Sujet national pour l'ensemble des centres de gestion organisateurs

CONCOURS INTERNE

D'INGÉNIEUR TERRITORIAL

SESSION 2017

ÉPREUVE DE PROJET OU ÉTUDE

ÉPREUVE D'ADMISSIBILITÉ :

L'établissement d'un projet ou étude portant sur l'une des options, choisie par le candidat lors de son inscription, au sein de la spécialité dans laquelle il concourt.

Durée : 8 heures
Coefficient : 7

SPÉCIALITÉ : INFORMATIQUE ET SYSTÈMES D'INFORMATION

OPTION : RÉSEAUX ET TÉLÉCOMMUNICATIONS

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- L'utilisation d'une calculatrice autonome et sans imprimante est autorisée.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 74 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.
S'il est incomplet, en avertir le surveillant.

- Vous préciserez, le cas échéant, le numéro de la question et de la sous-question auxquelles vous répondrez.
- Des réponses rédigées sont attendues et peuvent être accompagnées si besoin de tableaux, graphiques, schémas…

Vous êtes ingénieur territorial au sein de la Direction des systèmes d'information et des services numériques (DSISN) de la métropole d'INGECO.
Votre direction est sollicitée pour apporter sa contribution au projet global smart city de l'exécutif.
Votre directeur fait appel à vous pour éclairer les choix des élus dans ce domaine.

À l'appui de l'annexe A, vous répondrez aux questions suivantes :

Question 1 (4 points)

a) Vous rédigerez une note présentant les différents standards techniques applicables au domaine des objets connectés.
b) À partir de ces éléments, vous ressortirez quatre points techniques que vous souhaitez retenir pour mettre en évidence les particularités des réseaux permettant de relier des objets connectés et qui justifient l'existence de standards ou normes spécifiques.

Question 2 (3 points)

a) Vous rédigerez une note présentant les différentes solutions technologiques disponibles actuellement pour gérer des réseaux sans fil permettant de relier des objets connectés.
b) Vous expliquerez pourquoi certaines solutions sont plus adaptées que d'autres à la construction d'un réseau d'objets connectés.

Question 3 (5 points)

Vous rédigerez une note sur la sécurité des réseaux d'objets connectés et sur les enjeux juridiques.

Question 4 (5 points)

La métropole d'INGECO a décidé de déployer un réseau d'objets connectés pour gérer ses 10 000 places de stationnement, localisées en voirie et en souterrain. L'objectif est de fluidifier le trafic, réguler le stationnement et réduire la pollution liée aux déplacements inutiles.
Vous rédigerez la partie du cahier des clauses techniques particulières (CCTP) pour sélectionner une solution globale pour un réseau d'objets connectés afin de gérer les 10 000 places de stationnement d'INGECO.

Question 5 (3 points)

a) Quels sont les services innovants que pourrait proposer la collectivité auprès des citoyens via les objets connectés ? Vous présenterez leurs avantages et leurs inconvénients ainsi que leurs modalités de mise en œuvre.
b) Que proposez-vous pour le traitement et l'exploitation des données collectées ?

Liste des documents :

Document 1 : « Quel(s) réseau(x) pour la ville connectée ? » – *Pierre MANGIN et Ariel GOMEZ – smartcitymag.fr* – Juin 2016 – 6 pages

Document 2 : « Le vrai du faux sur les réseaux pour objets connectés en 5 questions clés » – Sylvain ARNULF – *usine-digitale.fr* – 9 décembre 2015 – 5 pages

Document 3 : « Villes intelligentes : cinq zones de sécurité à surveiller par les DSI » – *Christophe AUBERGER – smartcitymag.fr* – Juin 2016 – 1 page

Document 4 : « Peut-on penser la sécurité des objets connectés dès leur conception ? » – *Stéphanie CHAPTAL – zdnet.fr* – 4 juillet 2016 – 3 pages

Document 5 : « Sécurité des objets connectés » (extraits) – *Cyrille SCHOTT – Institut national des hautes études de la sécurité et de la justice (INHESJ)* – Décembre 2014 – 37 pages

Document 6 : « Saint-Sulpice-la-Forêt : le village breton devenu smart city » – *Christophe GUILLEMAIN – smartcitymag.fr* – Juin 2016 – 4 pages

Document 7 : « Smart parking : 18 mois pour ré-inventer le stationnement » – *Pierre MANGIN – smartcitymag.fr* – Juin 2016 – 6 pages

Document 8 : « Réduire les ordures ménagères grâce à la tarification incitative » – *Christophe GUILLEMIN – smartcitymag.fr* – Novembre 2016 – 2 pages

Document 9 : « Smart city et citoyen » – *Michel BAZAN – France Stratégie – strategie.gouv.fr* – 11 mai 2016 – 6 pages

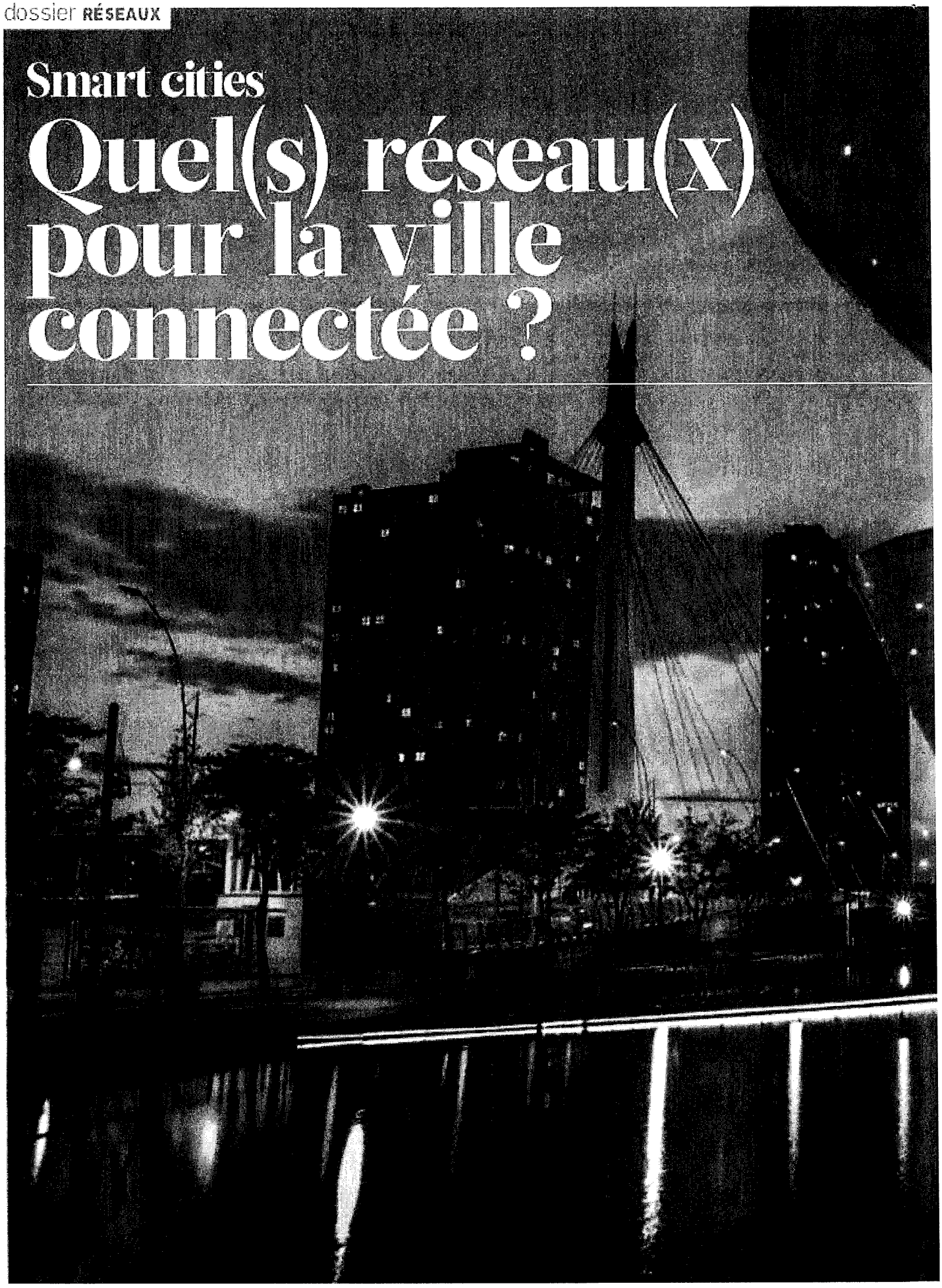
Annexe A : « Présentation de la stratégie globale smart city » (extrait) – *Président d'INGECO* – Janvier 2017 – 1 page – l'annexe n'est pas à rendre avec la copie

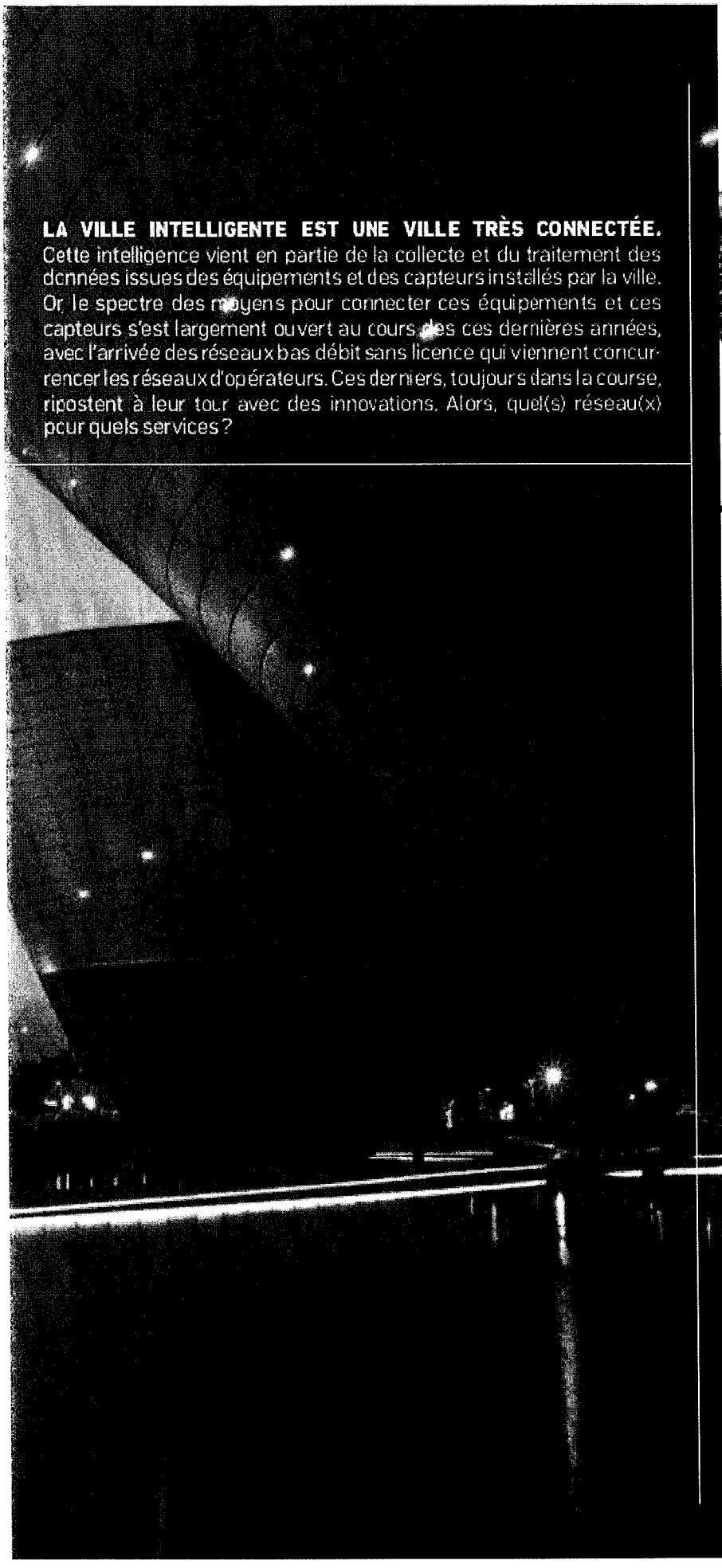
Documents reproduits avec l'autorisation du CFC
Certains documents peuvent comporter des renvois à des notes ou à des documents non fournis car non indispensables à la compréhension du sujet.

DOCUMENT 1

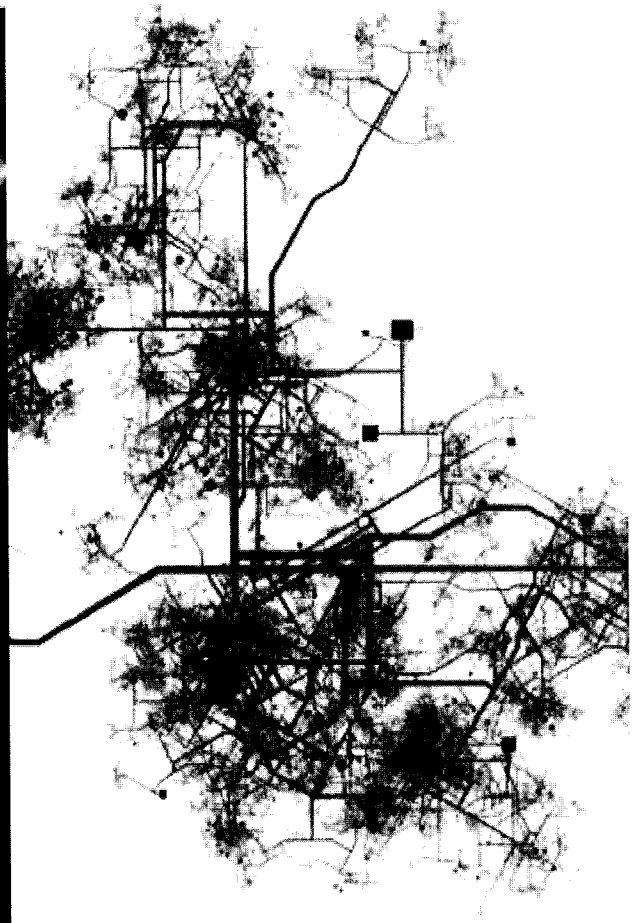
Smart cities

Quel(s) réseau(x) pour la ville connectée ?





LA VILLE INTELLIGENTE EST UNE VILLE TRÈS CONNECTÉE. Cette intelligence vient en partie de la collecte et du traitement des données issues des équipements et des capteurs installés par la ville. Or, le spectre des moyens pour connecter ces équipements et ces capteurs s'est largement ouvert au cours des ces dernières années, avec l'arrivée des réseaux bas débit sans licence qui viennent concurrencer les réseaux d'opérateurs. Ces derniers, toujours dans la course, ripostent à leur tour avec des innovations. Alors, quel(s) réseau(x) pour quels services ?



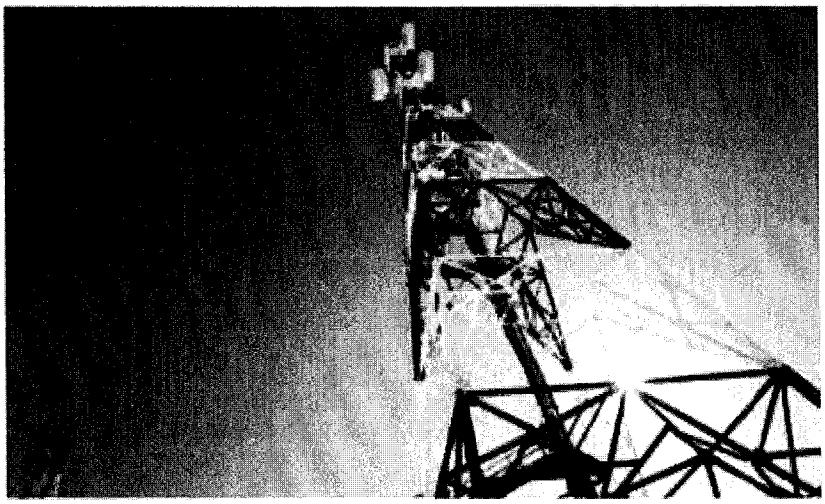
Dans la ville intelligente, la donnée est au centre de tout. Qu'il s'agisse de celle concernant l'occupation ou non d'une place de parking, du temps de passage des bus aux différents arrêts, ou encore de celle concernant la consommation et les fuites d'eau, cette donnée issue d'« objets connectés », pour être exploitable, doit être traitée par des algorithmes dits de Big Data. Mais pour être ainsi analysée en mise en valeur, elle doit d'abord être transportée depuis les capteurs et les équipements connectés qui l'ont générée, puis renvoyée, sous une forme « *utile* » vers les terminaux informatiques et les smartphones qui permettront à leurs destinataires (services municipaux, sociétés de gestion, citoyens…) d'en prendre connaissance et d'en faire bon usage pour prendre les bonnes décisions.

Nous n'allons pas nous attarder ici sur les grands réseaux fixes des opérateurs déjà installés (réseau cuivre) ou encore en cours de déploiement (en fibre optique) pour transporter les grands flux des données, mais plutôt sur les réseaux sans fil qui apportent une nouvelle forme de connectivité à la ville. Pendant de nombreuses années, les seules solutions disponibles pour connecter des objets ou des équipements à distance sans installer une ligne téléphonique fixe étaient les solutions dites machine to machine (ou MtoM) des grands opérateurs mobiles (Orange, SFR, Bouygues Telecom). Moyennant l'installation d'une carte SIM et un abonnement date de quelques euros par mois, elles permettaient à des équipements aussi divers que des motrices de train ou des distributeurs automatiques de confiseries d'indiquer leur position et de remonter de données à distance.

Aujourd'hui, le choix des moyens pour transporter ces données de la ville connectée s'est largement ouvert, grâce notamment à l'émergence d'une éco-

Fabrice Stevens,
Orange Business Services
« Il faut une approche pragmatique et modulaire »

Face aux multiples options M2M et IoT qui s'affirment depuis quelques mois sur le marché, Orange a décidé d'être « très modulaire ». « Nous considérons qu'il y a 4 briques » explique Fabrice Stevens, directeur MEM d'Orange Business Services (OBS). Des briques qui correspondent au choix des capteurs, des solutions de connectivité, système de collecte et du contrôle. Pour chaque cas d'usage, il faut se déterminer sur la fréquence des relevés, et le volume de données : « Pour des solutions de vidéo-surveillance en temps réel, il faut plus de débit et de qualité de service que pour certains objets. La durée de vie est un autre critère : s'agit-il d'une installation définitive ou susceptible d'être modifiée, déménagée? Pour certains équipements, il est question de 5 ans, voire de 10 ans d'autonomie ». « Pour des objets non alimentés électriquement, les solutions LPWAN (Low power wide area network) de Sigfox ou LoRA paraissent bien adaptées, poursuit Fabrice Stevens, grâce à leur faible consommation d'énergie, au chiffrement des données, et à autonomie des batteries satisfaisante. Les usages possibles sont désormais bien connus : gestion des déchets, détection/prévention d'incendie, suivi de température, du taux de CO2, traçabilité sur des équipements ou engins couteux, et tout le marché du 'smart metering' (relevé de compteurs ou consommation) ». N'utilisant pas des fréquences licenciées d'opérateurs (fréquences «libres»), ces solutions garantissent-elles une qualité de service suffisante? « Pas totalement, c'est pour cette raison que nous poussons à ce que, avec une normalisation, ces bandes de fréquences (868 MHz en ce qui nous concerne) puissent être licenciées aux opérateurs ». Pour les autres solutions possibles, trois groupes de travaux de normalisation sont à suivre, estime Fabrice Stevens : l'évolution de la 2G, avec l'EC-GSM, pour l'adapter aux besoins IoT (horizon 2017-2018), l'évolution de la 4G (LTE-M, etc.; horizon 2018) et le NB-IoT (Narrow-band IoT, horizon 2018). « Mais en attendant 2018, pour répondre aux besoins actuels, en complément du cellulaire, le LPWAN, dont LoRa nous paraît le plus pertinent, a été retenu par Orange Labs, après comparaisons d'une dizaine de solutions du marché (dont celles de Huawei ou Sigfox) ».



nomie de l'Internet des objets qui concerne aussi bien les objets connectés grand public que les usages des collectivités. Il n'est pas rare, en effet, que les données d'un collier connecté pour chien (qui permet de le localiser et de connaître son activité physique) empruntent les mêmes réseaux que celles des compteurs d'eau. En introduisant des technologies de réseau bas débit sans licence, dont l'abonnement est facturé quelques euros par an (au lieu de quelques euros par mois comme les cartes SIM), pour un flux de données très faible, cet écosystème technico-économique a ouvert de nombreuses possibilités de nouveaux services puisqu'il est possible, dans ces conditions, d'envisager un retour sur investissement (ROI) jadis inenvisageable.

Selon les technologies utilisés, le signal de chaque antenne sur un réseau bas débit peut porter plus ou moins loin : 12 à 15 km en technologie Sigfox, dans les 20 km en LoRaWAN et jusqu'à 60 km en Qowisio.

Les bons critères pour les bons choix

Pour la ville, le bon choix des réseaux dépend avant tout d'un certain nombre de critères qui vont déterminer le choix de la meilleure technologie. Dans ces critères, la question du coût occupe une place importante, puisque lorsque l'on envisage le déploiement de 20 000 capteurs dans sa commune, quelques euros de plus ou de moins par an et par capteur auront un impact non négligeable sur le budget global comme sur le retour sur investissement du projet. Mais avant de se poser la question du coût, il faut se poser celles de l'emplacement des capteurs qui génèrent les données (à l'air libre, en sous-sol, dans des bâtiments ?), celle de la nature et du volume du flux des données à transporter (des simples données informatiques, des images, de la vidéo...), celle de la fréquence d'émission des données (permanente, une fois par jour, quelques fois par mois ou par an...) et du besoin ou non d'échanger des données dans les deux sens entre les capteurs et les serveurs de traitement et de collecte. Le besoins ne sont pas du tout les mêmes entre un réseau de vidéosurveillance sans fil d'un chantier, qui devra transporter des images en haute définition, un capteur de la qualité de l'air qui enverra quelques bits de données plusieurs fois par jour et un compteur d'eau qui transmettra des données une fois par mois.

