Réguler l'Internet des objets en 2023 ?

Pierre-Jean Benghozi

RÉGULER L'INTERNET DES OBJETS EN 2023 ?

PIERRE-JEAN BENGHOZI (X76)
directeur de recherche
CNRS, École polytechnique

Qu'on se les approprie ou qu'on les appréhende, les objets connectés sont de plus en plus présents. Cet internet des objets induit des changements profonds en de nouveaux services, dans les entreprises comme par les volumes de données inédits qu'il génère. Le défi que pose la régulation de ce monde nouveau créé par l'IoT est rendu particulièrement ardu par la nature même de ses caractéristiques techniques et industrielles.

Les unes des journaux se font régulièrement l'écho de nouveautés en matière d'objets connectés. Ces évolutions structurent déjà des secteurs aussi divers que l'énergie, les transports, l'automobile, l'agriculture, les assurances, la santé, etc. Tous les produits y passent : compteur, montre, voiture, carte de transport, badge d'accès, store ou alarme, éclairage… ce seront facilement une dizaine d'objets qui chacun nous entoureront, d'où les dizaines de milliards d'objets facilement évoqués dans les prévisions. Le tout connecté sera bientôt une réalité. L'IoT soulève dès lors des problématiques multiples : technologiques bien sûr, mais aussi économiques, juridiques et sociétales. Au cœur du débat, la capacité collective de tous les acteurs, des équipementiers aux fabricants d'objets en passant par les opérateurs, de construire un écosystème stable et performant à même d'assurer de vraies utilité et fonctionnalité des services et objets connectés, tout en assurant la confiance des utilisateurs, particulièrement en ce qui concerne la sécurité des réseaux et la protection des données personnelles et industrielles. Car la une des journaux, ce sont aussi parfois, malheureusement, les cyberattaques massives récentes en déni de service, les données capturées et volées car mal protégées, les objets pilotés abusivement à distance, les craintes de la population qui ont pu s'exprimer à propos de Linky.

Tout change en même temps

Dans cette phase d'émergence et d'innovation foisonnante, la difficulté et les opportunités tiennent à ce que tout change en même temps. Les technologies disponibles ou éligibles sont particulièrement nombreuses et parfois en concurrence pour des fonctionnalités proches : à base de réseaux fixes ou mobiles, *via* des puces et capteurs différents, RFID (radio frequency identification) ou SIM (subscriber identity module), sur des réseaux partagés ou de basse consommation… Les usages ciblés sont tout aussi multiples, car ils concernent tous les volets de la vie quotidienne ou de l'industrie, des utilisateurs qui peuvent être autant des personnes âgées que des experts professionnels, des services qui ne sont plus singuliers mais se démultiplient et s'articulent les uns sur les autres, comme dans les voitures électriques et connectées. La question est autant sociale que technique, car les cadres économiques et juridiques (partage de la valeur, modèles d'affaires B2B et B2C, propriété des données, statut de la déconnexion, recours en cas de problèmes) restent encore largement indéfinis et appellent de nouvelles formes d'intermédiation associées aux services et au partage de données.

Une dynamique à maîtriser

L'enjeu est donc important pour les régulateurs et les acteurs publics. Il s'agit moins de définir un cadre corseté figeant les positions que de favoriser, dans tous ces registres, un élan assurant à la fois le respect des citoyens, soutenant le développement d'innovations et de services à même d'améliorer leur vie quotidienne, et garantissant protection, anticipation des risques, confiance et résilience. Cette omniprésence et place centrale de l'IoT se traduit en effet par des impacts croissants sur les individus, les entreprises et la société en général, dans ce qu'un rapport récent de France Stratégie qualifiait de « dynamiques à maîtriser ».

