

Les enjeux réglementaires et juridiques de l'Internet des objets (IoT)

Eric Vève

Avocat à la Cour

2, Porte de l'Europe

14000 Caen- France

+ 33 2 31 469 666 / + 33 6 73 793 693

e.veve@avocats-porteurope.com

www.veve-avocats.com



Définitions et applications




Définitions :

- « 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 interoperables existant ou en évolution » (UIT, 2012).
- « L'IoT correspond à un ensemble d'objets connectés, de communication et d'Internet, qui se conjugue avec les vagues du cloud et du big data » (ARCEP, Libre blanc, 2016).



Applications multiples :

- Habitat et lieux de travail connectés pour un plus grand confort,
- Industrie du futur (relève d'information, commande à distance...),
- Véhicules connectés,
- Santé connectée (sommeil, grossesse, diabète, etc.),
- Etc.



Un large écosystème pour une croissance exponentielle

- ▶ Large écosystème de l'IoT, entre les acteurs privés qui interviennent sur :
 - ▶ La couche des objets physiques possédant des technologies embarquées de capteurs d'intelligence et de connectivité (concepteurs, fabricants d'objets et de composants de modules...),
 - ▶ La couche de la connectivité afin de permettre le transport des données issues des objets (opérateurs et équipementiers de réseaux),
 - ▶ La couche du stockage et du traitement des données (opérateurs de cloud, fournisseurs de services et agrégateurs de données qui exploitent les données des utilisateurs générées par les objets pour répondre à leurs besoins...),
 - ▶ Tout ou partie de ces couches (intégrateurs, acteurs de la sécurité...).
- ▶ Une croissance exponentielle :
 - ▶ De 26 à 80 Mds d'objets connectés dans le monde d'ici 2020 (IDATE, CISCO, GARTNER)...
 - ▶ Cabinet Mc Kinsey identifie ce marché comme l'une des principales sources de croissance à l'avenir
 - ▶ La majorité de la valeur de l'IoT devrait revenir à la couche du traitement des données (56 Mds d'euros en 2025 A.T. Kearney).



Des enjeux réglementaires et juridiques protéiformes

- ▶ Le développement de l'IoT doit s'appuyer sur un environnement réglementaire et juridique sécurisé.
- ▶ Enjeux réglementaires et juridiques sont multiples :
 - ▶ La qualification réglementaire des acteurs de l'IoT;
 - ▶ Garantir la nécessaire confiance des utilisateurs, laquelle dépend de plusieurs leviers;
 - ▶ L'utilisation de ressources rares nécessaires au développement de l'IoT.



Les acteurs de l'IoT sont-ils soumis à la réglementation des communications électroniques

- ▶ La réponse est plus ou moins claire selon les acteurs.
 - ▶ Acteurs intervenant sur les objets : certains ne sont pas concernés par la réglementation des communications électroniques (ex : concepteurs d'objets à connecter...), d'autres si (fabricants : exigences essentielles).
 - ▶ Acteurs intervenant sur la connectivité : oui
 - Opérateurs qui établissent et exploitent des réseaux de communications électroniques;
 - Gestionnaires de réseaux d'énergie ou d'infrastructures qui mettent ceux-ci à disposition.
 - ▶ Acteurs intervenant sur la couche des données : la question peut se poser pour les fournisseurs de services connectés, même s'ils n'assurent pas eux-mêmes la transmission du signal.



Les acteurs de l'IoT sont-ils soumis à la réglementation des communications électroniques

- ▶ Le prestataire de services connectés peut être qualifié de fournisseur de services de communications électroniques dès lors qu'il :
 - Assure la fourniture d'un service au public reposant principalement sur la transmission de signaux,
 - Et assume la responsabilité contractuelle de cette transmission vis-à-vis du client,
 - ... quand bien même il n'assure pas lui-même la transmission des signaux.
- ▶ Conséquence : les obligations réglementaires applicables aux fournisseurs de services de CE s'appliquent (qualité de service, paiement de redevances, communications d'informations périodiques, etc.).
- ▶ Débat : faut-il appliquer strictement ces obligations, sachant que certains d'entre elles sont inadaptées (par exemple : interceptions de sécurité, appels d'urgence sauf pour voitures connectées)? Ou n'est-il pas préférable de les alléger dans une logique d'expérimentation (cf. le « bac à sable réglementaire » de l'ARCEP)?