Autre facteur important qui entre en ligne de compte : l'autonomie attendue des capteurs, puisque, lorsqu'ils sont déployés en grand nombre, il n'est pas envisageable d'en changer les batteries tous les trois mois. Certains capteurs de dernière génération installés sur les réseaux bas débit sont prévus pour offrir une autonomie qui dépasse les 5 ans.

Partant de cette matrice, la connectivité des équipements ou des objets connectés pour les villes intelligentes peut être architecturée soit via des services opérateurs sur les grands réseaux mobiles (2G, 3G, 4G et future 5G), soit via de nouvelles alternatives, sur des fréquences « *libres* », telles que LoRA, Sigfox, ou encore via des solutions propriétaires intégrées de type M2C City ou Actility.

Pour un aménageur, ces diverses options restent ouvertes - réseau sans licence ou réseau d'opérateur - avec leurs avantages et leurs inconvénients.

Réseaux bas débit, les « nouveaux barbares » des fréquences

La grande nouveauté de ces toutes dernières années, c'est l'émergence de nouvelles technologies de réseau sans fil bas débit, longue portée et sans licence que l'on range dans la catégorie des LPWAN (*Low-power wide-area networks*, réseaux à basse consommation et longue portée). C'est dans cette catégorie que se situent les technologies Sigfox et LoRaWan, complétées par l'UNB (Ultra Narrow Band, bande ultra-étroite) de Qowisio, et par le mix LoRa plus WiFi porté par Archos (cf plus bas).

L'exploitation de ces technologies répond à des modèles économiques différents.

Sigfox, opérateur international d'origine française, utilise une solution propriétaire. Son réseau s'étend sur 14 pays (mai 2016) et enregistre plus de 7 millions d'objets connectés. En octobre 2015, Sigfox après avoir obtenu la certification américaine FFC, a signé un marché avec la ville de San Francisco pour le développement d'un réseau pilote IoT (objets connectés à Internet). Plusieurs dizaines d'autres villes américaines ont montré un intérêt pour des projets identiques.

En avril 2016, Sigfox a signé un partenariat avec Microsoft pour intégrer son offre Cloud à la plateforme Azure IoT Hub pour le stockage et l'analyse des données recueillies. Sigfox a également signé un accord avec Altice (maison mère de SFR) pour que toutes les branches télécom du groupe dans le monde utilisent la technologie Sigfox dans le cadre de leurs déploiements IoT.

Pour sa part, la technologie LoRA (Long Range WAN -wide-area network) est un standard reposant sur une technologie de modulation propriétaire utilisant ses propres composants. Les opérateurs le déploient au niveau national mais en le centrant sur les villes. Il a été retenu par Bouygues Telecom et Orange (sur la bande de 868 Mhz) et par plus de 50 opérateurs dans le monde. La connexion à internet, chiffrée, pour des réseaux M-to-M ou des objets est assurée par des passerelles propriétaires et apporte des débits allant de 0,3 kbit/s à 50 kbit/s. Les composants électroniques proviennent de l'acquisition de la startup grenobloise Cycléo par Semtech en 2012, ce dernier restant le fournisseur officiel.

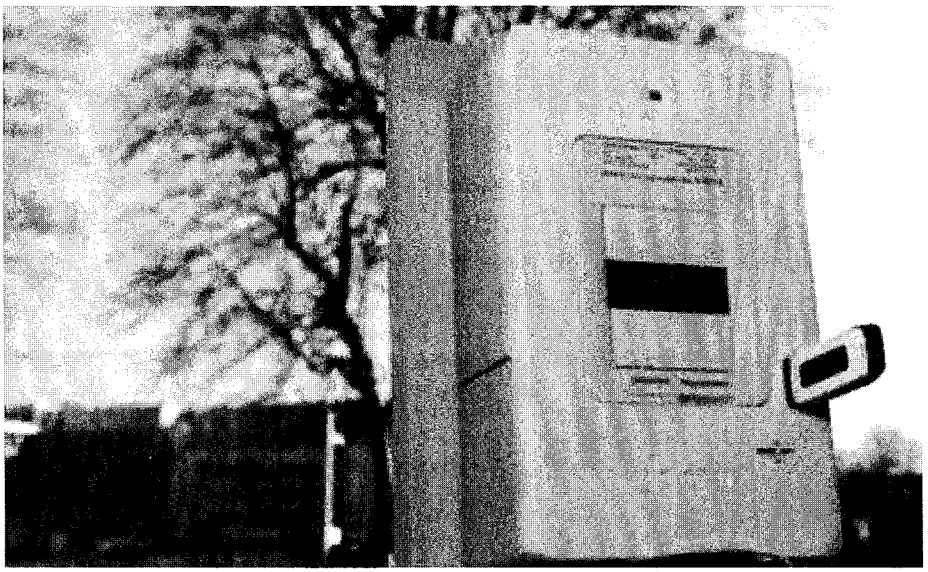
Autre acteur, autre techno : la société angevine Qowisio. Cet opérateur de réseau indépendant, a commencé à faire parler de lui lorsqu'il a levé il y a un an 10 millions d'euros pour financer son développement national. Qowisio exploite la technologie UNB (Ultra Narrow Band : ultra-étroite), qui peut se combiner avec LoRa ou avec la technologie Sigfox. Cet opérateur, qui vient tout juste de lancer officiellement son offre commerciale (cf page 8) se veut « *le plus ouvert possible* » à l'opposé d'un Sigfox qui reste sur un système propriétaire.

Mentionnons pour clore cette liste l'initiative d'Archos, société que l'on connaît surtout pour ses smartphones et ses tablettes. Sa solution, conçue notamment pour opérer à l'intérieur des bâtiments, repose sur un maillage de 'pico-passerelles', connectées en WiFi et connectées ensuite au réseau LoRa. Son coût est très modique, très inférieur à celui des infrastructures traditionnelles. Le déploiement de 200 000 pico-passerelles a été prévu pour lancer le service. Le modèle économique, encore en construction, reposerait sur un paiement annuel de 10 à 50 centimes par an, par objet connecté.

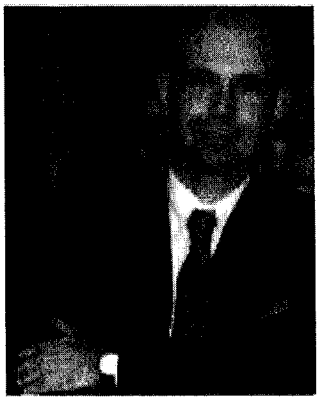
La riposte des opérateurs mobiles

Pour leur part, les opérateurs mobiles ont été un peu pris de court par cette déferlante autour de l'internet des objets, un nouveau marché auquel leurs offres machine to machine ne répondaient que très imparfaitement. Focalisés sur le développement de réseaux capables d'offrir toujours plus de débit et de services (comme la 4 G), sans trop se soucier de la consommation électrique des terminaux (les smartphones surtout), ils misaient sur la prochaine génération technologique des réseaux (la 5G, prévue à partir de 2020) pour intégrer pleinement les objets connectés dans leur écosystème. Or, la rapidité du développement des objets connectés, y compris ceux des villes, les a conduit à chercher rapidement des solutions pour ne pas rater un train qui était déjà bien lancé.

Si SFR, déjà empêtré dans un endettement gigantesque et de gros investissements à venir dans son réseau 4G, a fait le choix de signer un accord global avec Sigfox, Bouygues Télécom et, en un peu plus tard, Orange, se sont lancés dans le déploiement de réseaux LoRa. Ils ont pour cela profité de l'avantage de leurs infrastructures existantes pour le faire à moindre coût.

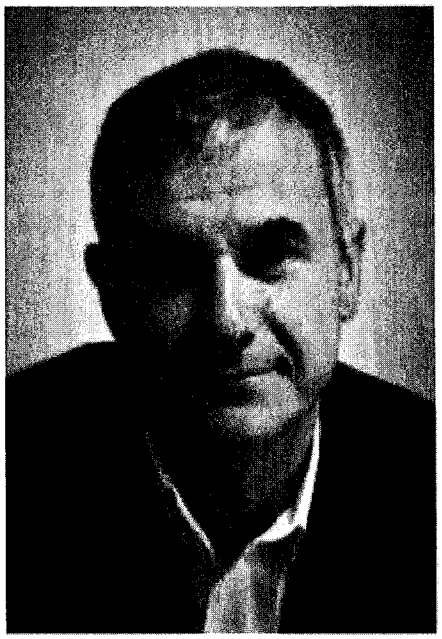


Le compteur intelligent Linky, qui suscite autant de controverses (cf page 10), permet de remonter les données de consommation via les réseaux radio, évitant ainsi de mobiliser des agents pour les relevés manuels.



Stéphane Lelux, fondateur du cabinet de conseil Tactis

Michel Liotard, Ericsson
« Nous nous fions aux grands standards »



Les nouveaux et futurs standards ' NB-IoT' (Narrow band IoT), définis sur les réseaux mobiles 2G et 4G ont l'avantage de disposer déjà d'une infrastructure. « Il suffit d'une mise à jour logicielle des équipements émetteurs/récepteurs» explique Michel Liotard, consultant IoT d'Ericsson Région Méditerranée. La 4G devrait répondre à un grand nombre de besoins de connexion IoT, « en apportant des services identiques à ceux de LoRA. Et la 5G, dans un futur proche, regroupera l'ensemble de ces technologies, en englobant M2M, IoT, le tout jusqu'aux très hauts débits ». Selon Michel Liotard, les spécifications NB-IoT pour les fréquences LTE ou GSM appelés 'EC-GSM-IoT', devraient être disponibles avant la fin de cette année 2016. « Plusieurs technologies vont coexister pour répondre à des besoins de débit différents selon les objets ou équipements connectés. Ainsi le LPWAN (Low power wide area network) - choisi par Sigfox et LoRA - apporte, il est vrai, un gain de signal, permettant d'émettre et recevoir jusqu'au niveau -1 des bâtiments en dur ». « Ericsson, pour le moment, ne s'est pas positionné sur le LPWAN, car, restant fidèle au modèle des réseaux radio cellulaires, le groupe oeuvre auprès des organismes de normalisation. LoRA et Sigfox sont des initiatives qui restent «propriétaires», sauf à ouvrir leur portefeuille de brevets». Aux Etats-Unis, Ericsson s'est engagé sur le« narrowband IOT » cellulaire 4G aux cotés de NTT et Verizon. « Dans les deux ans, selon les options prises par les opérateurs, le paysage peut encore changer. Et il est sans doute illusoire de penser que l'on va déployer un système autonome pour une durée de 10 ans ; car la technologie risque d'être dépassée dans des délais plus rapprochés, de l'ordre de 5 ans. D'où l'importance des standards et des normes » souligne Michel Liotard.

« Plusieurs technologies vont coexister pour répondre à des besoins de débit différents selon les objets ou équipements connectés. »

Mais si LoRa leur permettait d'accrocher quelques marchés naissants, cette technologie portait en elle la tare originelle de pouvoir être opérée sans licence, c'est-à-dire, sans les gardes fou d'usage qui permettent de garantir une qualité de communication. N'importe quelle entreprise peut en effet monter son propre réseau et l'opérer sans grand contrôle extérieur. Un mode de fonctionnement qui fait peser une incertitude intolérable pour un opérateur digne de ce nom.

Les opérateurs mobiles, avec l'aide de leurs fournisseurs, les équipementiers télécom (tels qu'Ericsson, Nokia ou Huawei), ont donc cherché la manière de rendre compatibles leurs réseaux existants avec les besoins de l'internet des objets, tout en restant dans l'univers normé des réseaux dit « *opérés* ».

Les villes connectées grâce aux réseaux 2G et 4G ?

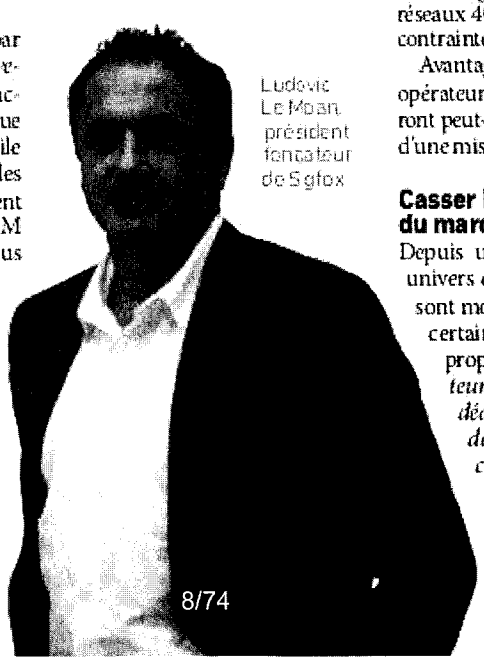
Cette évolution en cours est notamment portée par la technologie EC-GSM (EC pour *extended coverage*, ou couverture élargie). Cette technologie fonctionne sur la bande de fréquence des 900 MHz - que les opérateurs exploitent déjà en téléphonie mobile 2G et 3G - et pour lesquelles ils ont acheté à l'Etat des licences d'exploitation. L'EC-GSM offre notamment une bien meilleure couverture que le réseau GSM 2G classique (on parle d'une portée sept fois plus importante), avec la particularité de bien traverser les murs et de pouvoir être utilisée dans des endroits tels que les parkings ou autres installations souterraines pour équiper par exemple des compteurs d'eau.

Autre aspect crucial : l'amélioration de l'autonomie des appareils que permet cette technologie. A l'instar de ce qui est fait sur les réseaux Sigfox et LoRa, la techno EC-GSM permet de laisser les capteurs en veille profonde lorsqu'ils ne sont pas sollicités, optimisant ainsi leur autonomie. C'est une évolution majeure, prévue pour 2017, par rapport aux réseaux de téléphonie traditionnels, qui échangent en permanence des informations avec les terminaux qui les utilisent.

Testée sur les réseaux 2G, l'EC-GSM a également vocation à être déployée sur le standard 4G, qui fait actuellement l'objet de gros investissements de la part des opérateurs. La 4G de catégorie 0, qu'on appelle également LTE-M (pour « machine ») permet des débits théoriques jusqu'à 1 Mbit/s. Orange teste cette technologie avec Ericsson, ce qui lui permettra (à partir de 2018) d'avoir une offre étendue pour l'Internet des objets (cf en encadré l'interview de Fabrice Stevens).

Ajoutons à ces évolutions en cours celle du *Narrow Band IoT* (en cours de standardisation) qui devrait également, à l'horizon 2018, permettre aux réseaux 4G de prendre en compte les besoins et les contraintes des écosystèmes connectés des villes.

Avantage majeur de ces technologies pour les opérateurs télécom « *traditionnels* » : elles pourront peut-être déployées très rapidement par le biais d'une mise à jour logicielle de leurs équipements.



Ludovic Le Moan, président fondateur de Sigfox

Casser la structuration du marché en silos ?

Depuis une dizaine d'années, dans chacun des univers de services que gère la ville, les acteurs se sont modernisés dans la voie de la digitalisation : certains utilisent leurs propres capteurs et leurs propres dédiés réseaux de collecte. « *Ces acteurs n'ont pas attendu les nouveaux réseaux dédiés aux objets connectés / LPWAN : ils ont développé des solutions propriétaires, verticales, grâce aux nouvelles possibilités du digital. On est donc face à une structuration du marché en silos qui va progressivement*

Franck Moine, directeur général adjoint d'Objenius (Bouygues) « LoRA est actuellement une bonne solution »

Pourquoi avoir retenu l'offre LoRA ?
Nous avons décidé de créer Objenious sur l'offre LoRA pour travailler, de façon encore plus réactive avec un écosystème qui puisse rendre des services associés (collecte, supervision des données...). Nous nous sommes appuyés sur Bouygues Télécom pour déployer des antennes : il suffit d'une antenne et d'un 'gateway' par point haut. La portée d'une antenne est en théorie de 20 à 40 km, mais en ville, c'est environ 1 km. Nous en aurons déployé 4000 à la fin 2016, ce qui nous donnera un taux de couverture dépassant 50 % des villes. A ce jour, 30 « unités urboines » sont couvertes. Beaucoup d'objets n'étaient pas connectables via le GSM classique : trop de consommation d'énergie, nécessitant des opérations lourdes de renouvelement des batteries, etc.

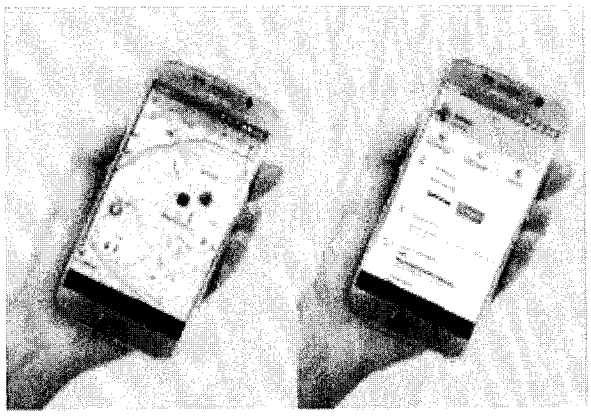
Quels sont les points forts de la solution ?
LoRa est actuellement l'une des meilleures technologies bidirectionnelles disponibles. Elle répond bien aux utilisations indoor dans des zones enfouies (relevés de compteurs, etc), où il suffit de transmettre quelques dizaines d'octets (débit de 300 bit/s à 50 kbit/s). Les données sont chiffrées, avec un tiers de confiance pour une partie des clés (Atos Bull, en France). Les 'chipsets' radio sont très économes en énergie (moins de 10 mAh), et leur coût est inférieur à 5 voire 2 dollars (contre 30 à 40 dollars pour les solutions en 4G). Grâce à un protocole radio spécifique (« haute sensibilité») il est possible de filtrer les bruits électromagnétiques. La technologie LoRA présente aussi l'avantage d'une géolocalisation pour les objets ou instruments qui peuvent être déplacés. Ceci explique pourquoi nous sommes membre de la LoRA Alliance aux côtés de 56 autres opérateurs dans le monde, dont 16 ont commencé les déploiements. C'est en train de devenir un standard de fait.

Avez-vous déjà des applications de référence?
Nous avons démarré un projet pilote de 'parking intelligent' avec le groupe Colas, qui utilise LoRA, mais également pour la gestion de flottes de leurs équipements de chantier. Dans l'éclairage public, il va devenir possible de piloter les réverbères à l'unité et ainsi décider, par exemple, d'en éteindre un sur deux quand c'est possible. De même, toute la gestion technique des bâtiments va pouvoir en bénéficier, notamment pour des économies d'énergie que la loi va bientôt imposer.

évoluer. Certains acteurs vont commencer à converger. L'important est de faire en sorte que les nouvelles générations de réseaux intelligents deviennent interopérables et en partie mutualisables », estime Stéphane Lelux, président de cabinet de conseil Tactis. Parmi ces pionniers des services « *connectés* » pour les villes qui font converger leurs réseaux, on compte des sociétés telles que M2O City, une filiale commune de Veolia et d'Orange. Initialement focalisée sur la gestion de l'eau (filiation à Veolia oblige), M2O City s'est depuis ouvert à la gestion de l'énergie, de l'air, du bruit... « *Nous avons commencé par connecter 500000 compteurs d'eau*, explique Stéphane Dumont, directeur marketing de la société, *aujourd'hui, avec 2000 villes couvertes et 1,9 millions d'objets connectés, nous sommes le premier acteur de ce marché* ». La société se vante en effet de traiter pas moins de « *74 millions de trames radio par semaine* ». Techniquement parlant, l'approche de M2O City est totalement agnostique en matière de réseaux. « *Nous sélectionnons la techno plus adaptée aux besoins de nos clients* », ajoute Stéphane Dumont. Selon la configuration de l'agglomération, les antennes peuvent être placées à hauteur d'homme comme en hauteur dans des immeubles. La technologie de son concentrateur « *home rider* » permet ensuite de tout agréger pour traiter ensuite les données et les rendre utiles.

Mutualiser les réseaux pour baisser les coûts

« *Plus de 90 % du temps, les réseaux dédiés aux relevés (eau, gaz, électricité) ne sont pas occupés. Donc, il y a un gain de productivité à mutualiser les infrastructures pour réduire les CAPEX et OPEX. Mais il faut le faire de façon éclairée car on augmente le risque d'ouvrir la voie aux actes de malveillance. Il faut, donc se soucier simultanément de renforcer la sécurisation de l'ensemble et rester très vigilant sur les risques encourus* », ajoute Stéphane Lelux.



Un vélo équipé d'un capteur peut être facilement localisé via les réseaux. L'application qui sert à retrouver ce vélo indique aussi la durée de vie restante de la batterie.

En parallèle il faut également considérer les infrastructures vitales qui vont devoir rester indépendantes, non mutualisées et non interconnectés à Internet et aux grands réseaux télécoms pour réduire leur vulnérabilité.

Les aménageurs des *smart cities* devront donc réfléchir en amont à la mutualisation des ressources au moment de faire des choix technologiques pour éviter le « couteux » travers de monter un réseau différent par direction métier. Ils devront également veiller à prévenir les risques d'interférence et de saturation qui existent sur les réseaux sans licence, notamment dans les villes.

Ces nouvelles solutions de connectivité radio utilisant des fréquences libres (LoRA, Sigfox...) sont en effet exposées à des risques de perturbation. Mais ce constat ne doit pas conduire à les exclure. Elles apportent souvent la bonne réponse.

PIERRE MANGIN, avec **ARIEL GOMEZ**

Le vrai du faux sur les réseaux pour objets connectés en 5 questions clés

Sylvain Arnulf | Publié le 09 décembre 2015 | usine-digitale.fr

Sigfox ? LoRa ? Qowisio ? Quels sont les points à surveiller au moment de choisir un réseau pour ses objets connectés ? Sur quels aspects subsiste-t-il encore des parts d'ombre ? L'Usine Digitale tente de faire le tri entre les annonces des opérateurs et les faits.

Qui couvre quoi ?