Internet of everything

Ces questions ne sont pas radicalement nouvelles. D'une certaine manière, ce sont les mêmes qui se posaient, il y a près de trente ans, au moment des balbutiements de l'internet et du e-commerce… et les solutions ont été depuis lors trouvées dans tous ces registres pour élaborer des réseaux performants. À se replonger dans l'histoire de l'informatique et de l'internet, on pourrait donc penser que l'IoT n'est pas, en soi, radicalement nouveau. La mise en réseau et l'interconnexion de machines existent depuis les années 70 et la notion même d'IoT est apparue dans les années 2000, dès le début de l'internet. Pourtant, s'ils étaient alors en germe, ses enjeux paraissent aujourd'hui prendre toute leur force, avec le caractère pervasif d'un système technique qui ne connecte plus simplement des terminaux fixes, mais désormais n'importe quel équipement, individu ou entité : on parle d'*internet of everything* comme une nouvelle étape de l'internet. Ce mouvement vers une hyperconnectivité de tous et de tout n'est absolument pas antinomique avec celui qui guide aujourd'hui l'internet vers une structuration dématérialisée du monde (jumeaux numériques, métavers…). Bien au contraire, la possibilité même de construire une représentation virtuelle du monde par le métavers suppose de penser et mettre en œuvre des interfaces matérielles – des objets connectés – de plus en plus nombreuses.

Un système de systèmes

Techniquement parlant, l'IoT ne peut être réduit à une technologie spécifique, mais doit être vu comme une extension des systèmes de codage et d'identification qui étaient déjà présents dans les codes-barres par exemple. Il consiste donc à associer, de manière standardisée, des éléments physiques (un conteneur, une machine, un capteur, voire un animal) à une identification numérique (par exemple une adresse IP ou un code RFID) et à un dispositif de collecte, transfert et traitement des données associées. L'IoT est une approche de la connectivité, portée par une multiplicité de solutions sous-jacentes (réseaux, protocoles, capteurs, données, équipements, lecteurs…), plus qu'une technologie en soi.

Des systèmes technologiques

Actuellement, l'enjeu majeur n'est pas tant d'inventer de nouvelles technologies que de perfectionner celles qui existent déjà, de les connecter et de les intégrer. Les principaux systèmes technologiques nécessaires au fonctionnement de l'IoT sont les suivants. D'abord les modes d'identification numérique pour caractériser et reconnaître chaque objet de façon unique. Puis les lecteurs et capteurs d'état pour recueillir la situation, les informations et les données de chaque objet et de son environnement. Ensuite les modalités de connexion pour mettre en relation les objets avec le réseau de communication. Les réseaux de communication pour connecter les systèmes entre eux et acheminer et transférer ces informations afin de pouvoir les traiter et les utiliser. Les protocoles d'articulation et d'intégration des couches techniques. Le stockage et traitement de données pour les analyser, appuyer la prise de décision ou déclencher des actions.

Une diversité ouverte

Le système technologique sous-jacent à l'IoT se caractérise donc par la diversité ouverte sur chacun de ces sous-systèmes. D'abord celui des capteurs, lecteurs, équipements, en un mot des objets connectés. Ensuite celui des modalités de connectivité et des réseaux, privés ou publics, radio, filaires, voire lumineux, embarqués ou pas, longue distance ou courte portée. Celui des modes de traitements et de stockage des données, en local, sur des serveurs distants ou dans le cloud. Enfin celui des protocoles et modes de communication des objets et services associés (en continu avec plus ou

moins de latence, ponctuellement, haut débit ou bas débit).

L'interopérabilité entre les systèmes de tous ces composants constitue de ce fait une préoccupation majeure pour savoir comment mettre en œuvre, connecter et intégrer les technologies existantes et les différents objets correspondants, en évitant notamment les conflits algorithmiques potentiels entre systèmes, en assurant l'évolution régulière et la compatibilité ascendante de chacun de ces systèmes techniques, en stimulant innovation et concurrence en évitant d'enfermer les utilisateurs dans des trajectoires techniques irréversibles. Une telle configuration appelle, naturellement, une multitude d'acteurs engagés dans l'IoT à un niveau ou une autre, sur une couche technique ou une autre. C'est d'ailleurs aussi ce qui rend particulièrement ardu de quantifier et mesurer l'ampleur des objets connectés, comme leur croissance. Mais cette multitude contribue aussi à constituer autant d'écosystèmes parfois indépendants ou autonomes, car correspondant à des besoins ou usages spécifiques : les dispositifs bas débit LPWAN (low power wide area network) *versus* les réseaux cellulaires *versus* les solutions LAN RFID (local area network & radio frequency identification) par exemple.

