont en capacité de prendre des décisions grâce à leurs IA

indécodables, de façon coordonnée et à haute fréquence au point d'être invisibles ? Ce n'est pas un hasard si, dès 2002, j'avais intitulé un article « objets communicants, avez-vous donc une âme ? ».

L'habitèle comme design de contrôle

Plus modestement, la question pourrait être posée en termes d'habitabilité du numérique. Cette dimension de nos capacités à faire peau, à faire enveloppe de tout équipement technique qui produit des intérieurs d'existence, peut être déclinée, comme je l'ai fait depuis mon livre « l'urbanité numérique » de 1999, en termes d'habitat tout en étant lié à l'habit (un des objets connectés majeurs), à l'habitable (et non de véhicule autonome qui reste pensé comme fonction technique de mobilité) et enfin à l'habitèle, néologisme qui permet de penser de façon dynamique le processus anthropologique de couplage avec nos peaux techniques numériques, faites de terminaux, de réseaux et désormais de tous ces objets.

Pour que cette extension infinie de la connectivité avec ces objets ne signe pas notre perte dans les flux incontrôlables de données et de traces, il faut aussi repenser le design de tous ces objets, pour en faire un « design de contrôle » du point de vue du citoyen et du consommateur. Oui, il perdra un peu en fluidité mais il récupérera une capacité de contrôle des accès à son univers, une capacité de filtrage, mais aussi une capacité de débrayage, qui permet d'arrêter à tout moment toute connexion sans que cela entraîne des blocages radicaux dans sa vie ordinaire (pensons à toutes les pannes de contrôle d'accès qui ne disposent pas d'une alternative). Que les objets parlent, pourquoi pas, mais aussi qu'on puisse les faire taire quand on veut et qu'ils n'en viennent pas à diriger insidieusement et moralement nos vies en quelque sorte ! L'apologie de la déconnexion semble un discours moral qui accuse implicitement les individus. Encore faudrait-il que tout le design des objets et des services ne soit pas organisé pour décourager toute déconnexion. Pour cela, il faut des interfaces, des services conçus explicitement pour offrir cette capacité.

La gouvernance de l'internet des objets, une réplique des erreurs déjà faites ?

La prise en charge de toutes ces questions pose des questions de gouvernance d'un nouveau réseau comme celui de l'internet des objets. Certes, il faut bien reconnaître que tout ce qui a été fait en matière de gouvernance du réseau des machines, des documents ou des personnes a engendré des dérives aux lourdes conséquences. Le principe dominant des quelques organismes ni inter-nationaux, ni de normalisation qui prennent l'internet en charge (IETF, ICANN) repose sur un *rough consensus and running code*, exprimé en 1996 par John Perry Barlow, qui a détruit l'esprit même de ce que l'auteur recherchait, cet esprit coopératif et ouvert des premiers temps d'internet. L'étape indispensable à l'aube du lancement de ce quatrième réseau, celui des objets, serait de le doter d'un organisme de régulation internationale que les Etats auraient en main. Cependant, dans la mesure où l'idéologie libérale, voire libertarienne, de beaucoup des gouvernements démocratiques les a conduits à abdiquer presque toute compétence de régulation, on ne peut qu'être inquiets.

Cependant, des sursauts comme le RGPD montre qu'il est encore possible d'inventer du droit qui crée des conventions et stabilisent ainsi les marchés, tout en protégeant les consommateurs et les citoyens. Au niveau national, on peut considérer qu'il serait difficile d'ajouter encore une agence de plus à tout l'appareil de gouvernance technique dont se sont désormais entourés tous les Etats libéraux. Mais l'Arcep serait tout-à-fait dans son rôle pour réguler tout l'internet des objets dans la mesure où tout dépend des fréquences qui sont exploitées, en l'occurrence la 5G puis la 6G. Le colloque à propos de l'internet des objets organisé dès 2016 par cette agence, m'avait donné d'ailleurs l'occasion d'alerter sur les prérequis en matière de sécurité des réseaux pour tout déploiement de l'internet des objets. Je ne pense pas avoir été entendu car je n'ai guère vu sortir de cahier des charges pour tous les constructeurs d'objets connectés, ni même d'articles

particulièrement contraignants dans ce domaine lors de l'attribution des fréquences de la 5G en 2020. La CNIL est évidemment l'agence directement concernée par tous ces sujets mais elle n'a pas un pilotage technique précis de certains domaines à effectuer et c'est pourquoi il convient de désigner une agence responsable de ce secteur.

Il est surtout nécessaire de produire les ***cahiers des charges*** qui permettront aux individus-consommateurs comme aux citoyens et aux pouvoirs publics de reprendre la main sur ces architectures qui organisent notre vie ordinaire selon des principes opaques et pourtant puissants.