Aucun opérateur ne publie, pour l'instant, de carte précise de couverture. Difficile de savoir qui a le meilleur réseau. Pour compliquer le tout, l'Ultra Narrow Band (Qowisio et Sigfox) et l'étalement de spectre (LoRa) sont deux technologies aux philosophies différentes, impossible donc de comparer le nombre d'antennes pour savoir qui a la meilleure couverture. Par définition, un réseau LoRa a besoin de plus d'antennes que Sigfox pour proposer un service équivalent.

Une chose est sûre : fin 2015, Sigfox est – largement – devant ses concurrents. Ses 1 500 antennes couvrent 91% de la population française, "*l'équivalent des réseaux 3G des autres opérateurs*", selon Thomas Nicholls, responsable marketing. S'il reste des zones blanches dans des régions montagneuses et isolées, Sigfox les corrige progressivement. La start-up compte densifier son réseau en fonction des besoins même si selon elle, son millier et demi d'antennes suffit déjà largement. *"Le réseau est largement scalable et peut gérer de très fortes capacités"*, assure le porte-parole..

Bouygues Télécom et LoRa sont encore en phase de pilotes. Ils prévoient l'ouverture commerciale de leur réseau au premier trimestre 2016. Orange annonce qu'il irriguera 17 agglomérations au démarrage soit 1200 communes. Bouygues promet de couvrir "l'essentiel de la population française" à la même date et l'ensemble du territoire fin 2016. La filiale télécoms du groupe de construction a calculé qu'il lui faudrait équiper environ un tiers des antennes de son réseau mobile, soit 5 à 8000 points hauts. Comme Orange, il densifiera à la demande lorsqu'il décrochera de gros contrats pour assurer une qualité de service optimale.

Qowisio prévoit d'installer le même nombre d'antennes que Sigfox, environ 1 500, et ouvrira son réseau début 2016. Il a signé un partenariat avec TDF, qui possède des pylônes radio partout en France.

Mais cette bataille de chiffres n'a pas grand sens : la qualité de couverture dépend de nombreux paramètres, comme la topographie et le nombre d'obstacles radio, la position géographique de l'objet récepteur et la qualité de sa fabrication, par exemple.

D'ailleurs les acteurs du marché se titillent sur la question de la connectivité indoor et même "deep indoor", Bouygues se proclamant champion de la couverture des endroits les plus inaccessibles. En réalité, aucun réseau n'a de sérieuse lacune sur ce point. LoRa comme Qowisio peuvent améliorer la couverture à l'intérieur des bâtiments et en sous-sol en ajoutant des amplificateurs de réseau (des Femtocell et des picogateways, qu'Archos veut d'ailleurs déployer en masse pour créer son propre réseau). Sigfox, de son côté, prétend avoir le meilleur bilan de liaison et ne pas avoir besoin d'artifices techniques pour briller dans ce domaine. "*On a beaucoup de clients indoor et sous terre et cela fonctionne très bien*, assure son responsable marketing. *Notre technologie peut, beaucoup mieux que d'autres, pénétrer les obstacles radio*".

Quant à la connectivité à l'étranger, Sigfox semble avoir une longueur d'avance. Quatre pays sont entièrement couverts début décembre 2015 et huit autres sont en cours de déploiement. La start-up annonce en moyenne un nouveau pays chaque mois... Ses clients n'ont qu'un seul contrat à souscrire pour connecter leurs objets dans toutes les zones où le réseau est disponible.

Bouygues et Orange devraient sur le papier signer des accords avec des opérateurs à l'étranger pour proposer la même chose. Mais les modalités et les coûts de ce roaming ne sont pas encore connus. Bouygues déclare néanmoins que la continuité du service d'un pays à un autre sera assurée.

Quant à Qowisio, il est le seul à proposer une compatibilité bi-mode, avec son propre protocole et celui de LoRa. Lui aussi, comme Orange et Bouygues, devrait permettre du roaming avec d'autres opérateurs LoRa dans le monde.

Quid de la bi-directionnalité ?

Bouygues comme Orange n'ont que ce mot à la bouche : bi-directionnalité. Ce serait l'avantage principal de LoRa par rapport à Sigfox : le premier a été conçu dès le départ comme une solution de communication bi-directionnelle symétrique (en clair, un objet connecté par le réseau peut recevoir et envoyer de l'information) tandis que Sigfox n'est pas nativement bi-directionnel. La différence est-elle si nette ?

Oui, Sigfox n'a pas été conçu au départ comme une technologie bi-directionnelle. Mais depuis cette fonctionnalité a été ajoutée. Sigfox a privilégié l'économie d'énergie et non le volume de données, conformément à sa philosophie. Donc sa bi-directionnalité est par définition limitée. Très précisément, un objet sous Sigfox peut envoyer jusqu'à 140 messages par jour (de 12 octets maximum) et en recevoir 4 de 8 octets. Et pas question d'ouvrir les vannes du débit à l'avenir. "*Cela ne nous intéresse pas du tout*, tranche Thomas Nicholls. *Notre technologie est hyper optimisée pour une communication très faible, cela n'aurait pas de sens*".

Bouygues Télécom affirme faire la différence sur la quantité de données que son réseau permet d'échanger, sans sacrifier l'autonomie des équipements. Les messages envoyés par les

objets sous LoRa peuvent aller jusqu'à 243 octets, mais la moyenne tourne plus autour de 50 à 60 octets. Avec une limite : plus le message est lourd, plus le temps de transmission est long.

Bouygues insiste aussi sur la dimension de bi-directionnalité symétrique, et sur la capacité de LoRa à pouvoir "réveiller" un objet en mode repos à n'importe quel moment pour lui envoyer des informations, là où Sigfox doit composer avec des fenêtres de communication plus étroites.

Les concurrents de Bouygues et Orange remettent en cause cette capacité annoncée de bi-directionnalité symétrique. "*Promettre un cas d'usage basé sur une bi-directionnalité intensive, c'est envoyer son client dans le mur*, tranche sans ambages Cyrille le Floch, le président de Qowisio. *Annoncer cela, c'est un leurre, ce sera très difficile à faire en pratique*".

Il explique pourquoi. "*Sur les bandes de fréquence gratuites (868 mzh pour les réseaux bas débit longue portée, NDLR), il faut respecter un taux d'occupation de la bande, de 1 à 10% selon les canaux,* développe-t-il. *Il est impossible d'imaginer des communications très fréquentes, sinon votre émetteur violera les conditions d'utilisation de la bande. L'Arcep pourra être saisie et décider de pénalités, voire d'une extinction temporaire d'émetteur*", argumente-t-il. "*Offrir des débits bidirectionnels élevés demandera de déployer un réseau qui coûte extrêmement cher*", ajoute Thomas Nicholls (Sigfox). Un coût supplémentaire qui sera facturé au client d'une façon ou d'une autre, avance-t-il.

Bouygues, comme ses concurrents, devra se conformer à cette règle de taux d'occupation de la bande, 1% du temps en général (soit 36 secondes maximum par heure) pour la fréquence 868mhz. Mais il s'y pliera sans problème, assure-t-il. "*On utilise plusieurs fréquences, certaines dédiées à la réception, d'autres à l'émission*", explique Franck Moine, le Monsieur LoRa au sein de l'opérateur. Pour la communication de l'antenne à l'objet, c'est la fréquence 169 mhz qui sera privilégiée. Celle-ci peut être utilisée 10% du temps, et non 1%, et avec davantage de puissance (27 dbm, soit 500 mW contre 14dbm). "*Cette fréquence nous permettra d'émettre davantage et de manière plus puissante dans ce sens*", précise Franck Moine.

Quelle précision pour la géolocalisation ?

Bouygues Télécom l'annonce haut et fort : son réseau pourra être utilisé pour géolocaliser des objets, "*avec une précision de 10 à 50 mètres*", affirme Franck Moine. La méthode de la triangulation sera utilisée. Cette promesse pourra donc être pleinement tenue lorsque le réseau de l'opérateur sera dense, au mieux fin 2016. Avant cela, Bouygues se dit néanmoins capable de proposer de la géolocalisation précise en jouant sur l'étalement de spectre : en augmentant la portée des antennes, les objets pourront être identifiés par davantage de relais, ce qui facilitera la triangulation et donc la localisation. Bouygues risque de faire facturer ce service en option plus cher que l'offre de base (son positionnement tarifaire n'est pas encore connu).

Sigfox est plus modeste : il propose d'ores et déjà une offre de géolocalisation par triangulation, mais "à grosses mailles". "*C'est utile pour des services où l'on a juste besoin de savoir si une palette ou un conteneur est arrivé dans telle ville ou tel centre de tri. La précision est de l'ordre de quelques kilomètres*", annonce Thomas Nicholls. Imaginer un service de géolocalisation précis comme le prétendent Orange et Bouygues, "*c'est tout simplement ridicule*", tacle-t-il. "*Le prix augmenterait de façon radicale*". Orange a laissé entendre qu'un tel service pourrait coûter 5 à 10 fois plus cher que le service de base, car il faudrait densifier le réseau de façon importante.

Cyrille le Floch, de Qowisio, ne croit pas non plus à la triangulation pour une géolocalisation précise. "*Si on annonce que la triangulation LoRa va remplacer le GPS, cela risque de générer de la frustration, car il va falloir attendre 2 ou 3 ans que les réseaux déployés soient matures,* juge-t-il. *Il vaut mieux travailler avec les constructeurs de GPS pour améliorer la technologie*". Qowisio propose une offre de macrogéolocalisation, comme Sigfox.

Dans l'écosystème Sigfox, on trouve des fabricants d'objets comme Ticatag et Hidnseek qui combinent UNB et GPS. Mais attention, le GPS étant pour l'instant extrêmement énergivore, ce type d'objet peut voir son autonomie chuter drastiquement en cas d'utilisation fréquente, loin des 5 à 10 ans espérés lorsque l'on utilise Sigfox. Pour le tracker GPS Hidnseek promet une durée d'utilisation de 9 mois avec une localisation par jour... et seulement 3 jours pour un rafraichissement toutes les 5 minutes ! Pour Tifiz de Ticatag, c'est 1 an d'autonomie pour "quelques positions par jour". Beaucoup mieux que le GPS, certes, mais loin de la décennie de batterie rêvée.
Ces cas illustrent bien le point d'équilibre à trouver lorsqu'on fait appel à un réseau bas débit longue distance : toute utilisation intensive (pour la géolocalisation ou une communication bi-directionnelle intensive) fait grimper les coûts et chuter l'autonomie des objets... ce qui fait perdre à ce type de connectivité son avantage compétitif par rapport à d'autres solutions.

Friture sur la ligne ?

Chaque opérateur accuse la solution concurrente d'être plus sensible que la sienne aux brouillages. Difficile de démêler le vrai du faux dans cette salade de fréquences. Il est vrai que les fréquences ISM (la bande industrielle, scientifique et médicale) sont utilisées pour de multiples usages et font craindre des perturbations pouvant aller jusqu'à des coupures de messages, en particulier dans les zones urbaines.

Chaque opérateur se dit le mieux armé pour s'en prémunir. Sigfox assure n'avoir aucun souci d'interférences, grâce au choix de la technologie de bande étroite, dans laquelle on peut loger énormément de messages, et quasi impossible à saturer ou brouiller. Bouygues; par la voix de Franck Moine, affirme pourtant que Sigfox est "*intrinsèquement plus sensible au brouillage*". Thomas Nicholls réplique en affirmant que les messages à spectre étalé "*risquent de se faire couper par tous les autres communications*".

Chaque opérateur s'est prémuni contre ce risque d'interférences. Bouygues a développé son propre système qui communique aux objets situés autour d'une une antenne les canaux de

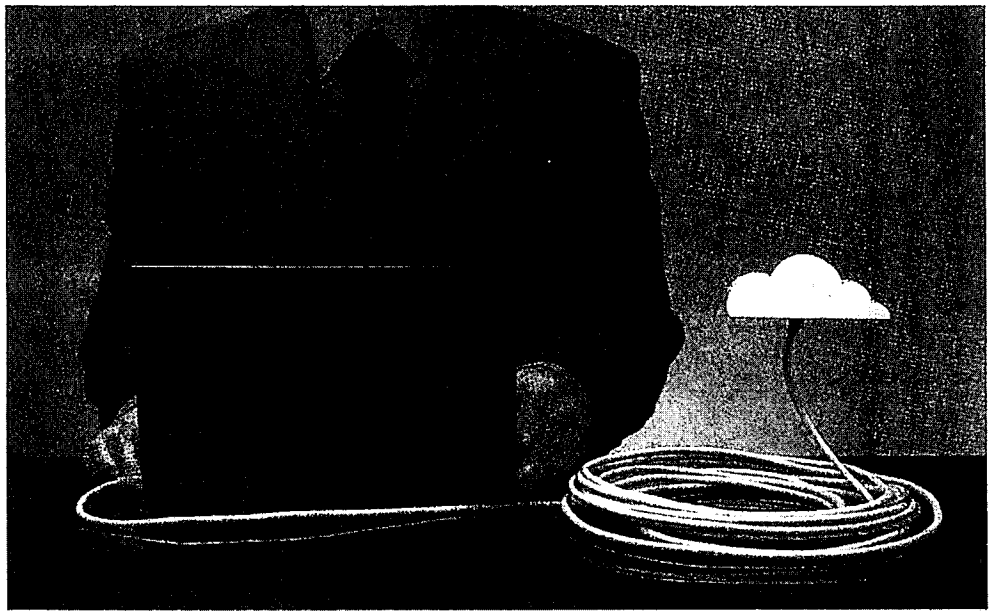
communication les plus propres. C'est notamment à cela que sert la fameuse bi-directionnalité annoncée. Le spécialiste de la sécurité incendie Finsecur dit avoir choisir LoRa en raison de sa robustesse.
Sigfox a lui aussi ses techniques (comme la répétition de messages) pour assurer une qualité de service optimale, quelle que soit la zone. Et lui aussi a été choisi par un spécialiste de la sécurité, Securitas Direct, en Espagne.

Combien ça va couter ?

Pour Cyrille le Floch de Qowisio, les arguments techniques avancés par certains opérateurs pour tenter de se différencier brouillent la perception du public et des futurs clients. Il faut revenir à un débat sur le business et les besoins métiers que peuvent combler les différents réseaux. *"Nos clients ne sont pas des électroniciens experts en radio, LoRa, Qowisio ou Sigfox ils s'en moquent, ce qu'ils veulent c'est qu'on leur assure une connectivité sur une zone donnée. Il n'y a pas une technologie qui est bonne et les autres mauvaises, surtout qu'on utilise des concepts radio connus depuis 50 ans. Personne n'a découvert le Graal. Essayer de se différencier sur la technologie, ce n'est pas pertinent et ça brouille le message. Cela crée un doute en leur faisant croire qu'ils doivent faire un pari sur la technologie ; leur vrai pari doit porter sur leurs futurs marchés".*

Sigfox annonce un tarif de 8 euros à 70 centimes d'euros par objet et par an (dégressif en fonction du volume d'objets à connecter). Il faudra attendre que Bouygues, Orange et Qowisio lèvent le voile sur leurs offres commerciales et leur approche business pour ouvrir un véritable débat sur leurs différences. Rendez-vous en janvier 2016.

Villes intelligentes
Cinq zones de sécurité à surveiller par les DSI



Grâce aux données des capteurs installés sur les routes et les véhicules, les systèmes de navigation embarqués dans les voitures peuvent signaler les embouteillages, les caméras repèrent les déchets dans les lieux publics et demandent l'intervention d'équipes de nettoyage ; les lampadaires de rue s'autorèglent... Voilà quelques-uns des scénarios qui pourraient se généraliser avec le développement des villes intelligentes, des villes qui sont sur le point de connaître une croissance exponentielle. Glasgow, Barcelone, Nice, New York, Londres et Singapour sont déjà engagées dans cette voie. D'après Navigant Research, le marché des technologies des villes intelligentes pourrait représenter 27,5 Mds de dollars annuels en 2023.

Souvent portées par le secteur public, les initiatives de villes intelligentes vont cependant avoir un fort impact sur les entreprises. Les DSI devront apprendre à exploiter les nouvelles infrastructures connectées de leur ville pour leurs activités. Les technologies des villes intelligentes, telles que l'IoT et les analyses des données vont sans doute donner lieu à des idées commerciales innovantes dans le futur. Mais ces technologies vont aussi créer de nouvelles vulnérabilités en matière de sécurité. Voici les CINQ zones à surveiller par les DSI.

Christophe Auberger

Directeur Technique France chez Fortinet

1. Davantage de fragmentation de l'IT.

Ces dernières années, les appareils mobiles et les services cloud ont proliféré au travail. Les DSI doivent désormais se faire à l'idée que les employés peuvent utiliser des services cloud non autorisés, via des téléphones non sécurisés, pour accéder aux données de l'entreprise. L'explosion attendue des appareils IoT — on parle de 40 milliards en 2020 dans le monde — entraînera davantage de fragmentation de l'IT dans l'entreprise. Pour protéger les données, les DSI doivent rechercher des appareils IoT capables d'offrir un chiffrement d'appareil à appareil et envisager la mise en place des systèmes de chiffrement complets afin de protéger les données stockées dans les réseaux, services cloud et terminaux.

2. Vulnérabilités des appareils

L'année dernière, des chercheurs ont trouvé des failles de sécurité dans les poupées Barbie connectées en Wi-Fi, les voitures Jeep Cherokee, les trackers d'activité et autres appareils connectés... Des failles exploitées par des attaques ciblant les appareils IoT à travers le monde. Les pirates vont utiliser les appareils IoT grand public comme tremplin pour des attaques de grande ampleur sur les réseaux des entreprises et les matériels auxquels ils se connectent (smartphones). Les DSI peuvent envisager de déployer des systèmes de protection réseau, comme les pare-feux de segmentation interne (ISFW), pour limiter les menaces à l'intérieur du réseau de l'entreprise. Ils devront également limiter la surface d'attaque IoT avec des solutions de sécurité réseau spécifiques. Les fournisseurs d'IoT doivent renforcer leurs produits et avoir une équipe d'intervention en cas d'incidents de sécurité des produits (PSIRT).

3. Les passerelles IoT peuvent être exploitées

Dans un déploiement IoT typique, la majorité des appareils sont et seront connectés en permanence. Contrairement aux téléphones mobiles, ces appareils bénéficient d'une authentification unique pour de multiples sessions. Cela les rend très attractifs aux yeux des pirates souhaitant s'infiltrer dans les réseaux d'entreprise. Le renforcement de la sécurité des passerelles qui connectent les appareils IoT est donc indispensable. Les DSI doivent cartographier la localisation et les liaisons de ces passerelles, internes ou externes, et établir un solide plan de mises à jour avec des correctifs de sécurité sur ces passerelles comme sur les appareils IoT.

4. Big data, plus de risques.

Les villes intelligentes et les dispositifs connectés vont générer d'énormes quantités de données qu'il faudra traiter et stocker. Autant de cibles attractives pour les pirates. Le Big Data amplifiera le phénomène, puisque les données devront pouvoir être accessibles à différents groupes de personnes. Il faudra donc renforcer les droits d'accès et les audits individuels.

5. Nouvelle boîte de Pandore.

De nouveaux vers, conçus pour les appareils IoT vont émerger et se propager d'appareil en appareil — notamment sur les appareils mobiles Android - en exploitant les vulnérabilités d'une surface d'attaque mobile et IoT croissante. La gestion des correctifs et les inspections de sécurité basées sur les réseaux — notamment, les systèmes de prévention d'intrusion (IPS) — capables de bloquer les vers sur IoT seront incontournables. ●

« Les villes intelligentes et les dispositifs connectés vont générer d'énormes quantités de données qu'il faudra traiter et stocker. Autant de cibles attractives pour les pirates. »

DOCUMENT 4

Peut-on penser la sécurité des objets connectés dès leur conception ?

Avenir de l'IT : *La récente découverte d'un botnet s'appuyant sur plus de 25 000 caméras de surveillance IP remet en lumière les risques informatiques liés à la généralisation des objets connectés. Peut-on les prendre en compte dès la conception de ces objets ?*

ZDNet

Par Stéphanie Chaptal | Lundi 04 Juillet 2016

Pour comprendre les risques de sécurité del'IoT.

Lorsque l'entreprise de sécurité américaine Sucuri a dévoilé fin juin l'existence d'un botnet regroupant plus de 25 000 caméras de surveillance IP, cette affaire a aussi remis sur le devant de la scène les risques informatiques posés par l'Internet des Objets et les nouveaux objets connectés. À tel point que pour Arnaud Cassagne, directeur du développement de l'intégrateur Cheapset, « La security by design (NDLR : ou prise en compte de la sécurité informatique dès la conception de l'objet) et les objets connectés sont antinomiques, parce que sur la partie objets connectés nous sommes dans une véritable course en avant, et où il faut sortir très très vite le nouveau produit.

Donc les start-ups vont prendre des systèmes et des logiciels open source déjà connus qui peuvent être faillibles, et dont la gestion de la mise à jour n'est pas hypersimple une fois que l'objet est en place. On se trouve avec des objets toujours connectés, qui sont toujours en fonctionnement et pas mis à jour, donc toujours vulnérables. On utilise des solutions très bien et peu onéreuses, mais qui demande de bonnes pratiques. »

Security by design, loin d'être une habitude pour tous

Or, hormis dans des domaines déjà sensibilisés à la sécurité, comme les fabricants de semiconducteurs et de cartes à puce travaillant pour le gouvernement, l'armée et le monde bancaire, les nouveaux entrants n'ont

pas la culture propre au security by design. Les acteurs classiques estiment eux qu'ils font du security by design depuis toujours. Ils constatent, en revanche, dans les domaines de l'IOT et du M2M (NDLR : Machine to machine – comme des caméras IP ou les compteurs Linky), les modèles d'attaques sont différents du modèle bancaire par exemple où tout est fermé et quasiment sous contrôle. Pour chaque objet connecté et pour chaque cas d'usage le concernant, il y a un modèle d'attaque à définir et des vulnérabilités à découvrir.