Des questions de régulation

Les conséquences de cette situation sont de plusieurs ordres en termes de régulation et de politique industrielle. J'en retiendrais essentiellement deux. En matière de technologie d'abord, il s'agit de penser l'IoT davantage en termes de structuration d'infrastructures, d'écosystèmes et de plateformes techniques sous-jacentes plutôt qu'en termes d'objets ou de solutions de connexion spécifique. En matière de régulation et de politique industrielle ensuite, il faut relever que, face à la multiplicité des enjeux évoqués, un cadre structuré existe déjà mais il pâtit d'une approche restant segmentée, qu'il s'agisse des registres mobilisés du droit et de l'économie ou des instances et autorités qui s'en saisissent.

L'IoT soulève d'abord des questions de concurrence (entre solutions et entre acteurs pour le contrôle des données). Comme le montre le cas de l'automobile ou de la santé, il s'agit d'éviter les effets de dominance de plateformes existant dans le reste de l'internet avec les GAFAM. L'IoT soulève ensuite des questions classiques en matière de contrôle des données personnelles, mais aussi des questions plus inédites d'ordre éthique, quand les objets connectés deviennent autonomes avec le couplage d'intelligence artificielle ou quand les individus eux-mêmes deviennent connectés et traçables. L'IoT démultiplie encore les risques et points d'entrée potentiels des cyberattaques, pour des utilisateurs peu sensibles et peu armés pour leur faire face, avec des objets à la qualité et fiabilité difficiles à contrôler. L'IoT place au premier chef les questions de standardisation – normalisation – interopérabilité à stimuler et garantir pour éviter la position dominante de certains acteurs, au niveau que ce soit de la couche réseau, de celle des applicatifs ou de celle du contrôle des données. L'IoT met tout particulièrement en avant les questions de souveraineté, car il articule très directement les dynamiques du numérique avec celle de la production industrielle, portant chacune un mouvement de globalisation dominé par les USA pour le numérique, la Chine pour les équipements et l'industrie manufacturière. Enfin le déploiement d'objets connectés à une très large échelle doit appeler à réfléchir aux impacts environnementaux de ces évolutions : dans les puces, les équipements et les réseaux, mais aussi dans l'impact des usages permis ou favorisés par l'IoT.

> ***"Les questions dépassent le cadre d'un IoT qui serait vu comme un simple segment de l'internet."***

Le cadre international

En conclusion, les évolutions et l'omniprésence des objets connectés supposent donc de mieux articuler d'une part les acteurs de la régulation, de repenser d'autre part en conséquence tous les volets de l'action publiques. La difficulté principale en la matière est en outre que l'IoT s'inscrit dans un cadre international (en termes de R & D, de technologies, d'équipements, de standardisation, de platesformes applicatives…) qui se définit pour une large part hors du cadre de régulation que maîtrise chaque État. À cet égard, on voit bien que les questions soulevées sont emblématiques et spécifiques de toute l'économie numérique et dépassent donc le cadre d'un IoT qui serait vu comme un simple segment de l'internet.

Références

- Benghozi Pierre-Jean et Mellier Guillaume, *The internet of things: A new paradigm for regulation?*, *Journal of Law & Economic Regulation*, vol. 9, n° 1, pp. 160-188, (2016).
- Benghozi P.J., S. Bureau et F. Massit-Follea (2009) *The Internet of Things: What challenges for Europe?*, (publication bilingue), Éditions MSH-collection praTICs.
- France Stratégie (2022), *Le monde de l'Internet des objets : des dynamiques à maîtriser* (sous la direction de C. Kirschner), 299 p. fs-2022-rapport-iot-fevrier.pdf (strategie.gouv.fr).