Quels sont les leviers pour instaurer un climat de confiance parmi les utilisateurs ?

- Premier levier : la liberté d'utiliser ou non un objet connecté doit être protégée (cf. par exemple, la problématique des compagnies d'assurances)
- Deuxième levier : réglementation de l'objet connecté
 - Agrément à obtenir ou déclaration à procéder par le fabricant ou l'importateur de l'objet connecté préalablement à sa mise sur le marché pour s'assurer de sa conformité aux exigences essentielles.
- Troisième levier : la réglementation des données
 - Sans confiance des utilisateurs dans la collecte, le stockage, le traitement et la restitution des informations issues des objets connectés, pas de développement de l'IoT
 - Sans exploitation des données, pas de business viable pour l'IoT

Quels sont les leviers pour instaurer un climat de confiance parmi les utilisateurs?

► Troisième levier :

Il faut donc des outils pour réglementer la collecte, l'usage et la sécurité des données:

- La protection et la confidentialité des données doivent être traitées dès la conception de l'objet (« Privacy by design »).
 - ✓ Voir étude de 2014 de Fortify, division d'HP dédiée à la cybersécurité : beaucoup d'objets connectés non sécurisés
 - ✓ Cyberattaques et vols de données (Instagram, Adobe, Sony, Ashley Madison...)
- Le service proposé doit demander le minimum d'infos nécessaires (« Privacy by default »)
- Obligation d'information de l'utilisateur sur l'identité du collecteur, la finalité de la collecte des données, son caractère obligatoire ou facultatif, les destinataires de ces données, le droit d'opposition, d'accès, de modification et de suppression...
- Système de déclaration/autorisation pour tout traitement de données personnelles (ex: loi française) ou de responsabilisation/contrôle des acteurs (RGPD)
- Dispositif de sanctions dissuasives, appliqué en cas de manquement



Quels sont les leviers pour instaurer un climat de confiance parmi les utilisateurs?

- ▶ Quatrième levier : la couverture du territoire et la résilience qui peuvent être garanties de différentes manières impliquantes pour les régulateurs, outre les solutions de type LPWAN :
 - Une redondance inter-technologies (multi-sourcing), ce qui suppose une réglementation et une régulation favorisant la multiplicité des technologies aussi bien pour des réseaux à portée locale ou au déploiement étendu (neutralité technologique, logique d'expérimentation);
 - Une haute disponibilité intra-technologique (multi-roaming) = itinérance
- ▶ Cinquième levier : à moyen terme, il faudra veiller à mettre en place des standards capables de garantir une interopérabilité entre objets connectés afin d'augmenter le bien-être des utilisateurs, la fluidité des objets et de maximiser les effets de réseau (ex: voitures connectées)



Quelle utilisation des ressources rares pour le développement de l'loT?

- La fourniture de services connectés mobilise souvent deux ressources rares : les fréquences et les adresses. Elles le seront d'autant plus que la croissance des objets connectés est exponentielle.
- Problématiques pour les fréquences :
 - Le développement de l'loT devrait principalement être porté par l'utilisation des technologies sans fil et mobiles.
 - En fonction des usages, les acteurs auront tendance à se tourner soit vers des bandes libres, soit vers des bandes attribuées à titre exclusif.
 - Plusieurs enjeux :
 - Développement de la 5G (problématiques réglementaires : déploiement et redevances)
 - Etre dans une démarche d'anticipation en veillant, à moyen terme, à la disponibilité des ressources en fréquences pour l'ensemble des acteurs, y compris les bandes libres (risques de brouillages)
 - Adapter les conditions d'usage de certaines bandes libres (logique d'expérimentation), tout en veillant à minimiser les brouillages



Quelle utilisation des ressources rares pour le développement de l'IoT?

- Problématiques pour l'identification des objets, compte tenu de la croissance des objets connectés :
 - Eviter une pénurie des identifiants ouverts (numéros de téléphone mobiles, identifiants de carte SIM, adresses IP...).
 - Certains opérateurs internationaux souhaiteraient accéder à une itinérance permanente au niveau mondial avec les ressources nationales de leur pays d'origine, ce qui ne va pas sans poser de problèmes...



Conclusion : monter dans le train de la révolution de l'loT ou le regarder passer

- Différentes approches de réglementation et de régulation sont possibles...
- L'loT est un sujet de court terme, mais plus encore de moyen et de long terme. Il pose des problématiques qu'il faut savoir et pouvoir anticiper...