Ce modèle de travail existe depuis toujours dans les sociétés qui font de la sécurité. Mais il est loin d'être la norme. Comme nous le confie un ingénieur, « pour avoir fait des animations à la Cantine ou autres, la sécurité est le dernier des problèmes des start-uppers sauf ceux qui font vraiment un business de sécurité. Dans l'IOT on est plutôt sur des problématiques de connectivité, de protocole correct, de responsiveness, et pas forcément sur les problématiques de sécurité. »

Des prestataires pour contourner les difficultés internes

Comment pallier cette faiblesse ? Pour certains fournisseurs il faut placer le curseur de sécurité ailleurs. Ainsi pour Christophe Jolly, directeur de l'offre sécurité pour Cisco France, elle se situe avant tout au niveau du réseau. « Le security by design peut avoir plusieurs sens : sécurité par rapport à l'objet, mais aussi par l'infrastructure. Pour qu'on soit sur les 50 milliards d'objets à horizon 2020 et 300 milliards d'objets à horizon 2030 à un standard de sécurité pour les objets connectés ce n'est pas demain la veille. Or tous ces objets-là parlent l'IP, et laissent une trace. Le réseau peut s'utiliser comme un capteur pour identifier les objets (modèles, marques, identifiants utilisés et alimenter un référentiel de l'objet), donc détecter si tel objet de telle marque a telle vulnérabilité en croisant avec l'état de la sécurité et il peut agir un filtre pour empêcher un objet qui ne montre pas patte blanche ou qui n'est pas sur de se connecter sur le réseau de l'entreprise. D'autant qu'il suffit d'un maillon faible pour corrompre les autres objets à côté. »

Tanguy de Coatpont, directeur général Kaspersky France, propose d'accompagner les développeurs : « Une fois que la société a développé son produit, nous cherchons pour eux tous les problèmes de sécurité qui peuvent se poser grâce à trois méthodes : "test de la boite noire", simuler une attaque externe pour savoir s'il est accessible, quelles sont les informations recueillies et les conséquences, "test de la boite grise" où les attaques simulées proviennent d'utilisateurs légitimes qui présentent différents profils, "test de la boite blanche" plus complet où on audite le code source de l'objet. Ce process peut être fait aussi au cours du développement de la solution ». Or « développer un produit communicant sécurisé coute de 10 à 15 % à minimum plus cher qu'un même produit non sécurisé ».

Tanguy de Coatpont reconnaît que les clients de cette offre sont déjà sensibilisés à la sécurité. « Nos clients sont principalement tout ce qui

tourne autour de la finance, et nous commençons à travailler avec les différents acteurs du monde automobile pour les aider à sécuriser leur cloud et les capteurs intégrés. Mais la route est encore longue. La culture cybersécurité dans la domotique et les start-ups, n'est pas encore acquise. Le principal problème est une compréhension des risques et le coût financier. Ce n'est pas à ça que pensent les start-ups qui se lancent dans ce genre de projet. »

Vers l'établissement de standards ?

Mettant en cause des temps de développements de plus en plus courts, Arnaud Chassagne plaide lui pour un encadrement du security by design : « Vu aujourd'hui comme les cycles de développement des applications se réduisent à peau de chagrin, on va tellement vite qu'on ne peut pas penser à tout, or la sécurité nécessite un certain recul et de la réflexion. Le security by design c'est très joli, mais il n'y a pas de norme et de règles de bonnes pratiques derrière. Il faut arriver à faire travailler des développeurs pour faire du code propre et pas seulement pratique et rapide, avec une belle interface. »

C'est notamment le rôle du W3C. « À travers "Web of Things", le W3C tente de réfléchir à la définition d'un format commun pour échanger des données entre les éléments composant le réseau des choses. La sécurité est prise en compte, mais il reste pas mal de chemin à parcourir. Ainsi, la sensor API qui permet de récupérer les données des capteurs, avait été conçue sans ajouter l'envoi des données chiffrées. Depuis la question a été ouverte et sera résolue dans un développement futur », explique Virginie Galindo, Chair du Groupe W3C Web Cryptography Working Group. « Le W3C travaille particulièrement l'écosystème de l'automobile. Ici encore la sécurité reste au menu, bien que peu de contributions en ce sens soient intégrées. Néanmoins le W3c a mis en place une étape obligatoire de revue de sécurité et de privacy, et ces spécifications devront faire leurs preuves sur ces aspects-là, avant d'être définitivement acceptées par le W3C comme des recommandations. »

(...)

DOCUMENT 5

Extraits de « Sécurité des objets connectés »

Sommaire

EXECUTIVE SUMMARY

PRÉAMBULE

INTRODUCTION
- DOMAINES D'APPLICATION DE L'INTERNET DES OBJETS CONNECTÉS
- PANORAMA : RECHERCHE D'UNE DÉFINITION. DE L'INTERNET DES OBJETS CONNECTÉS
- VERS L'ÉCLOSION DU MARCHE DE L'INTERNET DES OBJETS CONNECTÉS ?
- LA NÉCESSAIRE PRISE EN COMPTE DES RISQUES DE L'INTERNET DES OBJETS CONNECTÉS

LES STANDARDS TECHNIQUES
- INTRODUCTION
- LES STANDARDS DE L'ITU-T (*International telecom union-telecommunication standardization*)
- L'INITIATIVE IEEE ET IETF
- L'INITIATIVE GS1
- L'INITIATIVE OASIS

ENJEUX JURIDIQUES ET ÉTHIQUES
- INTERNET DES OBJETS CONNECTÉS ET GOUVERNANCE
- OBJETS CONNECTÉS ET PROTECTION DES DROITS DE LA PERSONNALITÉ
- INTERNET DES OBJETS CONNECTES FACE AUX DROITS DE LA PERSONNALITÉ
- QUELLE RESPONSABILITÉ POUR LES OBJETS INTELLIGENTS ?
- LA PRATIQUE JURIDIQUE FACE AUX OBJETS CONNECTES

SÉCURITÉ TECHNIQUE ET OPÉRATIONNELLE
- INTRODUCTION
- CHANGEMENT DE CONTEXTE
- PRÉCONISATIONS POUR LA SÉCURITÉ DES PROJETS AVEC DES OBJETS CONNECTÉS

LA PROBLÉMATIQUE DES USAGES
- UTILISATION D'UN SI ET USAGE D'UN OBJET CONNECTÉ
- AMÉNAGEMENTS DE LA GOUVERNANCE DES SYSTÈME D'INFORMATION POUR LES OBJETS CONNECTÉS
- ÉVOLUTION DES REPRÉSENTATIONS COLLECTIVES DE LA FONCTION SI

ANNEXES
- RÉFÉRENCES
- ACRONYMES

© INHESJ - Décembre 2014 - Sécurité des objets connectés

EXECUTIVE SUMMARY

Pour aborder l'« Internet of Things », on peut retenir d'une revue de littérature française quatre formules: Internet des Objets, Objets Connectés, Systèmes d'Information Connectés aux Objets et Services Délivrés *via* des Objets Connectés.

La lecture de cette liste montre que l'« *Internet of Things* » est un domaine encore flottant et qu'il serait aventureux d'arrêter un discours définitif, notamment en matière de sécurité. Néanmoins, en vue de progresser vers ce discours, cette liste de quatre formules peut suggérer aux entreprises quatre points de vue, qui sont respectivement de nature juridique, technique, opérationnelle et commerciale.

Le premier point de vue, qui régit les autres, est le point de vue juridique. L'usage des objets connectés révèle des risques importants notamment en termes de protection de la vie privée et de responsabilité pour les utilisateurs et fabricants. Pour ces derniers, le corpus juridique révèle un ensemble d'obligations que les entreprises doivent respecter notamment dans les domaines des standards et normes applicables aux ondes. La conjonction de ces éléments oblige les acteurs à agir en amont tant au niveau d'une pratique indispensable de la RSE, mais aussi sur le plan de la conception des objets connectés ou une approche de « *Privacy by design* » est largement encouragée.

Le point de vue technique ouvre le champ des potentiels. Dans le fil de l'héritage de l'Internet, la technique se focalise sur les normes d'interopérabilité. Ces normes avancent une architecture globale d'un système avec des objets connectés, des protocoles de réseau utilisés par les objets, un adressage des objets et des mécanismes de messagerie entre les objets. La sécurité est d'emblée traitée dans chaque norme.

Le point de vue opérationnel trace le faisable. Pour les grandes entreprises, l'introduction des objets connectés et leur connexion au système d'information introduit des changements majeurs : nature et volume des données, périmètre du réseau d'entreprise, localisation des accès et des utilisateurs, impacts matériels voire physiques sur les personnes, empilement de technologies anciennes et nouvelles... Ces changements de contexte exigent une adaptation de l'approche sécurité au niveau des projets, en adaptant et renforçant les outils et méthodes existantes et en élargissant la gouvernance. Les entreprises devront aussi anticiper les modifications des opérations internes liées à l'introduction des objets connectés et visant à assurer la confidentialité, la disponibilité et l'intégrité du système d'information, et gérer de manière sécurisée son ouverture.

Enfin, le point de vue commercial adresse le réel *via* l'usage. L'entreprise doit s'attendre à des usages imprévus, détournés, parfois inconséquents, voire malveillants ou illicites. Par ailleurs, du fait de l'embarquement de capteurs et d'actionneurs, l'usage d'un objet connecté fait naître des risques sur les personnes, les biens et l'environnement. La gouvernance des systèmes d'information connectés au objets pourra être aménagée en instituant un Responsable des usages aux cotés du Chef de projet Maîtrise d'ouvrage et du Chef de projet Maîtrise d'œuvre, une phase d'expérience client en situation réelle, un travail spécifique de définition des conditions d'utilisation et le financement de fonctionnalités propres à assurer un usage conforme. On peut s'attendre à une évolution des représentations collectives de la fonction système d'information.

PRÉAMBULE

Miser sur la diversité des compétences pour répondre à des menaces protéiformes.

La sécurité numérique doit se concevoir sur le modèle des multiples formes d'agressions rendues possibles par les technologies de l'information et de la communication qui irriguent désormais les organisations économiques, administratives ou militaires. C'est la raison pour laquelle la réflexion et la stratégie en matière de cybersécurité doivent se concevoir en mettant à contribution une grande variété de compétences et d'expertises : dans les domaines industriels, techniques, informatiques, juridiques, judiciaires, militaires, policiers et même politiques.

De ce croisement de savoir-faire émergeront les stratégies utiles à mettre en place pour concevoir une sécurité numérique plus performante. C'est dans cet esprit que chaque année les auditeurs du cycle « Sécurité numérique » de l'Institut national des hautes études de la sécurité et de la justice (INHESJ) travaillent à analyser et éclairer une problématique qui se trouve au cœur des intérêts stratégiques des entreprises, et donc des États. Ils ont pour mission d'expliquer les enjeux de la thématique qui leur a été confiée, d'en présenter les mécanismes et de formuler des réponses réalistes et concrètes pour réduire ou faire cesser l'exposition au risque qu'elle représente. Soit une démarche résolument tournée vers une amélioration continue de la notion de sécurité, au bénéfice du plus grand nombre.

Vous trouverez dans ce document le fruit de leurs réflexions après une année d'étude passée au sein de l'INHESJ à échanger entre pairs et à rencontrer les experts et les praticiens les plus expérimentés dans le domaine de la sécurité numérique. Ils aboutissent à chaque fois à des recommandations opérationnelles directement transposables dans la réalité des entreprises et des administrations.

Ce sont donc des contributions utiles à une meilleure sécurité numérique.

Éric DELBECQUE
Chef du Département
« Sécurité économique »

Nicolas ARPAGIAN
Directeur scientifique du cycle
« Sécurité des usages numériques »

INTRODUCTION

Il n'est pas un jour où un article, une étude, un rapport essaye d'analyser et de déterminer les contours de ce que serait « l'internet des objets connectés ». Force est de constater que la mise en œuvre des objets connectés au sein de notre environnement quotidien a dépassé le stade de la preuve de concept. Ainsi, Cisco prévoit que le nombre d'objets connectés à internet soit multiplié par dix en 8 ans conduisant à près de 250 milliards d'objet potentiellement connectés. [1]

Conscient ou inconscient l'émergence de ce nouveau marché met en exergue un mode nouveau d'appréhension de notre quotidien tant personnel que professionnel. La CNIL a récemment tenté d'extrapoler de nouvelles pratiques comportementales du fait de l'usage des objets connectés [2]. Mais les entreprises ne sont pas en reste tant les implications conduiront à muter les systèmes d'informations de ces dernières. Les objets connectés semblent aujourd'hui être perçus comme une chance d'un renouveau industriel Français et plus globalement européen. Ainsi, un des 34 plans de reconquête industrielle du ministère du Redressement productif y est consacré. L'ère de la généralisation s'ouvre avec des applications ciblées sur les entreprises, un produit, un groupe de produits ou bien une marque [3].

Il importe de constater que les pouvoirs publics prennent en compte une approche différenciée en termes d'émergence du marché de l'Internet des Objets [4].

- La Chine, conscient des enjeux de l'Internet des Objets a déjà mobilisé des moyens considérables. Porté par le plus haut niveau de l'État un plan permettant de faire de ce pays le pays de l'Internet des objets en (dès) 2015 va être mis en œuvre.
- Singapour a mis en place une politique globale de l'Internet des Objets associant autorité et secteur public créant des centres de ressources et développant des applications dans les domaines portuaires aéroportuaires, environnementaux, du transport, de la santé...
- Corée du Sud et Malaisie ont mis en œuvre des politiques sectorisées dans des secteurs jugés prioritaires : gestion de la ville, de l'eau, des transports, de la pollution ou encore des frontières.
- Pour les États-Unis, l'innovation est principalement portée par le secteur privé, tout en étant accompagné et suivi par un secteur public volontariste. Ainsi, la FCC à créé une direction des soins - *healthcare* - pour traiter le sujet de l'internet des Objets pour les soins à domicile et à l'hôpital.
- La Commission Européenne a quant à elle beaucoup communiqué pour réduire son activité, laissant place à des politiques nationales. Ainsi, le Royaume-Uni a défini et lancé une politique industrielle portant sur les applications de l'Internet des objets à travers une politique de coopération. L'Allemagne, quant à elle, se tourne principalement vers une politique favorisant le M2M.

(1) Dace Evans - L'internet des objets - Comment l'évolution actuelle d'Internet transforme-t-elle le monde - CISCO - Avril 2011.

(2) Cahiers IP n°2, Le corps, nouvel objet connecté : du *quantified self* à la M-Santé : les nouveaux territoires de la mise en données du Monde - De nouvelles pratiques individuelles - Ecosystème et jeux d'acteurs - Quels axes de régulation, Les voies à explorer - Juin 2014.

(3) Jean-Pierre DARDAYROL, Loïc Lentoi DE LA COCHETIERE, Claudine DUCHESNE (2013) : « Rapport Internet des objets et logistique "Vers des nets avec des objets" Situation internationale, perspectives des acteurs et débats », Conseil Général de l'économie de l'industrie, de l'énergie et des technologies.

(4) *Supra* « Vers des nets avec des objets. Situation internationale, perspectives des acteurs et débats », Conseil Général de l'économie de l'industrie, de l'énergie et des technologies.

Il apparaît dès lors que l'horizon de maturité de l'Internet des Objets est perçu en Asie à plus court terme qu'en Europe : 2015 pour la Chine, 2020/2022 pour L'Europe.

Domaines d'application de l'internet des objets connectés

Les impacts de l'Internet des Objets apparaissent déjà : l'internet est désormais doté de capacités sensorielles (température, pression, vibration luminosité, humidité, tension) ce qui nous permet d'anticiper plutôt que de simplement réagir. Mais l'avenir que promet l'Internet des Objets connectés semble plus profond, modifiant notre *habitus* et pouvant accroître ou résorber une fracture tant sociale que comportementale. Quel serait l'avenir de l'humanité face à la connexion de notre corps, de nos capacités sensorielles ou de notre fonction décisionnelle[5] ?

(5) *Supra* Cahiers IP n°2 pour une tentative d'approche.

En effet, les domaines impliqués par les objets connectés sont multiples. Ainsi, (1) le secteur hospitalier, de la santé, de la dépendance et du bien-être (2) la ville intelligente et la gestion des flux (eau, énergie avec les *Smart Grid*, véhicules, personnes) et (3) le secteur du commerce et du marketing, sont aujourd'hui ceux qui connaissent déjà la mise en œuvre des objets connectés.[6] Mais force est de constater que nous pouvons raisonnablement avancer que tout objet existant, fixe ou mobile, est susceptible d'être connecté, mais il faut également s'attendre à l'émergence d'objets inédits munis d'applications innovantes dans tous les compartiments de l'activité humaine. Les exemples de la domotique et de la robotique sont aujourd'hui frappant tant les investissements dans ces domaine se multiplient.

(6) *Supra* « Vers des nets avec des objets. Situation internationale, perspectives des acteurs et débats », Conseil Général de l'économie de l'industrie, de l'énergie et des technologies.

Ainsi, le Conseil Général de l'économie de l'industrie, de l'énergie et des technologies a-t-il pu référencer les perspectives suivantes dans le cadre du développement du Machine à Machine (M2M) : traçabilité des bouteilles de vin ou des paquets de cigarettes, la géo-localisation et la mesure de l'environnement et du contenu des containers frigorifiques, la configuration des composantes d'un aéronef ou encore l'authentification des pièces de monnaie...

Panorama : recherche d'une définition de l'internet des objets connectés

Alors que 81 % des Français ont déjà entendu parler d'objets connectés[7], la définition de la notion demeure complexe. Générique par nature, le terme « Internet des objets connectés » ne connaît pas de définition clairement admise.

(7) Sondage CSA pour Havas Média Janvier 2014 - Étude: Internet des Objets - les Chiffres clefs.

Sa première occurrence est retrouvée en 1999 au sein des travaux du groupe Auto-ID du MIT travaillant sur l'identification de la fréquence radio (RFID) en réseau et sur les technologies de détection (*Ang: Radio Frequency Identification, RFID*). C'est lors d'une présentation pour *Procter & Gamble* que Kevin Ashton évoquait pour la première fois l'idée selon laquelle la RFID pourrait avoir un rôle majeur au sein de la chaîne d'approvisionnement de P&G[8] au travers d'objets connectés.

(8) Kevin Ashton, «That 'Internet of Things' Thing», *RFID Journal*, 22 June 2009.

Comme le souligne l'ensemble des écrits dans le domaine, le terme recouvre une très grande diversité de visions. Ainsi, certaines définitions utopistes laissent entendre que l'objet pourrait devenir un acteur actif, autonome au sein des réseaux :

> *« Objets connectés : Objets ayant des identités et des personnalités virtuelles, opérant dans des espaces intelligents et utilisant des interfaces intelligentes pour se connecter et communiquer au sein de contextes d'usages variés »*[9]

(9) Anonyme, 2008, Internet of Things in 2020, Roadmap for thr Future, 1.1 ed : 27 Infso D.4 Networked Entreprise & RFID ; Infso G.2 Micro & Nanosystems un co-opération with the working group RFID of the EPOSS. P.4

« Identité », « personnalité », « intelligence » ne peuvent permettre de déterminer un objet, bien meuble par essence. Il n'en demeure pas moins que la terminologie est en elle-même porteuse d'une appréhension de la réalité matérielle étudiée : à savoir un objet doté d'une capacité d'échange avec un ou plusieurs éléments de son environnement. Ainsi, le Conseil Général de l'Économie, de l'Industrie, de l'Énergie et des Technologies (CGEIET) préfère utiliser le terme « d'Internet avec des Objets »[10], formule qu'il place dans le sous-titre du rapport « Internet des objets et logistique ».

(10) Jean-Pierre DARDAYROL, Loïc Lentoi DE LA COCHETIERE, Claudine DUCHESNE (2013) : « Rapport Internet des objets et logistique "Vers des nets avec des objets" Situation internationale, perspectives des acteurs et débats » Conseil Général de l'économie de l'industrie, de l'énergie et des technologies.

Un tel choix se retrouve également dans la définition proposée par le rapport IDATE où l'Internet des Objets peut être regardé et défini comme des objets auxquels on greffe une connexion Internet, même s'il ne disposent pas des « composants électroniques requis pour une connexion directe (RFID ou autre technologie d'étiquette) ». À titre d'exemple, une telle analyse se retrouve dans le produit *Mother* et *Motion Cookies* de *Sen.se*

Ce choix, pour important qu'il soit, tend à démontrer une continuité entre les Internets que nous connaissons et cet avenir qu'est l'objet connecté où les théories de Mark Weiser sur l'*Ubiquitous computing* deviennent réalité. Cette filiation est source d'un débat agitant les acteurs de l'Internet des Objets. En effet, il est admis que le réseau Internet ne se prolonge pas dans le domaine physique. Or, comme le note le CGEIET :

> *« L'Internet des Objets dépasse ce prisme pour étendre Internet au monde réel en associant des étiquettes munies de codes, de puces RFID ou d'URL aux objets et/ou aux lieux ».*

Il demeure, comme le souligne le CGEIET que :

> *« Les experts et les utilisateurs, notamment au sein des entreprises, envisagent, non pas un Internet prolongé au monde physique, vivant*

ou géographique, mais plutôt des applications et des systèmes s'intéressant aux objets en utilisant les technologies de l'Internet».

Cette même vision est celle défendue par la définition donnée par l'Union Internationale des Télécommunications (UIT) :

« L'Internet des objets représente une extension de l'Internet tel que nous le connaissons aujourd'hui en créant un réseau omniprésent et auto-organisé d'objets physiques connectés, identifiables et adressables permettant le développement d'applications au sein de secteurs verticaux clés et entre ces secteurs par le biais des puces intégrées ».

Ainsi, le caractère « d'extension de l'Internet » apparaît au travers du système de nommage Internet « traduisant une convergence des identifiants numériques (...) Ainsi, le réseau s'étend jusqu'à l'objet et permet de créer une forme de passerelle entre les mondes physique et virtuel. »[11]

(11) BENGHOZI Pierre-Jean, BUREAU Sylvain, MASSIT-FOLLÉA Françoise (2008): « L'Internet des objets. Quels enjeux pour les Européens ? », ministère de la Recherche, Délégation aux usages de l'Internet, Paris.

Pour mesurer l'importance et les moyens d'émergence de l'Internet des objets, il faut comprendre la différence fondamentale entre l'Internet et le *World Wide Web*.

- L'Internet est la couche physique, c'est à dire le réseau composé de commutateurs, de routeurs et d'autres équipements. Sa fonction est de transporter les informations d'un point A à un Point B de façon rapide, fiable et sécurisée.
- Le Web, lui, est la couche applicative qui intervient sur Internet. Son rôle est de fournir une interface permettant d'exploiter les informations circulant sur l'Internet.[12]

(12) Dace Evans - L'internet des objets - Comment l'évolution actuelle d'Internet transforme-t-elle le monde - CISCO - Avril 2011.

Pour rappel, le journal officiel en date du 16 mars 1999 donnait pour définition suivante du terme « Internet » :

« Réseau mondial associant des ressources de télécommunication et des ordinateurs serveurs et clients, destiné à l'échange de messages électroniques, d'informations multimédias et de fichiers. Il fonctionne en utilisant un protocole commun qui permet l'acheminement de proche en proche de messages découpés en paquets indépendants. »

Or, cette filiation doit être tempérée par le fait que l'Internet des Objets n'est pas qu'un simple prolongement des Internets puisque reposant pour partie sur un nouveau système indépendant et une infrastructure propre (bien qu'intégrée pour partie sur celui des Internets). Cette précision apportée par la Commission Européenne[13] démontre certaines spécificités de l'Internet des Objets et la non pertinence de le voir comme une simple continuité de l'évolution que connaît le monde depuis l'apparition des réseaux Internets.

(13) Communication de la commission au parlement Européenne au conseil, au comité économique et social européenne et au comité des régions : « Internet des objets - Un plan d'action pour l'Europe » - 18 juin 2009.

Dès lors, donner une définition unitaire de « l'Internet des Objets connectés » ne saurait échapper à une détermination générique. La diversité que recouvre ce terme est certaine et se retrouve dans la multiplicité des expressions de cette évolution technique. Ainsi, des usages, des architectures techniques extrêmement diverses peuvent être soulignés permettant l'émergence d'Internets des Objets connectés pouvant viser des finalités multiples (M2M, objet à objet, humain à objet, etc.). C'est pourquoi, le cabinet Gartner propose aujourd'hui une définition générique sur son site :

> *« L'Internet des Objets est le réseau des objets physiques qui embarquent des technologies pour communiquer et interagir avec l'environnement externe selon leurs états internes.* (Ang : «The Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment» [14]). »

(14) Gartner - Glossary - http://www.gartner.com/it-glossary/internet-of-things.

Ainsi, tout objet existant, fixe ou mobile, est susceptible d'être connecté, mais également des objets nouveaux munis d'applications nouvelles mises en œuvre en relation étroite avec des nouveaux services dans l'ensemble de la vie tant des consommateurs que des entreprises. C'est donc un changement de paradigme qu'impose l'Internet des Objets et non une simple continuité des usages antérieurs: il s'agit bien de l'émergence progressive du Web 3.0. Ainsi, il n'est pas à douter que l'Internet des Objets est et sera une composante essentielle des « Systèmes d'information ou systèmes industriels » auxquels nous nous référons en partie dans le présent document.

Vers l'éclosion du marché de l'internet des objets connectés ? la nécessaire prise en compte des risques de l'internet des objets connectés

L'éclosion d'un nouveau marché nécessite son appréhension par l'ensemble du corps social: États, Consommateurs, Entreprises. Cette dernière nécessite par essence une prise en compte des risques de ce marché conduisant à s'interroger vis-à-vis de ceux auquels doit faire face l'Internet des Objets connectés.

Alors que 6% des Français affirment disposer d'un objet connecté du type balance connectée, montre connectée, tensiomètre connecté ou capteur d'activité[15] et que le nombre d'utilisateurs pourrait tripler d'ici trois ans pour atteindre 11 millions de Français[16], les risques inhérents aux objets connectés inquiètent. 78% des personnes interrogées se déclarent inquiètes en matière d'atteinte à la vie privée[17] et 12% perçoivent un « danger, en partant du postulat que les objets connectés ont la capacité de recueillir et d'analyser des informations personnelles et confidentielles »[18].

(15) Sondage IFOP pour Havas Media - Février 2014 - Observatoires des objets connectés.

(16) Atelier BNP Paris Décembre 2013 - (http://www.atelier.net/services/library/objets-connectes-centre-un-nouvel-ecosysteme-de-sante_425892)t.

(17) Sondage CSA pour Havas Média - Janvier 2014 - Étude : Internet des Objets - les Chiffres clefs.

(18) Sondage BVA pour Syntec Numérique - Févier 2014 - Baromètre de l'innovationue.

Cette appréhension est un frein certain à l'éclosion du marché de l'Internet des Objets. En effet, ce dernier doit faire face à de nombreux défis. Ainsi, des informations mal gérées pourraient révéler des données individuelles ou compromettre la confidentialité des données d'entreprises, une attribution inadéquate des droits et des devoirs des acteurs privés pourrait freiner l'innovation, une défaillance dans l'obligation de rentre des comptes pourrait

menacer le fonctionnement du système de l'Internet des Objets.[19] Peuvent aussi être soulignés les risques mis en exergue pour la Commission Européenne par RAND Europe[20] (identification de l'objet, protection et sécurité des données et de la vie privée, architectures, éthiques, normes, gouvernance).

Pour les entreprises l'enjeu est dichotomique. En tant que producteur d'objets connectés et en tant qu'utilisateurs de ces derniers, les entreprises devront faire face à une multiplicité de risques. Il apparaît que ce sont ces dernières qui deviendront récipiendaires des enjeux de l'Internet des Objets connectés :

- Comment l'identification de l'objet est-elle structurée ? Ce qui conduit à s'interroger sur la normalisation permettant de désigner de l'objet.
- Qui attribue l'identifiant renvoyant à la question de l'autorité chargée de l'attribution ?
- Comment et où des informations supplémentaires sur cet objet y compris sur son histoire peuvent-elle être retrouvées conduisant à s'interroger sur un mécanisme d'adressage et référentiel d'information ?
- Comme la sécurité des informations est-elle garantie ?
- Quelles parties concernées ont l'obligation de rendre des comptes pour chacune des questions ci -dessus et par quel mécanisme[21] ?

Ainsi, l'entreprise est au cœur de l'émergence de l'Internet des Objets connectés. Cette dernière ne pourra se faire sans une certaine cohésion des acteurs économiques. Mais les risques auxquels l'ensemble des acteurs doivent faire face sont multiples. Comment garantir l'intégrité, la disponibilité, la confidentialité et la traçabilité tant de l'objet que des données qui en sont issues ?

La sécurité des objets connectés apparaît dirimante à leur généralisation et est clairement prise en compte par les pouvoirs publics. Ainsi, l'appel à projet « Cœur de filière numérique – Logiciel embarqué et objets connectés » souligne l'importance de l'enjeu de la sécurité des objets connectés :

> *« La diffusion croissante de ces objets génère également de nouveaux risques pour la sécurité numérique des institutions, des entreprises et des particuliers, qui appellent de nouvelles réponses ».*

Il découle de la résolution de ces risques deux scénarios extrêmes :

- Un premier **scénario optimiste** où les objets sont connectés entre eux et dont les bénéfices touchent tous les domaines, la prise en compte des risques permettant de réduire ces derniers à un niveau raisonnable.
- Un second **scénario pessimiste** où les objets génèrent plus de complexité, moins de sécurité, moins de contrôle.

C'est dans une optique prospective que seront analysés dans le cadre du présent document (I) les Standards afférents à l'Internet des Objets, (II) les enjeux juridiques et éthiques issues de l'Internet des Objets puis (III) les moyens afférents à la sécurité technique et opérationnelle de l'Internet des Objets. Enfin, (IV), nous terminerons sur la problématique de l'usage de l'Objet Connecté, qui est différente de l'utilisation d'un système d'information.

(...)

(19) Communication de la Commission au Parlement européen, au Conseil, Comité économique et social européen et au Comité des régions - L'internet des objets : un plan d'action pour l'Europe /* COM/2009/0278 final .

(20) RAND Europe « Europe's policy options for a dynamic and trustworthy development of the Internt of Things SMART 2012/0053

(21) Supra Communication de la Commission /* COM/2009/0278 final */

ENJEUX JURIDIQUES ET ÉTHIQUES

Internet des Objets connectés et Gouvernance

Contexte de Gouvernance : vers la nécessaire prise en compte des Stakeholders

Alors que la gouvernance des systèmes techniques est une composante fondamentale à la gouvernance des sociétés modernes, la gouvernance de l'Internet est aujourd'hui remise en cause dans ses fondements. Écho de l'affaire Snowden, les échanges tendent à s'orienter vers le développement d'une vision multipolaire. Ainsi, dès mars 2014, la NTIA (*National Telecommunication & information Administration*»[23] a annoncé son attention de transférer les éléments relatifs à la gestion des noms de domaines dans le cadre d'une mise en avant des différentes parties prenantes.

Dans une étude réalisée pour la Commission Européenne par Rand Europe[24], il est précisé que la gouvernance de l'Internet des Objets, au même titre que la gouvernance de l'Internet implique une standardisation, une politique gouvernementale et un élément d'autoréglementation. Il en découle que la gouvernance ne saurait être regardée comme une composante parmi d'autres de l'Internet des Objets, mais comme une condition au bon développement de cet ensemble. La Gouvernance correspondrait dès lors à l'émergence de normes issues des Parties Prenantes (*stakeholders*) dans l'ensemble des domaines techniques, économiques, politiques et juridiques. Cette vision d'une gouvernance regroupant l'ensemble des Parties Prenantes est celle mise en avant par le Netmundial. Tenue les 23 et 24 avril 2014 à Sao Paulo, la « réunion multipartite mondiale sur l'avenir de la gouvernance de l'Internet » s'est fortement opposée au mode de gouvernance actuel et à souligné que :

> *"Internet governance should be built on democratic, multistakeholder processes, ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical community, the academic community and users. The respective roles and responsibilities of stakeholders should be interpreted in a flexible manner with reference to the issue under discussion."*

(23) http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

(24) RAND Europ « Europe's policy options for a dynamic and trustworthy development of the Internt of Things SMART 2012/0053

Cette déclaration comporte le vœu pieu d'une collaboration entre l'ensemble des stakeholders[25]. Ces échanges devant permettre l'élaboration d'une gouvernance « transparente, multilatérale et démocratique »[26]. Il demeure, comme le souligne l'appel à projet « Cœur de filière numérique – Logiciel embarqué et objets connectés[27] » qu'« un des besoins principaux [de l'Internet des objets] est la définition de standards transverses indépendants de couches matérielles et compatibles avec les ressources limitées, notamment en bande passante ». Dès lors, l'enjeu de la gouvernance apparaît bien comme essentiel pour faire émerger l'Internet des objets connectés au sein de différents territoires. En ce sens, l'Union européenne dispose de nombreux atouts au travers de ses instances et méthodes de convergences entre *stakeholders*.

(25) Pour plus de développements sur la notion : François Guy Trébulle, Odile Uzan, Responsabilité sociale des entreprises : Regards croisés Droit et Gestion, ed. Economica.

(26) Sommet mondial sur la société de l'information (SMSI) Genève 2003 - Tunis 2005 organisé par l'Union Internationale des Telecommunications (UIT).

(27) http://investissement-avenir.gouvernement.fr/sites/default/files/user/20130603%20AAP%20Logiciel%20embarqu%C3%A9%20et%20objets%20connect%C3%A9s.pdf

La Neutralité de l'Internet, consécration et menaces sur un fondement de l'Internet des Objets

La neutralité de l'internet[28] apparaît comme l'une des clefs de voûte du développement des objets connectés[29]. Ainsi, le Parlement européen a voté le 3 avril 2014 en faveur de la proposition de règlement du Parlement européen et du Conseil établissant des mesures relatives au marché unique européen des communications électroniques et visant à faire de l'Europe un continent connecté précisant qu'un service d'accès à internet est « *un service de communications électroniques accessible au public, qui fournit une connectivité à l'internet,* ***conformément au principe de neutralité de l'internet****, et, partant, une connectivité entre la quasi-totalité des points terminaux connectés à l'internet, quels que soient la technologie de réseau ou les équipements terminaux utilisés* » étant entendu que la neutralité de l'internet est « *le principe selon lequel l'ensemble du trafic internet est traité de façon égale, sans discrimination, limitation ni interférence, indépendamment de l'expéditeur, du destinataire, du type, du contenu, de l'appareil, du service ou de l'application* ».

(28) Le concept de « network neutralité » a été développé par Tim WE en 2003 dans « Network Netrality, Brodband Discriminiation, in Journal of Telecomunications and Hih Technology Law Val. 2 p.141, 2003 disponible à l'adresse suivante : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863

(29) BENGHOZI, Pierre-Jean ; BUREAU, Sylvain ; y MASSIT-FOLLÉA, Françoise. La nécessité d'une gouvernance adaptée In: L'Internet des objets: Quels enjeux pour l'Europe [en línea]. Paris: Éditions de la Maison des sciences de l'homme, 2009 (generado el 23 mayo 2014). Disponible en Internet: <http://books.openedition.org/editionsmsh/93>. ISBN: 9782735115877..

La position des 28 a rejoint la position du Comité des Ministres du Conseil de l'Europe relative à la neutralité du réseau, adoptée le 29 septembre 2010[30] complétée le 16 avril 2014 par l'adoption d'un Guide des droits de l'homme pour les utilisateurs d'Internet[31] précisant notamment :

> « *Dans vos relations avec les pouvoirs publics, les fournisseurs d'accès à internet, les fournisseurs de contenus et de services en ligne, ou avec d'autres utilisateurs ou groupes d'utilisateurs, vous ne devez subir aucune discrimination sous quelque motif que ce soit* ».

(30) Déclaration du Comité des Ministres sur la neutralité du réseau, adoptée le 29 septembre 2010(https://wcd.coe.int/ViewDoc.jsp?Ref=Decl(29.09.2010_2)&Language=lanFrench&Ver=original&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383).

(31) Recommandation CM/Rec(2014)6 du Comité des Ministres aux Etats membres sur un Guide des droits de l'homme pour les utilisateurs d'internet (adoptée par le Comité des Ministres le 16 avril 2014, lors de la 1197e réunion des Délégués des Ministres) https://wcd.coe.int/ViewDoc.jsp?id=2184819&Site=CM

Ainsi, le principe de non-discrimination et de neutralité des réseaux fait l'objet d'accords entre les 47 États membres du Conseil de l'Europe.

Les principes défendus par l'Union européenne font face aux propositions de la Federal Communications Commission (FCC) en date du 15 mai 2014 mettant en œuvre un « traitement préférentiel » entre les différents acteurs de l'internet[32]. Or, la formulation employée par la FCC semble correspondre aux limites accordées par le Conseil de l'Europe le 29 septembre 2010 :

(32) http://www.fcc.gov/document/fcc-launches-broad-rulemaking-protect-and-promote-open-internet

> *« Pour autant que cela s'avère nécessaire [...], la gestion du trafic ne doit pas être perçue comme contradictoire au principe de neutralité des réseaux. Cependant, toute exception à ce principe devrait être considérée avec beaucoup de circonspection et être justifiée par des raisons impératives d'intérêt public majeur. Dans ce contexte, les Etats membres devraient être attentifs aux dispositions prévues par l'article 10 de la Convention européenne des droits de l'homme et à la jurisprudence pertinente de la Cour européenne des droits de l'homme. »*

Dès lors, une nouvelle dichotomie apparaît entre les instances communautaires et celles des États-Unis sur cette question pourtant essentielle à l'évolution de l'Internet des objets.

Internet des Objets vers une balkanisation normative ?

Le monde des objets connectés et plus spécifiquement celui de la RFID, met œuvre un ensemble de normes déjà existantes comme nous l'avons précédemment démontré. Mais aucune norme n'est contraignante et obligatoire au niveau supra-étatique. Ainsi, chaque entreprise ou État est libre de développer et mettre en œuvre un standard qui lui est propre conduisant à une multiplication des systèmes et à d'importantes difficultés en termes d'interopérabilité.

À titre d'exemple, peut être souligné le développement du standard ONS (*Object Name System*) développé par EPCglobal pour les étiquettes RFID est calqué sur le DNS actuel avec la même arborescence centralisée et le même propriétaire privé (*l'américain VeriSign*). Dérivé de ce standard, GS1-EPCglobal et OBS ont créé une racine française de l'ONS. Comme le soulignait Madame Pecresse, *« L'étape suivante du développement de cette initiative correspondra à la mise en œuvre de technologies qui permettront l'interopérabilité avec la racine américaine ainsi qu'avec celles qui ne manqueront pas d'être crées dans le reste du monde »* [33] Une telle démarche conduit à mettre en exergue l'indépendance que procure la création d'une racine nationale et le caractère déterminant que prendront à l'avenir les règles relatives à l'interopérabilité.

(33) Discours de Madame Valérie Pecresse, ministre de l'Enseignement supérieur et de la Recherche le 3 décembre 2007.

À l'opposé des normes ci-dessus mentionnées la **gestion de fréquences** connaît tout à la fois un ensemble de règles globalisées au niveau européen et une gestion largement territorialisée dans leur mise en œuvre. Ainsi, concernant la gestion des spectres, l'Union européenne a harmonisé les pratiques en la matière au travers de la directive 2002/21/CE du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive « cadre »). Comme le précisent les considérants de ce texte :

> *« La convergence des secteurs des télécommunications, des médias et des technologies de l'information implique que tous les réseaux de transmission et de services associés soient soumis à un même cadre règlementaire. [...] Les radiofréquences constituent une donnée essentielle des services de communications électroniques fondés sur les fréquences radioélectriques ».*

Ainsi, au terme de la loi n°2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communications audio-visuelles, le législateur Français a mis en œuvre un cadre juridique applicable à l'ensemble des réseaux de communications électroniques. Une telle solution, aussi positive soit-elle sur le territoire national, souligne que la gestion des fréquences est fondée sur une base nationale conduisant à des spécificités étatiques. De telles spécificités ne permettent pas une standardisation des bandes utilisées par les objets connectés conduisant parfois à des impossibilités d'utiliser certains objets sur différentes zones géographiques.

Il apparaît donc difficile d'harmoniser les pratiques normatives différenciées au sein même de l'Union européenne. La gestion des spectres relevant pour partie de la défense, il semble difficile à l'Union de s'engager plus en amont dans le domaine. Il demeure, que la multiplicité des normes et des intérêts divergents dans leurs gestions conduisent à une mise en exergue des besoins d'interopérabilité.

Internet des Objet et Santé publique

Nous évoluons dans un environnement baigné par les radiofréquences. Il apparaît toutefois que la plupart des dispositifs relatifs à l'Internet des Objets utilisent des radiofréquences (*c'est-à-dire inférieures à 100 kHz*) et fonctionnent à une très faible puissance. Cette dernière semble peu susceptible d'engendrer des niveaux importants d'exposition aux champs électromagnétiques.

Fréquences	**Exemples d'application**
9 kHz – 87,5 MHz	Radiodiffusion, télédiffusion (bande I)
87,5 MHz – 108 MHz	Radiodiffusion FM
108 MHz – 880 MHz	Télédiffusion (bandes II à V), alarmes, télécommandes
880 MHz- 960 MHz	Téléphonie mobile GSM 900
1710 MHz-1880 MHz	Téléphonie mobile GSM 1800 (ou DCS)
1880 MHz-1900 MHz	Téléphonie sans fil domestique (norme DECT)
1920 MHz-2170 MHz	UMTS (standard téléphonie-internet) ou 3G
2400 MHz-2500 MHz	Wi-Fi, Bluetooth, four à micro-ondes

Ainsi, l'usage et la multiplication des sources d'émission d'ondes constituent un enjeu de santé publique pleinement appréhendé par les instances. Ces dernières ont mis en œuvre un corpus juridique permettant de : « *protéger le public dans la Communauté contre les effets nocifs avérés pour la santé qui peuvent survenir à la suite d'une exposition à des champs électromagnétiques*[34] » comme le précise la recommandation du conseil du 12 juillet 1999 relative à la limitation de l'exposition du public aux champs électromagnétiques (*de 0Hz à 300 GHz*). Outre ce texte, l'ensemble légal est aussi composé de la directive 2004/40/CE du Parlement et du Conseil européen pour la protection des travailleurs relative à l'exposition des travailleurs aux risques dus aux agents physiques et la directive 2006/95/CE du Parlement européen et du conseil du 12 décembre 2006 concernant le rapprochement des législations des États membres relatives au matériel électrique destiné à être employé dans certaines limites de tension. Il convient de souligner que ce cadre réglementaire est régulièrement mis à jour afin de prendre en compte l'ensemble des évolutions

(34) Considérant 4 : recommandation du conseil du 12 juillet 1999 relative à la limitation de l'exposition du public aux champs électromagnétiques (de 0Hz à 300 GHz).

technologiques et de garantir un niveau d'exigence sanitaire adéquat en matière de sécurité et de santé. Sur le terrain de la *soft-law*, peuvent-être cités les guides établis par l'ICNIRP (*International Committe for Non-Ionising Radiation Protection*).

Il demeure qu'à ce jour, les relevés effectués semblent indiquer un taux d'exposition bien inférieur aux seuils tolérés[35] mais il demeure difficile d'évaluer sur le long terme leur impact sur la santé publique.

(35) Dorothée Grange, Sabine Host, sous la direction d'Isabelle Grémy, Observatoire régional de santé d'Ile de France, Radiofréquences, santé et société 2009 http://www.radiofrequences.gouv.fr/IMG/pdf/ORS_IDF_Radiofrequences_sante_et_societe_decembre_2009.pdf

Émergence de l'Internet des objets et gestion des déchets

Ligne directrice de l'ensemble de la réglementation actuelle, la responsabilité de la gestion des déchets repose sur ceux qui les produisent. La directive dite « cadre »[36] prévoit la mise en œuvre d'une « hiérarchie des déchets » devant être mise en œuvre au sein des États membres. Il incombe à ces derniers d'introduire dans leur législation les moyens prévus permettant de :

- Prévenir la production de déchets
- Préparer les déchets en vue de leur réemploi
- Les recycler
- Les valoriser
- Les éliminer de manière sûre et dans des conditions respectueuses de l'environnement.

(36) Directive 2008/98/CE du Parlement européen et du Conseil du 19 novembre 2008 relative aux déchets et abrogeant certaines directives

Le développement de l'Internet des objets conduit à remettre en cause pour partie le cycle traditionnel de retraitement des biens. En effet, l'introduction au sein d'objets du quotidien de capteurs électroniques conduit à introduire ces objets dans le champ de la directive 2012/19/UE relative aux déchets d'équipements électriques et électroniques[37] (DEEE). De ce fait, les fabricants devront impérativement modifier le cycle habituel de retraitement des déchets et en supporter l'ensemble des coûts.

De plus, comme le souligne la Commission Européenne[38], le fait que les marqueurs soient fabriqués en métal, peut constituer d'importantes difficultés sur les chaînes de recyclage du verre, du plastique, de l'aluminium et du fer-blanc. Ainsi, elle conseille de mettre en œuvre un processus permettant d'identifier facilement les objets connectés afin de faire l'objet d'un retraitement différencié.

(37) Directive 2012/19/UE du parlement européen et du conseil du 4 juillet 2012 relative aux déchets d'équipements électriques et électroniques (DEEE).

(38) Communication de la Commission au Parlement Européenne au Conseil, au Comité économique et social européenne et au comité des régions : « Internet des objets - Un plan d'action pour l'Europe » - 18 juin 2009 : « Il n'est pas à douter que l'IdO modifiera notre conception de la vie privée ».

Conséquences

Force est de constater que les enjeux de gouvernance dépassent ceux que connaît l'internet traditionnel. Le fait que l'Internet des objets connectés prolonge le monde virtuel au sein du monde physique conduit à mettre en œuvre deux corpus juridiques parfois fondamentalement distincts. Ainsi, les enjeux qui en sont issus sont entremêlés et souvent complexifiés obligeant un regard quelque peu pessimiste sur la faculté des *stakeholders* à générer un corpus normatif efficient et adapté. Preuve en est, « *les acteurs ne se projettent pas dans un système global mais dans un mode ou coexisteront des pluralités de standards, de technologies, d'architectures et d'opérateurs.* »[39]

(39) Conseil Général de l'économie de l'industrie, de l'énergie et des technologies Rapport Internet des objets et logistiques « vers des nets avec des objets « Situation international, perspectives des acteurs et débat » http://www.cgeiet.economie.gouv.fr/Rapports/2013_07_01_2012_25_Rapport.pdf

Objets connectés et protection des droits de la personnalité

Passés sous silence lors de la rédaction du Code civil, les droits de la personnalité sont longtemps restés dans le champ des hypothèses juridiques. Nés par, et en raison du développement de la technologie, les droits à la personnalité constituent un des principaux enjeux du développement de l'Internet des Objets[40].

Ainsi, l'émergence de nouvelles techniques potentiellement attentatoires aux droits de la personnalité a par le passé conduit à une prise en compte juridique des risques y attachés (A) conduisant à envisager l'application du corpus normatif actuel au sein des l'IdO (B)

(40) Communication de la Commission au Parlement Européenne au Conseil, au Comité économique et social européenne et au comité des régions : « Internet des objets - Un plan d'action pour l'Europe » - 18 juin 2009 : « Il n'est pas à douter que l'IdO modifiera notre conception de la vie privée ».

Genèse et facteurs d'émergence des droits de la personnalité

Le droit de la personnalité relève d'un champ qui s'est construit progressivement. Ainsi, il peut recouvrir, en fonction de la branche du droit évoqué, le droit à la vie privée, le droit à l'image, le droit moral de l'auteur, les droits sur les traitements de données à caractère personnel etc. Il apparaît donc clairement que les objets connectés ne peuvent s'émanciper de ces droits mais seront eux-mêmes source d'évolution de ce droit.

En effet, il apparaît clairement que la création, parfois prétorienne, des droits de la personnalité n'est qu'un écho à l'évolution des moyens technologiques pouvant conduire à la mise en danger des droits inhérents à la personne humaine. Accentuée à compter de la seconde moitié du XX^{e} siècle, la prise en compte de ces droits n'a cessé de se diversifier. Ainsi dès 1957, le législateur a consacré le droit moral de l'auteur sur son œuvre en raison de la multiplication des moyens permettant la copie de ces derniers.

Mais c'est principalement dans les années 1970 que les risques issus du développement des technologies obligent à des interventions multiples du législateur dans le domaine de la protection des droits de la personnalité. Ainsi, l'émergence des moyens d'enregistrement des voix et de l'image (caméra, zoom) ont conduit le législateur à introduire, par la loi du 17 juillet 1970, la consécration de la protection de la vie privée au sein du Code Civil[41].

(41) Art 9 du Code civil : « Chacun a droit au respect de sa vie privée. »

Mais le développement de l'informatique va permettre l'émergence d'un corpus novateur visant à éviter initialement l'immixtion des pouvoirs publics au sein de la sphère de la vie privée. La prise de conscience des dangers que peut permettre le développement de l'informatique se fera au travers de la mobilisation à l'encontre de SAFARI (*Système Automatisé des Fichiers Administratifs et du Répertoire des Individus*) permettant l'interconnexion des fichiers publics à partir d'un identifiant unique. Suivant l'exemple de la Suède et du Land de Hess (Allemagne), le législateur Français a mis en œuvre une législation contraignante permettant la protection des traitements automatisés des « informations nominatives ».

Ainsi, la loi n°76-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, visait à encadrer et sécuriser l'usage des « Informations nominatives » précisait en son article 1er que :

> *« L'informatique [...] ne doit porter atteinte ni à la l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».*

Ces « informations nominatives » devenant en 2004[42], sous l'impulsion européenne[43], les données « à caractère personnel[44] » sont aujourd'hui un des socles de garantie des droits individuels face au développement de la société de l'information. Ainsi, sont consacrés le droit d'opposition (*Loi du 6 janvier 1978, art 38*), le droit d'accès (*art 39*) et le droit de rectification (*art 40*). Il convient de souligner qu'il n'existe pas de droit à l'oubli, dont la portée pourrait être précisée par le projet de règlement européen.[45]

C'est ainsi une vision très large de la donnée personnelle qui est ici entérinée[46] accroissant *de facto* le champ d'application matériel de la Loi. Ainsi, sont considérées comme des données personnelles les références directes relatives à l'identité comme le nom, du prénom, de l'âge, du sexe, des dates et lieux de naissance, des numéros d'identification sur la carte d'identité, le passeport, les coordonnées personnelles et/ou professionnelles ou encore les coordonnées électroniques[47], une photographie, une vidéo permettant de reconnaître les individus, l'enregistrement de voix[48]. Constituent aussi des données personnelles les habitudes de vie, les comportements de consommation, les loisirs, les diplômes et l'adresse IP[49] malgré certaines réticences de la Cour de cassation[50].

La protection de données relatives à la personnalité forme aujourd'hui un socle protecteur minimal au regard des risques du numérique. Consacré sur le plan national, il l'est tout autant sur le plan international. Ainsi, peut être cité l'article 12 de la Déclaration Universelle des Droits de l'Homme adoptée par l'Assemblée Générale des Nations unies le 10 décembre 1948[51], la Convention Européenne de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales, adoptée par le Conseil de l'Europe le 4 novembre 1950[52] et ratifiée par la France en 1974[53].

Enfin, la Charte des droits fondamentaux de l'Union européenne, socle des évolutions futures dans le domaine et dont la portée est devenue obligatoire depuis le 1er décembre 2009 *via* l'adoption du Traité de Lisbonne précise :

Article 7 : Respect de la vie privée et familiale

Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.

Article 8 : Protection des données à caractère personnel

1. *Toute personne a droit à la protection des données à caractère personnel la concernant.*
2. *Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.*
3. *Le respect de ces règles est soumis au contrôle d'une autorité indépendante.*

(42) LOI n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(43) Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données

(44) Art 2, al 2 de la loi 78-17 du 6 janvier 1978 modifiée : « Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. »

(45) Pour un état des lieux de l'état d'avancement du Projet : Rapport d'activité 2013 de la Commission nationale de l'informatique et des libertés.

(46) Pour une vision du Groupe de travail « Article 29 » : Avis 4/2007 sur le concept de données à caractère personnel.

(47) Cass Crom, 14 mars 2006, n°05-83.423.

(48) TGI Paris, 1re chambre, 4 avril 2006 n° 05/18.400.

(49) CA Rennes, 3ech 22 mai 2008 C.S. c/ SACEM où il a été jugé que l'adress IP est une donnée personnelle ; ou encore Cons.Const, 10 juin 2009 n°2009-580 DC, JO 13 juin ; ou encore CJCE, 29 janvier 2008 aff. C-275/06, Productores de musica de Espana c/ Telefonica de Espana SAU.

(50) Cass Crom, 13 janvier 2009, n° 08-84.088.

(51) Art 12 DUDH : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

(52) Article 8 de la convention européenne des droits de l'homme : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ».

(53) Il convient de souligner que cette ratification intervient dans les années 70 ou la France prend conscience des enjeux de la protection des droits de la personnalité.

C'est au travers de ces fondements que le Conseil National du Numérique, dans le cadre du Projet Transatlantique de Commerce et d'Investissement entre l'Union européenne et les États-Unis, a pu affirmer que « *toute libéralisation de la circulation des données devra être complétée par des dispositions permettant des restrictions fondées sur des objets de protection de la vie privée des personnes et de sécurité publique.* »

C'est donc un corpus normatif complet qui est aujourd'hui existant en matière de protection des droits de la personnalité. Il demeure, comme le soulignait Epicure[54], qu'une règle ne peut être intangible pour qu'elle soit « juste ». Les droits de la personnalité plus que tout autre démontrent que la règle de droit doit s'adapter aux circonstances et à son environnement d'application.

Dès lors, la loi est-elle la plus à même d'appréhender les enjeux qu'impliquent le numérique ? La création de la norme juridique par une entité étatique ou supra-étatique est-elle la plus adéquate face aux enjeux globaux qu'implique, par exemple, le transfert de données personnelles ? La *ratio legis*, (la raison d'être de la loi) demeure, son appréhension se retrouve comme principe fondamental devant guider les acteurs du numériques. Ainsi, comme le souligne Isabelle Falque-Pierrotin, « *une plus grande adaptation au numérique [de la loi informatique et libertés] devient urgence, et c'est bien le sens du projet de règlement européen. Les principes « Informatique et Libertés » demeurent robustes et adaptables aux évolutions technologiques* »[55].

Pour nombre d'auteurs, la pyramide normative Kelsenienne arrive aujourd'hui au terme du processus. La verticalité qu'elle impose s'oppose à l'horizontalité normative aujourd'hui en recherche. Ainsi, chartes, normes, GIE, labels sont aujourd'hui autant de garanties que l'utilisateur comprend et appréhende. En est-il de même du corpus juridique traditionnel ?

(54) EPICURE Maximes XXXVIII « *Là où, sans que des circonstances extérieures nouvelles soient apparues, dans les actions mêmes, ce qui avait été institué comme juste ne s'adaptait pas à la prénotion, cela n'était pas juste ; en revanche, là où, à la suite de circonstances nouvelles, les mêmes choses établies comme justes n'avaient plus d'utilité, alors, dans ce cas, ces choses avaient été justes, lorsqu'elles étaient utiles à la communauté des concitoyens entre eux, et ultérieurement ne l'étaient plus, lorsqu'elles n'avaient pas d'utilité.* »

(55) Rapport d'activité 2013 de la Commission nationale de l'informatique et des libertés.

Internet des Objets connectés face aux droits de la personnalité

Identification des risques

L'ensemble des acteurs s'accorde à dire que les orientations prises en matière de protection des données personnelles et de la vie privée auront un impact déterminant sur le développement de l'internet des objets connectés. Toutefois, et il est essentiel de le souligner, l'objet connecté n'est potentiellement qu'un moyen de collecte de données personnelles. Le traitement et l'usage demeurant une étape postérieure.

À titre liminaire, M. Philippe Lemoine, commissaire de la CNIL, avait, dans une communication du 30 octobre 2003[56] sur le sujet de la radio-identification, identifié 4 pièges pouvant conduire à minorer le risque de l'IdO sur la protection des données personnelles et la vie privée :

- l'insignifiance [apparente] des données,
- la priorité donnée aux objets [en apparence toujours vis-à-vis des personnes],

(56) Communication de Philippe Lemoine relative à la radio identification, Cnil, séance du 30 octobre 2003.

- la logique de mondialisation [normalisation technologique basée sur un concept américain de « privacy » [57]] sans prise en compte des principes européens de protection de la vie privée[58]]

- Le risque de « non vigilance » individuelle [présence et activation invisibles].

le Web 2.0 était celui du web participatif et social, comme le désignait Tim O'Reilly [59]. Ce dernier avait vu l'émergence d'un Internet ou l'utilisateur devenait acteur et auteur. Certains considèrent que les utilisateurs ont pris conscience du risque inhérent à l'usage de l'Internet et sauraient aujourd'hui maîtriser les méthodes permettant la protection de leur intimité.

Une telle assertion nous semble dangereuse sur trois points :

- Premièrement, les moyens de capter des données se sont aujourd'hui multipliés et diversifiés. Donner son âge sur *Facebook* est-il la même chose que d'accepter un cookie intrusif ? de se déplacer avec son téléphone portable ou sa montre connectée ? La vigilance individuelle n'est aujourd'hui plus suffisante afin de garantir la protection de sa vie privée tant la collecte de donnée se généralise.

- Dans un deuxième temps, un tel présupposé remettrait en cause le rôle des organes publics dans la protection de l'individu et conduirait à admettre qu'Internet serait une zone de droit non étatique.

- Dans un troisième temps, il faut noter le caractère contaminant de l'usage des objets connectés sur les tiers. Ainsi, l'usage de *Google glass* n'impacte t-il uniquement que l'utilisateur ? une réponse négative ne peut que s'imposer et il importe donc que des règles protectrices soient mises en œuvre à un niveau dépassant l'utilisateur afin de protéger ceux qui subiront l' usage d'objets connectés.

L'identification des risques inhérents aux objets connectés demeure encore aujourd'hui relativement incertaine, l'usage ayant toujours dépassé la pensée. Ainsi, il est intéressant de constater l'évolution de la politique des États-Unis dans le domaine eu égard aux impacts sur la « Privacy » que peut générer le Big data :

> *«These implications make urgent a broader national examination of the future of privacy protections [...] While notice and consent remains fundamental in many contexts, it is now necessary to examine whether a greater focus on how data is used and reused would be a more productive basis for managing privacy rights in a big data environment».* [60]

Il demeure que la confiance nécessaire entre l'utilisateur et les objets qui l'entourent nécessite de prendre en compte les intérêts inhérents à la protection de sa vie privée dès la conception des objets connectés.

Vie privée et conception de l'objet connecté
(Privacy by design)

Le projet actuel du règlement européen ne semble pas consacrer le principe du « privacy by design » mais appelle à prendre en compte la vie privée dès

(57) Pour approfondir la dichotomie, : James Q.Whitman, The Two Western Cultures of Privacy : Dignity versus Liberty, Yale Law School Legal Scholarship Repository, 2004.

(58) Pour l'évolution de la position juridique des Etats Unis - Executive Office of the President , BIG DATA : Seizing opportunities preserving values Mai 2014

(59) Oct. 2009: Tim O'Reilly and John Battelle answer the question of «What's next for Web 2.0?» in Web Squared: Web 2.0 Five Years On. http://oreilly.com/web2/archive/what-is-web-20.html

(60) Executive Office of the President, BIG DATA : Seizing opportunities preserving values Mai 2014.

la conception de l'objet. Dans la même lignée, la Commission européenne[61] a émis le souhait que les usagers puissent désactiver les puces.

Toutefois, le pas de la réglementation obligatoire n'a pas été franchi tant au terme de la conception de l'objet que de celle afférente à la désactivation des puces. Il demeure que les instances Européennes indiquent très clairement la prise en compte des dangers des objets connectés par les instances communautaires. Dans une démarche de conseil, la CNIL préconise la mise en place de mécanismes de désactivation des objets connectés dans certaines situations et selon le choix des utilisateurs tout en soulignant que la désactivation conduirait à ne plus permettre l'usage final de l'objet[62].

C'est dans un tel contexte que le Groupe de Travail Article 29 conseille aux entreprises de mettre en œuvre une évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence.[63] Une telle proposition ne doit pas être regardée comme restrictive et doit s'appliquer à notre sens à toute mise en œuvre d'objets connectés et pas seulement à ceux faisant usage de la RFID.

(61) Communication de la Commission au Parlement européen, au Conseil, Comité économique et social européen et au Comité des régions - L'internet des objets : un plan d'action pour l'Europe - Bruxelles le 18 juin 2009 COM(2009)278 final.

(62) CNIL, RFID : Des puces aux usages multiples et aux impacts variés en termes de vie privée 26 septembre 2013 : http://www.cnil.fr/linstitution/actualite/article/article/rfid-des-puces-aux-usages-multiples-et-aux-impacts-varies-en-termes-de-vie-privee/

(63) Avis 9/2011 sur la proposition révisée des entreprsies relative au cadre d'évaluation de l'imapact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquecne (RFID).

Quel consentement pour l'Internet des objets connectés ?

Le consentement, bien connu au travers de la loi de 78, est un élément fondamental dans l'ensemble des droits de la personnalité. Par ce dernier, la personne affirme sa maîtrise sur les droits subjectifs sur sa personnalité. Cette maîtrise peut correspondre en un droit de rétention, de révélation, de mise au point et/ou de rectification. C'est donc un droit éminemment marqué par la volonté du titulaire de ces droits: la personne elle-même ou son représentant légal pour les majeurs incapables[64] et les titulaires de l'autorité parentale pour les mineurs. Toutefois, pour ces derniers, leur avis peut être déterminant et apprécié au cas par cas par les juges en fonction de l'appréciation de la capacité de discernement du mineur[65].

Ainsi, le consentement répond à certains critères de formalisme: le consentement doit être spécial, en ce sens qu'une personne ne peut consentir de façon générale à une atteinte à sa vie privée ou à son image[66] ou à une cession de ses créations[67]. Toutefois, il ne doit pas nécessairement être exprès[68]. Ainsi la loi de 78 précise seulement que « *le traitement de données à caractère personnel doit avoir reçu consentement de la personne concernée*[69] ». Toutefois, et rappelons le, en la matière, la charge de la preuve appartient au défendeur[70] et il ne serait que plus prudent d'obtenir un consentement formel au travers d'une case à cocher ou d'un mail de validation par exemple. Une telle solution semble aisée lorsqu'une interface existe, mais bien plus difficile lorsqu'elle n'existe pas (puces passive, RFID...). Le simple usage correspondrait-il à un consentement ? Ainsi, peut-on analyser par mimétisme le consentement au traitement de données personnelles et le consentement pouvant être tacitement accordé à une personne filmée[71] ?

(64) Civ 1er, 24 février 1993

(65) Aix en Provence, 19 décembre 1968 ; TGI Nanterre, 4 mars 2002

(66) TGI Paris 19 novembre 2007

(67) L131-1 du Code de la Propriété Intellectuelle « La cession globale des œuvres futures est nulle. »

(68) Civ1er 7 mars 2006 « le consentement à la diffusion d'images de la personne ou de faits de sa vie privée peut être tacite ».

(69) Art 7 de la Loi du 6 janvier 1978.

(70) En effet, malgré l'article 1315 du Code civil, c'est à celui qui prétend disposer du droit d'user d'un des éléments du droit de la personnalité d'un tiers de s'en prévaloir.

(71) Pour des exemples illustratifs de la faculté et des limites : TGI Paris, 18 mai 2009, TGI Paris 27 septembre 2004, Toulouse 31 mars 2009, TGI Paris 5 décembre 2007)

Internet des objets connectés et multiplicité des données collectées[72]

L'obtention du consentement de l'utilisateur direct des objets connectés n'est pas la seule difficulté à laquelle doivent faire face les responsables de traitement. En effet, en précisant que « *les données sont collectées et traitées de manière loyale et licite*[73] » la loi informatique et liberté met en exergue une des garanties fondamentales du droit au respect de la vie privée comme l'a rappelé le Conseil Constitutionnel[74]. Peut-on parler de collecte licite lorsque *Facebook* génère des profils de personnes qui ne sont pas utilisateurs de ses services ? [75] La problématique des « profils fantômes » est endémique dans le cadre de l'usage de services permettant une interaction directe (ex : enregistrement d'un environnement) ou indirecte (l'utilisateur dépose des photographies). En effet, comment maîtriser le bruit, c'est-à-dire des données personnelles récoltées sans qu'un consentement quelconque ne soit accordé ? Comment maîtriser la captation de données aujourd'hui insignifiante et permettant probablement dans le futur d'identifier indirectement une personne ? C'est là, à notre sens, une des principales difficultés que doivent prendre en compte les entreprises souhaitant mettre en œuvre des objets connectés et notamment ceux afférents à la domotique.

Par essence, la mise en œuvre d'objets connectés capables d'interagir avec leur environnement conduira à l'enregistrement et au traitement de données personnelles de personnes n'ayant pas donné leur consentement. À titre d'exemple, a été considéré comme déloyal le fait de collecter des adresses MAC rapprochées d'identifiants SSID d'utilisateurs de réseau WI-FI[76]. Dans ce même avis, il est intéressant de constater que la CNIL admet, au regard de l'article 32 III de la loi informatique et libertés[77], « *que l'information individuelle des titulaires des adresses MAC et des identifiants Wi-Fi est effectivement impossible à mettre en œuvre* » dans le cadre de l'usage des *Google cars*, mais elle estime que la Société *Google* aurait dû mettre en œuvre une information généralisée comme elle l'avait fait dans le cadre de la collecte de photographies par les *Google cars*.

Autre cas de figure pouvant être envisagé dans le cadre de ce bruit est l'usage de l'article 7 5° disposant qu'un traitement de données à caractère personnel peut être mis en œuvre s'il satisfait à la condition suivante :

> « *[...] La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.* »

Il nous semble que l'usage de la présente exception dans le cadre de la mise en œuvre d'objets connectés ne puisse être soulevée qu'en cas de traitement dont la finalité demeure le bon fonctionnement exclusif de l'objet et à condition que ce fonctionnement ne soit pas trop intrusif. En effet, la finalité du traitement est un élément essentiel au degré d'application de l'article 7 5°. Ainsi, une finalité mercantile[78], de marketing ou de démarchage est appréciée très strictement par la CNIL conduisant à une obligation de loyauté « renforcée » pour ces catégories[79]. Ainsi, comme le souligne Romain Perray « *la méthode*

(72) Pour une description plus approfondie du lien entre objets connectés et Santé et notamment une analyse comparative et prospective de la législation y afférente: Cahiers IP n°2, Le corps, nouvel objet connecté : du quantified self à la M-Santé : les nouveaux territoires de la mise en données du Monde - De nouvelles pratiques individuelles - Ecosystème et jeux d'acteurs - Quels axes de régulation, Les voies à explorer - Juin 2014.

(73) Art 6 de la Loi du 6 janvier 1978.

(74) Conseil Constitutionnel dés. N°2007-557 DC 15 nov 2007.

(75) http://www.lefigaro.fr/secteur/high-tech/2011/10/25/01007-20111025ARTFIG00540-les-etranges-profils-fantomes-de-facebook.php

(76) CNIL, délib n°2011-035, 17 mars 2011 ; Affaire Google Street View.

(77) Article 32 III al 2 [...] « *Ces dispositions ne s'appliquent pas non plus lorsque la personne concernée est déjà informée ou quand son information se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche* ».

(78) Usage de données personnelles relatives à des professeurs notés par leurs élèves TGI Paris 3 mars 2008.

(79) Romain PERRAY, Formulaire commenté Lamy Droit de l'Immatériel II 600.40.

d'analyse suivie par la CNIL et les juridictions repose ici avant tout sur une mise en balance des intérêts en présence. Elle se distingue en cela de celle préconisée par le Groupe de l'article 29 qui privilégie davantage l'examen du critère de nécessité[80] ».

(80) Groupe art 29, avis n°1/2008 4 avril 2008.

Conséquences

Il convient de souligner que de nombreux sujets ayant traits aux droits de la personnalité vont connaître des bouleversements au regard des objets connectés. Ainsi, la CNIL, dans son rapport d'activité 2013, envisage et analyse le développement du chantier Bien-être et santé numérique au travers du prisme des objets connectés, tout en soulignant certaines difficultés juridiques qui seront soulevées par ces développements. Peut aussi être envisagé le développement du secret des affaires par la montée en puissance des moyens d'espionnage des entreprises[81] *via* les objets connectés (*par exemple : Target et l'attaque au travers du système de climatisation*) ou même du droit social et de la surveillance des salariés.

(81) Pour la reconnaissance de droits de la personnalité aux personnes morales en matière de diffamation (Cass Crim 10 juillet 1937 Bull.crim. n°147 ; Civ. 2e, 18 déc. 1995, n°93-21.287), dénonciation calomnieuse (Cass Crim 22 juin 1999 n°98-80.593), concurrence déloyale (Cass com 9 février 1993 n°91-12.258).

Ainsi, c'est avec une attention certaine que les entreprises devront mettre en œuvre les obligations issues du futur règlement européen. Ce dernier aura *a minima* le mérite d'unifier au sein de l'Union européenne des divergences d'application des normes applicables aux données personnelles[82], qualifiées par certain d'« or noir du futur numérique ». Il n'empêche que la *ratio legis* de la loi informatique et libertés demeurera et que les principes sous-jacents à cette dernière forment aujourd'hui le socle de la protection de la vie privée des concitoyens européens.

(82) À titre d'exemple, certains États membres excluent la sécurité publique du champ de la Directive 95/46/CE du 24 octobre 1995.

Quelle responsabilité pour les objets intelligents ?

L'usage des objets connectés conduira nécessairement à interroger le droit de la responsabilité. Certains enjeux impliquent les accords contractuels en matière d'objets connectés, notamment en termes de champs de responsabilité. Il apparaît toutefois que d'importants enjeux propres à la responsabilité délictuelle peuvent apparaître et principalement en terme de dommages survenant à un tiers à tout engagement contractuel lié aux objets connectés.

Objet connecté et responsabilité délictuelle du fait des choses

Comme nous l'avons déjà souligné, l'objet n'a pas de statut légal au sein du Code civil, tout au plus est-il un bien meuble. Ainsi, le bien n'est que le corolaire d'un autre droit, que ce soit en terme de propriété (art 544 C.C : *La propriété est le droit de jouir et disposer des choses de la manière la plus absolue, pourvu qu'on n'en fasse pas un usage prohibé par les lois ou par les règlements*), de la légalité d'une convention (art 1128 C.C Il n'y a que les choses qui sont dans le commerce qui puissent être l'objet des conventions.), en terme de responsabilité

(art 1384 On est responsable [...] des choses que l'on a sous sa garde.)... Les choses ne sont pas des sujets de droit *per se*.

Le fait que le bien n'ait pas de statut n'a pas empêché la jurisprudence de chercher une définition de ce qu'est une chose au sens du Code Civil. En effet, le développement du machinisme à la fin du XIXe siècle a conduit à la multiplication des dommages causés par des choses sans que la responsabilité directe de leur propriétaire ne puisse être établie au moyen de l'article 1382[83]. S'en suivit l'usage extensif par les juridictions de l'article 1384 alinéa 1er disposant:

> *« On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde. »*

Ainsi, la chose est un bien meuble, définie notamment comme « les *animaux et les corps qui peuvent se transporter d'un lieu à un autre [...]* », ou un bien immeuble. Constitue aussi une « chose » au sens de la jurisprudence, une onde sonore ou électrique, une image de télévision[84]. De plus, le fait que la chose soit inerte ou en mouvement[85], actionnée ou non par la main de l'homme[86] est indifférent à l'application de l'article 1384 du Code Civil.

Au visa de l'article 1384, le domaine de la responsabilité du fait des choses démontre la résilience du droit et conduit à affirmer que ce dernier pourra s'appliquer aux dommages causés par les objets connectés.

(83) Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer.

(84) TGI Paris 27 février 1991 : JCP 92, II,21809.

(85) Cass Civ, 19 et 24 février 1941, Cass 2e civ 16 octobre 1963.

(86) Cass ch réunies 13 février 1930.

Vers une responsabilité spéciale applicable aux objets connectés ?

Malgré les dispositions applicables à la responsabilité délictuelle, le législateur a souhaité garantir l'indemnisation des victimes en instaurant des régimes spéciaux plus protecteurs. Appelées lois d'indemnisation, ces dispositions spécifiques pourraient suppléer les dispositions générales évoquées ci-dessus dans le cadre de la mise en œuvre des objets connectés. En effet, la mise en œuvre de la responsabilité délictuelle d'une personne se heurte toujours à la solvabilité de ce dernier.

Responsabilité spéciale et accident de la circulation

Tel est le cas en matière d'accident de la circulation, objet de la loi n°85-677 du 5 juillet 1985. L'objectif de cette loi n'est pas de rechercher un responsable, mais un débiteur solvable et, à travers lui, un assureur garantissant l'indemnisation de la victime. C'est pour cela que la présente loi oblige toute personne faisant circuler des véhicules terrestres à moteur à souscrire une assurance[87]. Une telle loi pourrait s'appliquer par exemple aux automobiles connectées de type *Google cars*.

(87) Article L 211-1 du Code des assurances. Notons qu'il n'est pas ici question de « conducteur », permettant de couvrir l'usage de voitures automatisées.

Responsabilité spéciale du fait des produits défectueux et émergence d'un droit à l'expérimentation

Peut aussi être citée la loi n°98-389 du 19 mai 1998 relative à la responsabilité du fait des produits défectueux permettant d'engager directement la responsabilité du producteur qu'il soit ou non lié par un contrat avec la

victime. Élément essentiel de cette loi la responsabilité du fabricant peut être engagée sans faute. Cette loi s'applique aux termes de l'article 1386-2 à la réparation du dommage qu'il résulte d'une atteinte à la personne et/ou à la réparation du dommage supérieur au montant de 500€[88] qui résulte d'une atteinte à un bien autre que le produit défectueux lui-même. Cette loi s'applique à l'ensemble des biens meubles, même incorporés à un bien immeuble[89]. Ce dernier point trouvant une application particulièrement intéressante dans le cadre de la domotique.

Aussi, il convient de souligner que les clauses exonératoires de responsabilité prévues à l'article 1386-11, intégré au sein du code par la loi du 19 mai 1998, prévoient notamment une exonération pour *risque de développement* ayant fait l'objet de très nombreux débats. Il demeure que notre corpus légal est aujourd'hui assez peu adapté face aux besoins d'expérimentations que nécessite l'émergence des objets connectés. Ainsi, le rapport France robot Initiative[90], propose que la France se dote d'un organisme compétent dans le domaine de l'évaluation de la certification de produits robotiques non industriels. Une telle solution permettrait à tout le moins de s'interroger sur les évolutions et adaptation nécessaires de la réglementation nationale en faveur de l'innovation.

(88) Décret n° 2005-113 du 11 février 2005 pris pour l'application de l'article 1386-2 du code civil.

(89) 1386-3 du Code civil.

(90) Ministère du Redressement Productif, Ministère de l'enseignement supérieur et de la recherche, France Robot Initiative 2013.

Conséquences

Il convient de s'interroger sur l'évolution que connaîtront les objets connectés, notamment dans le cadre du M2M et de l'ensemble des processus d'aide à la décision. Ainsi, qu'en serait-il d'un accident de la circulation issu de données d'un capteur tiers ? à notre sens, de tels contentieux pourront survenir et conduiront à d'importantes difficultés pouvant mettre à mal l'organisation juridique actuelle. Ainsi, la généralisation d'objets connectés et leurs interconnexions conduiront à des contentieux en termes d'imputabilité de la responsabilité d'un dommage. De telles actions feront l'objet d'expertises complexes et incertaines comme peuvent en connaître certains contentieux logiciels (rappelons le, il existe aujourd'hui plus de logiciels dans une voiture que dans les premières navettes spatiales). De ce fait les possibles lenteurs inhérentes à ces expertises peuvent conduire à des délais d'indemnisation particulièrement intolérables, notamment en cas de dommages corporels (et ce, malgré l'existence de fonds de garantie). Ces risques doivent être évoqués au sein de la gouvernance de l'Internet des objets et conduiront certainement à l'intervention du législateur dans le domaine du fait de la multiplication des contentieux.

La pratique juridique face aux objets connectés

Les quelques éléments ici soulevés conduisent à déterminer certains postulats applicables à une analyse juridique des objets connectés :

- L'objet connecté n'est pas un sujet de droit, mais les conséquences de son usage peuvent conduire à une révolution copernicienne de la notion de vie privée et au développement d'un corpus juridique spécifique.
- Les objets connectés sont multiples et fortement différenciant. Y introduire des règles génériques serait un échec.
- La multiplicité des *stakeholders* rend peu probable une entente globale en matière de Gouvernance.

Dès lors, les entreprises souhaitant mettre en œuvre des objets connectés doivent impérativement respecter certains prérequis :

- Préalablement à leur mise en œuvre, les objets connectés doivent faire l'objet d'une évaluation de l'impact sur la protection des données et les conséquences directes et indirectes de leur usage.
- Une démarche d'information doit être réalisée auprès des utilisateurs finaux. De tels objets ne doivent en aucun cas être introduits sans information préalable comme ce fut le cas pour les téléviseurs LG[91].
- Le développement commercial d'un objet connecté dépend de sa capacité d'adaptation à son environnement. Ainsi, des mécanismes permettant tout à la fois de protéger l'évolution technologique réalisée par l'objet connecté et son interopérabilité avec d'autres objets et d'autres services connectés doivent être mis en œuvre. Une réponse juridique adaptée doit être imaginée dès la conception de l'objet.
- Enfin, la préoccupation éthique est rendue plus complexe par la richesse des pré-supposés historiques, culturels, religieux, qui déterminent le socle de chaque société. À titre d'exemple, la notion de propriété, de vie privée (avec les difficultés relatives à la définition de *privacy*) sont multiples et divergent en chaque point du monde. Une analyse par marché doit être réalisée.

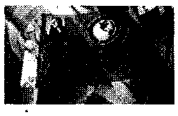
Il nous apparaît dès lors essentiel que la mise en œuvre d'objets connectés nécessite non seulement le respect des dispositions légales aujourd'hui applicables, mais doivent conduire à une véritable démarche RSE par les acteurs du secteur. Ainsi, une démarche de labellisation et d'entente sectorielle doit être encouragée reprenant les principes développés par le RFID *Bill of Rights* proposé par Simon Garfinkel[92] qui énumère les droits suivants :

- le droit de savoir si un produit contient des étiquettes RFID ;
- le droit au « silence des puces[93] » pour que les puces soient ôtées ou désactivées une fois l'achat effectué ;
- le droit d'utiliser des services à base de RFID sans étiquettes RFID ;
- le droit d'accès aux données stockées sur les puces ;
- le droit de savoir quand, où et comment les données sont lues.

(91) Laure MARINO, «To be or not to be connected: ces objets connectés qui nous espionnent. À propos des téléviseurs LG», Recueil Dalloz 9 janvier 2014, n°1, Point de vue p. 29.

(92) An RFID Bill of Rights Wireless ID tags will soon be everywhere. We need a manifesto!By Simson Garfinkel on October 1, 2002.

(93) Le Conseil des ministres des télécoms de l'UE à souligné en 2008 son souhait de reconnaitre ce «droit au silence des puces» RFID mais ne semble pas aujourd'hui rentrer dans le cadre du droit positif en l'état.



SÉCURITÉ TECHNIQUE ET OPÉRATIONNELLE

Introduction

Nous traitons dans ce chapitre le contexte de l'entreprise, et notamment les grandes entreprises membres du CIGREF, confrontée à l'introduction au sein de ses systèmes d'informations d'objets connectés pour répondre à des besoins qui sont soit cœur de métier soit de support aux activités de l'entreprise.

Lorsque ces besoins sont au cœur de métier, les objets connectés améliorent un produit ou un service rendu au client final :

- Pour un **Produit**, un exemple est la voiture connectée. La mise en œuvre doit garantir la sécurité du produit final et sa protection contre des défaillances d'origine accidentelle ou intentionnelle.
- Pour un **Service**, un exemple est la mise en œuvre de réseaux de capteurs pour améliorer l'efficacité globale d'un réseau de fourniture de commodités. Ainsi, dans le domaine de la distribution d'eau, une mesure rapprochée dans le temps de la consommation individuelle des abonnés à leur domicile permet de repérer très rapidement des fuites et de les réparer. La réactivité constatée améliore à la fois le service rendu au client et diminue les coûts de production. Là encore, il convient de s'assurer que la gestion globale de ces capteurs connectés se fasse en garantissant la disponibilité et l'intégrité des données. Ces derniers devenant les principales exigences pour s'assurer que le service est effectivement rendu.

Lorsque les besoins sont de support[94], il s'agit d'améliorer la gestion des fonctions dites supports de l'entreprise, par exemple, la mise à disposition de bâtiments qui sont alors dotés de capteurs intelligents en vue de diminuer la consommation électrique. Dans ce contexte, l'entreprise est simplement consommatrice d'objets connectés et non plus conceptrice comme dans le premier contexte.

(94) Support est défini par rapport à la chaîne de valeur de M. Porter.

Même si l'étendue et la nature des risques peuvent changer, il n'en demeure pas moins que l'introduction d'objets connectés, même de manière marginale, est de nature à créer de nouveaux risques pour le système d'information. Un bon exemple est la société Target qui a été attaquée via un système annexe dédié à la climatisation de ses bâtiments.[95]

(95) Sandrine CASSINI - *La difficile lutte des entreprises contre les hackers* - Les Echos.fr : http://www.lesechos.fr/19/02/2014/LesEchos/21630-094-ECH_la-difficile-lutte-des-entreprises-contre-les-hackers.htm

Changement de contexte

Le déploiement d'objets connectés au sein d'un système d'information d'entreprise amène des changements importants de contexte, qui vont fortement transformer l'approche en sécurité des SI. Ces changements portent sur les points suivants :

- l'environnement de travail et le personnel ;
- le volume et la nature des points de connexion ;
- le périmètre du réseau de l'entreprise ;
- la complexité d'intégration ;
- l'évolution de la *Supply chain IT* ;
- l'importance de la localisation ;
- le volume de données et leur traitement ;
- la nature des données.

L'environnement de travail et le personnel

Les objets connectés, suivant leur nature, peuvent changer l'environnement de travail, par exemple un management de consigne de température (maison connectée), un déplacement d'un instrument ou sa régulation (activation d'une pompe dans un réseau...).

Dans certains cas, la mise en œuvre d'objets connectés peut potentiellement mettre en danger la sécurité physique des personnes à proximité.

Dans le cas de la voiture connectée, le contrôle de certaines fonctions du véhicule telles que la direction, le freinage... ont un impact direct sur la conduite et tout dysfonctionnement peut amener une sortie de route. Sans parler des objets connectés dans le domaine de la santé (pacemaker, pompe...) dont les dysfonctionnements peuvent avoir un impact vital.

On se rapproche donc d'un sujet, la sécurité physique des personnes et des biens, bien connu et très familier dans le domaine de l'informatique industrielle, où ces considérations sont depuis longtemps largement pris en compte et traitées.

Le volume et la nature des points de connexion

La dissémination d'objets connectés au sein ou à la frontière de l'entreprise peut être massive. Le nombre de points de connexions peut être exponentiel au regard du nombre de points de connexion auparavant gérés par l'entreprise.

En outre, ces points de connexion peuvent être hétérogènes, la plupart du temps avec un usage spécifique porté par une mise en œuvre elle aussi spécifique. On sort ainsi du cadre habituel où le support physique d'un service est standardisé (*poste de travail ou serveur Windows ou autre, smartphone de marque et d'OS standard...*).

Le niveau de protection intrinsèque de ces nouveaux objets serait disparate et complexe, voire impossible même pour un simple monitoring des objets.

La capacité de l'entreprise à maîtriser ses points de connexion deviendrait particulièrement complexe et difficile.

Le périmètre du réseau de l'entreprise

Les modes de connexion des objets connectés avec le réseau de l'entreprise vont se diversifier :

- intégration complète sur le réseau IP interne avec un adressage IP propre à l'entreprise ;
- intégration à un réseau IP spécifique de l'entreprise, éventuellement structuré différemment (*type hub and spoke*) et communiquant au réseau de l'entreprise *via* une passerelle ;
- objet directement connecté sur internet et échangeant des données avec un système hébergé dans le *cloud*, lui-même interconnecté au réseau d'entreprise *via* une *gateway* ;
- objet connecté *via* des réseaux spécifiques, avec des protocoles de plus bas niveaux (voire chapitre norme), l'interconnexion avec le réseau d'entreprise se faisant via une passerelle adaptée.

Dans la plupart des cas, le lien sera plus ou moins maîtrisé entre les objets connectés et le réseau interne de l'entreprise.

Avec des objets connectés également accessibles par des entreprises tierces, par exemple pour des raisons de maintenance ou de mise à niveau, le nombre de points d'entrée sur le réseau de l'entreprise risque d'exploser.

La notion de sécurité périmétrique du réseau IP interne de l'entreprise ne reste plus pertinente (l'ennemi est dans la place).

La nature de l'intégration

Les objets connectés peuvent faire appel à une multitude de technologies, classiques ou exotiques, mises en œuvre de manière spécifique pour rendre un service ciblé à des coûts différenciés. Ce sont l'apparition de nouveaux protocoles réseaux, de systèmes d'exploitation spécifiquement conçus pour un usage et un prix définis.

Le cycle de vie de ces objets sera variable, s'écartant du cycle standard de 3 à 5 ans observé pour les infrastructures informatiques actuelles. Les cycles pourraient être plus longs en raison des capacités de remplacement limitées en regard du grand nombre de points.

L'intégration de ces nouvelles technologies au sein d'un SI basé sur les standards actuels du marché (*Windows, IP..*) sera complexifiée.

Le processus de Supply chain IT

Le caractère spécifique, *ad hoc*, des objets connectés devrait changer la nature de la *supply chain* à laquelle les équipes informatiques ont été habituées dans un monde standardisé autour des technologies de type *Microsoft*.

Un tel changement est celui de l'introduction du BYOD où il a fallu composer avec les utilisateurs et leurs choix personnels de "*device*" et de technologie.

Mais ce changement devrait être plus important en raison de la diversité des cas d'usage et de la spécificité des technologies employées. De plus

les intervenants sur ces objets devraient se multiplier, notamment pour des interventions maintenance ou de mise à niveau

La gestion de ce nouvel ensemble va demander une adaptation de la *supply chain* interne de l'IT.

La localisation des objets

Les objets connectés sont des objets, pas des services.

L'IT s'est progressivement dématérialisé avec l'avènement du *cloud* et il est devenu possible de construire et faire fonctionner un système d'information sans *datacenter*, en gérant essentiellement des terminaux et des points d'accès.

Avec les objets connectés, la localisation et la protection physique font leur retour.

Suivant le cas d'usage, il faudra prendre en compte les mesures nécessaires de protection des objets, notamment si ces objets sont des actionneurs. Il faudra à la fois les protéger de l'environnement mais aussi protéger leur accès pour éviter qu'ils ne soient accessibles par des personnes non autorisées ou par accident.

Le volume de données et leur traitement

Les objets connectés vont générer des volumes de données majeurs en proportion de leur étendue fonctionnelle et leur nombre.

Le stockage et l'exploitation de ces nouvelles données sont une source potentielle de très forte valeur ajoutée. Par exemple, le stockage et le traitement de données urbaines (capteurs de présence, de pollution, de trafic...) doit permettre d'optimiser la consommation d'énergie (régler l'éclairage urbain en fonction du trafic ou de la présence de population), la régulation du trafic urbain, l'occupation de l'espace de stationnement...

Les besoins de collecte, de stockage et de traitement de ces données devrait demander de nouvelles compétences en particulier celles liées au *big data*. L'augmentation drastique des besoins de stockage devra être contrebalancée par l'usage de technologies adaptées (*type de support suivant l'usage et la rapidité d'accès nécessaire, stockage dans le cloud...*).

Les compétences en matière de traitement des données "*big data*" sont récentes et peu disponibles en entreprise.

La nature des données

De par le grand nombre de cas d'usage potentiel, les objets connectés devraient générer des types de données très diverses qui pourront sortir du cadre de gestion habituel pour les données des systèmes d'information d'entreprise actuels: données personnelles ou médicales, données « industrielles » de type consigne...

À titre d'exemple, l'usage de lunettes telles que les *Google* glass dans une entreprise pour la maintenance (visualisation de plan d'installation ou de schéma, prise de photo et interaction avec un centre d'expertise...) soulève, en

raison du caractère potentiellement intrusif de cet objet, des questions inédites pour un responsable SI telles que :

- Quand activer ces lunettes ? Tout le temps ? Sur le lieu d'intervention ?
- Où et quand activer une prise de vue ou de son ?
- Quelle interaction si des personnes, notamment extérieures à l'entreprise (par exemple des clients) sont dans le périmètre de capture visuelle ou sonore ?
- Quelles données garde-t-on ? pour quel usage et pour combien de temps ?
- Une législation particulière s'applique-t-elle (protection de la vie privée...) ?

En outre, lorsque ces lunettes sont portées par un salarié, les données de localisation de l'appareil renseignent également sur la localisation du salarié et dès lors, doivent faire l'objet d'une attention particulière notamment de la part de la direction des ressources humaines.

Pour chaque donnée particulière, il faudra identifier et prendre en compte les problématiques juridiques ou sociales pertinentes.

Synthèse

En synthèse, il faudra engager pour la mise en œuvre des objets connectés des acteurs dont le profil va au-delà du cadre des équipes traditionnelles du système d'information :

- Automaticiens, informaticiens industriels, pour les aspects relatifs aux interactions entre les objets connectés et leur environnement
- Services généraux, agents de sécurité, pour les aspects relatifs à la localisation et à la protection éventuelle des objets connectés
- Fournisseurs de services tiers, pour la maintenance et la mise à niveau des objets connectés
- Spécialistes juridiques, pour traiter les contraintes spécifiques liées à l'usage et la mise en œuvre des objets connectés
- Spécialiste en gestion de ressources humaines, pour traiter les contraintes liées à la collecte et au traitement de données spécifiques à caractère personnel voire médical, à la localisation...

La gouvernance des projets relatifs à la mise en œuvre d'objets connectés et des opérations s'en trouve changée et complexifiée.

- Les problématiques de sécurité deviennent plus diverses, notamment d'un point de vue technique.
- Les approches habituelles de gestion, de monitoring peuvent devenir inopérantes
- Un renforcement des analyses d'impact avec un accent mis sur la résilience et l'intégrité des données doit être fait avec l'introduction éventuelle de méthodes nouvelles pour l'informatique de gestion, néanmoins courantes en informatique industrielle
- L'environnement RH et juridique doit être soigneusement pris en compte.

Préconisations pour la sécurité des projets avec des objets connectés

Les projets d'entreprise mettant en œuvre des objets connectés soulèvent de nouvelles problématiques de sécurité et ne rentrent pas forcément dans l'approche classique de sécurité de systèmes d'information.

Il semble donc difficile de trouver sur l'étagère une trousse à outil permettant de couvrir l'ensemble des problématiques.

Cependant, malgré leur diversité, les objets connectés font aussi largement appel à des technologies éprouvées en entreprise et pour lesquelles peuvent exister des approches et des standards de sécurité. La sécurité d'objets connectés développés sur une base de type *Android* pourra par exemple être couverte par un standard existant de l'entreprise sur ce système d'exploitation.

Le RSSI devra développer une approche *ad hoc*, qui sera une combinaison d'outils et de méthodes existantes complétées par des apports techniques et méthodologiques trouvés en dehors de son domaine habituel de compétence dans d'autres fonctions de l'entreprise, le tout sous une gouvernance adaptée.

Les grands axes de cette approche pourraient être les suivants :

- intégration de la sécurité en amont ;
- compréhension des besoins métiers et de leurs conséquences techniques ;
- adaptation de la gouvernance ;
- analyse de risque ;
- identification de l'ensemble des technologies et des risques inhérents ;
- prescriptions d'architecture liées à la sécurité ;
- prescription de dispositifs d'exploitation liés à la sécurité ;
- intégration de l'ensemble de ces prescriptions dans le plan projet ;
- revue de sécurité au cours de projet ;
- contrôle de la faisabilité et de l'efficacité des mesures de sécurité en production.

Intégration de la sécurité en amont

Il faut intégrer dès le lancement la sécurité au sein des projets Objets connectés ; comme dans tout projet SI, c'est la première recommandation.

Compréhension des besoins métiers et de leurs conséquences techniques

Dès le lancement, il faut comprendre et prendre en compte les objectifs et contraintes métiers, le caractère négociable (ou non) des exigences métier

en vue de dégager leur impact potentiel en matière de sécurité et leurs conséquences techniques.

Cet impact se traduit en termes de volumétrie d'objets, de besoins de communication, et de besoins d'intégration dans le SI existant.

Adaptation de la gouvernance

Il faut identifier l'ensemble des fonctions de l'entreprise parties prenantes et les intégrer à l'approche sécurité. Cela peut concerner l'informatique industrielle, les services généraux, le service juridique, la RH...

Analyse de risque

Au début du projet, il faut faire une analyse de risque globale.

Par rapport à une analyse de risque d'un projet IT habituel, une attention particulière doit être portée sur les aspects relatifs à la sécurité des personnes, aux conditions d'environnement des objets et aux risques associés, mais aussi aux risques juridiques ou sociaux potentiels.

Même si le traitement de ces risques n'est pas du ressort du RSSI, il semble pertinent de les identifier lors de la même analyse de risque de façon à pouvoir en coordonner le traitement.

Vue la multiplicité des aspects à couvrir, il faut s'assurer que la méthodologie d'analyse de risque en vigueur dans l'entreprise est bien adaptée ou complétée pour en couvrir tous les aspects.

Identification de l'ensemble des technologies et des risques inhérents

Une fois l'analyse de risque effectuée, il convient identifier l'ensemble des technologies mises en jeu et évaluer pour chacune de ces technologies, les standards de l'entreprise applicables.

Il faut vérifier le caractère applicable de ces standards par rapport à la configuration du projet.

De plus Il importe aussi identifier les technologies ne faisant pas l'objet de standard existant au sein de l'entreprise et définir comment l'approcher.

Lorsque les technologies identifiées sont déjà mises en œuvre dans l'entreprise, notamment pour les systèmes industriels, c'est une opportunité pour harmoniser et standardiser une approche commune à l'informatique de gestion et à l'informatique industrielle.

Si ce n'est pas le cas, il faudra définir la façon de mobiliser en interne ou en externe compétences correspondantes, aussi bien en matière de conception que d'exploitation.

Prescriptions d'architecture liées à la sécurité

Il convient de prescrire des choix d'architecture, à partir des standards existants ou d'approches et d'études spécifiques.

Prescription d'exploitation liées à la sécurité

Il faut prescrire les dispositions opérationnelles particulières devant être mises en œuvre et définir comment elles pourront s'intégrer, ou non, aux pratiques en vigueur. Par exemple :

- Est-ce que les objets connectés devront être patchés ?
- Si oui, à quelle fréquence ?
- Les outils existants dans l'entreprise peuvent-ils être utilisés ?

Intégration de l'ensemble de ces prescriptions dans le plan projet

Il faut intégrer l'ensemble des actions relatives à la sécurité dans le planning et la gestion des ressources du projet en veillant à anticiper les impacts potentiels sur l'exploitation et la maintenance.

Revue de sécurité au cours de projet

Il faut s'assurer que tous les aspects relatifs à la sécurité font l'objet de revue régulière, notamment à des étapes clés du projet, notamment en fin de phase de conception et en fin de phase de test avant mise en production. Suivant la nature du projet et des risques, des procédures particulières de test pourront être définies et mises en œuvre.

Contrôle de la faisabilité et de l'efficacité des mesures de sécurité en production

Lorsque de nouveaux outils ou processus de sécurité auront été mis en œuvre, il est pertinent de s'assurer, une fois en production, que ces outils ou processus répondent aux attentes et sont efficaces. Ceci pourra potentiellement se faire via des tests de vulnérabilité, d'intrusion ou autre, suivant la nature du projet.

Synthèse

Au final, ces préconisations présentent beaucoup de similitudes avec des projets classiques ; les problématiques techniques, la diversité des acteurs et la nature particulière des risques constituent les principales différences.

LA PROBLÉMATIQUE DES USAGES

De nombreuses réflexions et travaux alertent le management des systèmes d'information sur le besoin d'une meilleure prise en compte dans les méthodes et pratiques de la voix des utilisateurs. Par exemple, le CIGREF a décerné le prix CIGREF-AIM 2014 à un article préconisant une organisation des parties prenantes au système d'information autour de trois pôles, un « pôle utilisateurs », un « pôle managérial » et un « pôle technique »[96].

(96) « Le modèle d'alignement stratégique traduit: une approche par les pratiques », Isabelle Walsh, Alexandre Renaud, Michel Kalika, SIM, 2013.

L'irruption des Objets Connectés dans les systèmes d'information devrait renforcer ce recentrage sur l'utilisateur, voire sur l'usager.

Utilisation d'un SI et usage d'un objet connecté

Vue d'une entreprise, un objet connecté est un objet qui est connecté au système d'information en vue de délivrer un service, et qui est muni de capteurs et d'actionneurs.

Pour le directeur du système d'information, l'objet connecté est une composante du système d'information mais avec deux spécificités adressant respectivement les usages et les risques.

- Si l'entreprise entend d'un utilisateur qu'il utilise un équipement mis à sa disposition conformément à sa destination et à sa conception, elle reste incertaine sur l'usage fait par le détenteur d'un Objet Connecté. Il lui faut également s'attendre à des usages imprévus, parfois inconséquents, voire détournés ou illicites.
- Par ailleurs, du fait de l'embarquement de capteurs et d'actionneurs, l'usage d'un objet connecté fait naître des risques sur les personnes, les biens et l'environnement, qui sont de nature différente de ceux auparavant identifiés par les pratiques de management de systèmes d'information.

Aménagements de la gouvernance des système d'information pour les objets connectés

Pour faciliter la conduite de ce changement, le directeur des systèmes d'information peut considérer l'opportunité de traiter spécifiquement la problématique des usages.

Dans cette perspective, il pourra s'appuyer sur les pratiques de gouvernance et de management de projet en vigueur, mais avec des aménagements.

Les opportunités d'aménagement concernent :

- les métiers de l'informatique, avec l'institution d'un responsable des usages ;
- la gestion du cycle de vie de projet, avec des expériences client en situation réelle ;
- les méthodes d'analyse, avec des référentiels adaptés ;
- les livrables de management, avec la définition renforcée de conditions d'utilisation.

Responsable des usages

Pour adresser le premier point, il pourra instituer au côté du Chef de projet Maîtrise d'ouvrage et du Chef de projet Maîtrise d'œuvre[97] un responsable des usages[98]. Selon les besoins, ce responsable pourra convoquer aux comités de direction de projet le responsable CNIL ou le responsable des actifs immatériels de l'entreprise.

(97) Les métiers des systèmes d'information dans les grandes entreprises Nomenclature RH, 2011, Cigref.

(98) Instituer un Chef de projet Maîtrise d'usage en vue de l'Internet des Objets, Tru Dô-Khac, Le Cercle Les Echos, mars 2014.

Expérience clients en situation réelle

Pour adresser le second point, on pourra mener des expériences client en situation réelle : ainsi *Google* a mobilisé 10000 testeurs parmi ses employés pour explorer les usages de la *Google* Glass. Parmi ces usages, on peut facilement imaginer une utilisation des *Google Glass* lors d'un simple contrôle par un agent de la circulation ou par un vendeur de magasin accueillant un client, mais non équipé de *Google Glass*...

Identification des vulnérabilités au niveau du système

Parallèlement, une approche analytique de la sécurité pourra être menée.

La première étape est l'identification des composants vulnérables.

Dans le cadre d'une démarche *top down*, une perspective physique fournira une décomposition faisant apparaître l'objet et une représentation en couches apportera une perspective fonctionnelle.

Pour une organisation physique du système, on pourra suivre une modèle en trois couches (*Service Domain, NGN Domain, Device Domain*[99]).

(99) UIT-T Y.2061.

Pour la perspective fonctionnelle, on pourra s'appuyer sur les standard émergents IoT définissant deux couches « le monde physique » et le « monde de l'information ». Mais également, on pourra reprendre les référentiels éprouvés tel que ceux proposés sur le site de l'ANSSI, qui distinguent la couche « bien essentiel » et la couche « bien support »[100].

(100) Menaces sur les systèmes informatiques, Guide 650, SGDN Premier Ministre, Sept 2006.

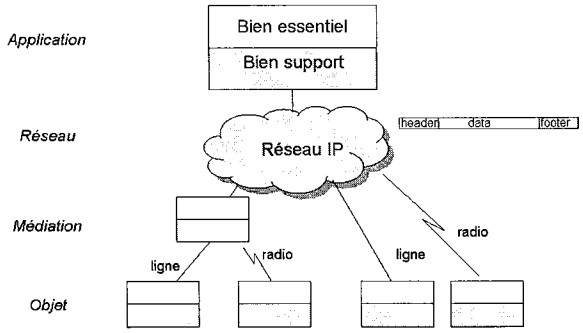


Schéma d'identification des vulnérabilités

	Définition	Description / caractérisation
Objet	Objet connecté à un système d'information ou un système industriel	Nature de l'objet Interface humain Fonctions Capteur Actionneur Interface de communication Interaction avec un système
Bien essentiel	Information du patrimoine de l'entreprise, porteur de besoins de sécurité	Information nominative (contractuelle, privée…), administrative et financière, professionnelle et / ou technique (savoir-faire, recherche, projet métier), commerciale, scientifique.
Bien support	Composant du système sur lequel repose des éléments essentiels et sur lequel peuvent porter des menaces	logiciels matériels réseaux sites organisations personnes

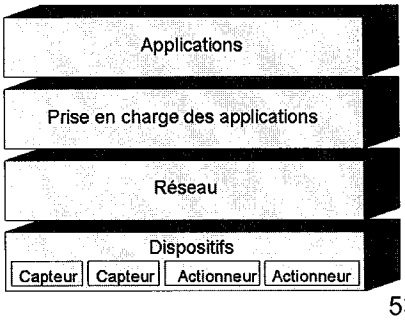
Grille d'analyse d'un système Objet Connecté

Un tel cadre fera aisément apparaître des composantes essentielles d'un Objet Connecté sur lesquelles les analyses opportunités/risques d'affaires reposeront: par exemple, en cuisine connectée, ce sera un catalogue de recettes de cuisine, en maison connectée, un répertoire de procédures d'intervention en cas d'incident sécurité définies par les clients, et en corps connecté, des informations de santé, d'alimentation et de durée de vie.

Identification des vulnérabilités au niveau de l'objet

Un deuxième niveau d'identification sera au niveau de l'objet. En s'appuyant sur les standards émergents, on pourra faire figurer quatre couches: la couche application, la couche de prise en charge des applications, la couche réseau, et la couche dispositif [101].

(101) UIT-T Y.2060.



Identification des vulnérabilités au niveau des usages

Connectés au système d'information de l'entreprise, les objets introduisent des vulnérabilités nouvelles, notamment du fait de leur usage qui porte sur les biens essentiels du système d'information accessibles *via* l'objet et les modalités d'emploi de l'objet.

Pour une grande entreprise menant plusieurs projets objets connectés, une typologie des biens essentiels et des modalités d'emploi peut être intéressante.

Biens essentiels	• Information privée • Information d'entreprise • Information littéraire • Information artistique • Savoir-faire artisanal • Savoir-faire industriel
Modalités d'emploi	• adressable avec IP : oui/non • énergétiquement autonome : oui/non • connexion sous demande humaine ou automatique • transmission de données sous supervision humaine ou automatique • modification d'état de l'objet sous supervision humaine ou automatique

Conditions renforcées d'utilisation des services

Enfin, pour les adresser spécifiquement, on pourra extraire les clauses afférentes aux les conditions d'utilisation des *Service Level Agreement*, qui désignent souvent dans les référentiels de management de système d'information des accords de niveau de service.

Pour marquer ce changement de gouvernance, la formule de *User Level Agreement*[102] pourra être introduite dans les référentiels de management informatique.

(102) Aligner la gouvernance des systèmes d'information sur la stratégie de l'entreprise, Tru Dô-Khac, la Jaune et La Rouge, Janvier 2007.

Évolution des représentations collectives de la fonction SI

Les représentations collectives d'un groupe social sont construites à partir des règles et des valeurs reconnues dans le groupe. Elles ont pour rôle d'orienter les individus dans leur perception du monde social qui les entoure et dans les actes qu'ils accomplissent. Selon les auteurs, elles naissent soit de l'agrégation des consciences individuelles qui portent, chacune et préalablement, ces représentations, soit de raisons d'agir qui sont collectivement repérables dans le groupe[103]. Dans les deux cas, elles sont à la fois un levier et un frein au changement.

Le modèle dit « Maîtrise d'ouvrage-Maîtrise d'œuvre » (MOA-MOE) est une représentation collective de la fonction système d'information. Cette représentation porte la croyance que la relation client fournisseur entre

(103) Les représentations collectives, Marc Audebert, Institut de sciences humains appliquées, Les carnets du temps N°105, avril 2014, Enseignement militaire supérieur Air.

une direction métier et la direction des systèmes d'information est source d'alignement des systèmes d'information sur la stratégie de l'entreprise. Ainsi le modèle reconnu dit «*Strategic Alignment Model*» (SAM) de N. Venkatraman et de J.C Henderson [104] éclaire les interactions d'une relation client fournisseur entre l'entreprise («*business*») et la direction des système d'information («*Information Technology*») [105].

Également, le «*Service Level Agreement*» (SLA) est une représentation collective qui vise à la définition et au contrôle conjoint par le client et le fournisseur des niveaux de service.

Avec les objets connectés, le rôle de l'usager devient aussi déterminant que le rôle du client et du fournisseur.

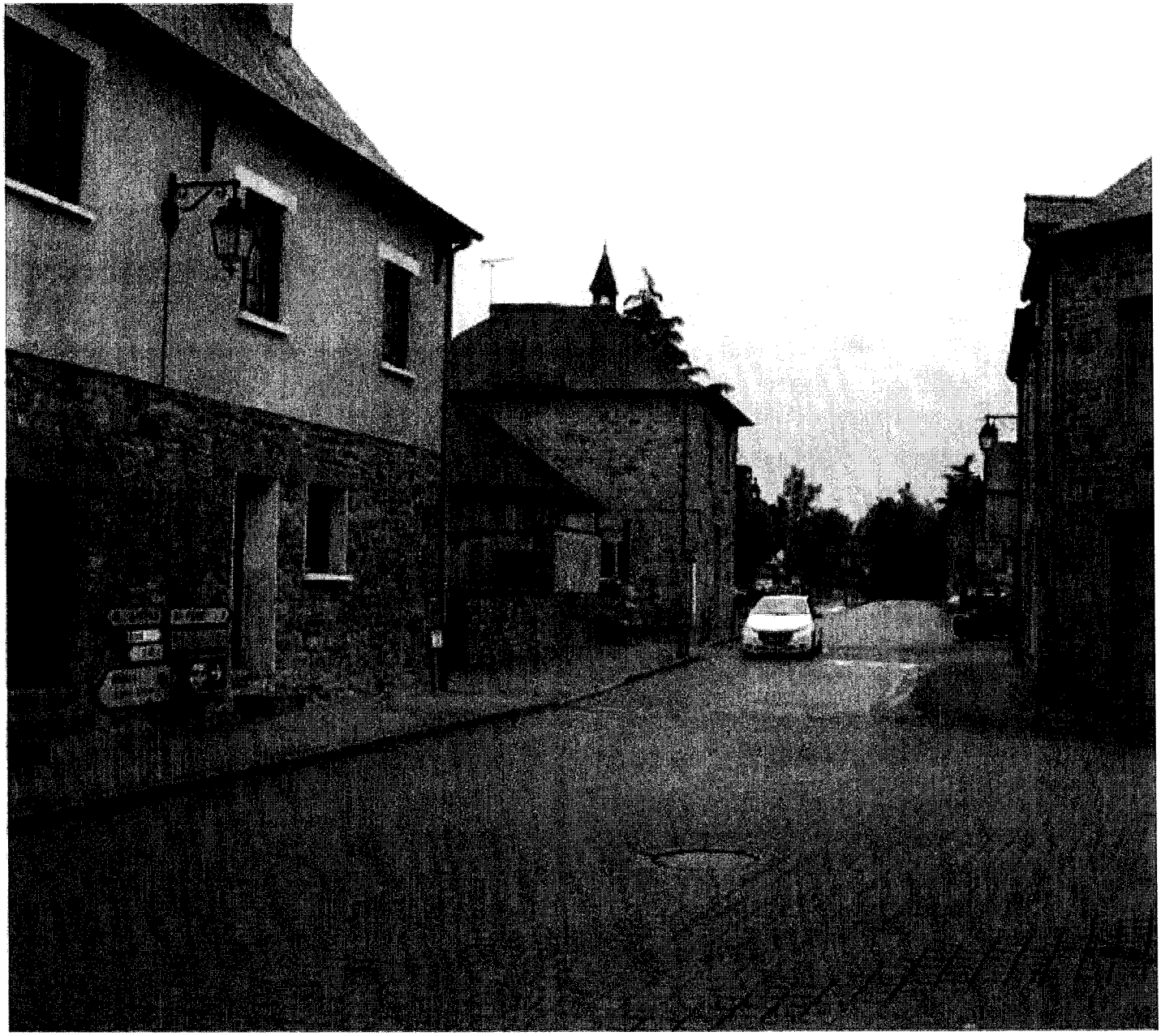
On peut s'attendre que les représentations collectives Maîtrise d'ouvrage-Maîtrise d'œuvre et *Service Level Agreement* soient aménagées pour les directions de systèmes d'information qui seront partie prenante de projet de systèmes d'information connectés à des objets [106].

(104) Strategic alignment: leveraging information technology for transforming organisations, J.C. Henderson et N. Venkatraman, IBM Systems Journal, 1999.

(105) Aligner les systèmes d'objets connectés avec la stratégie de l'entreprise, Tru Dô-Khac, Le Cercle Les Echos, 13 juin 2014.

(106) La maîtrise d'usage pour aligner les objets connectés sur la stratégie de l'entreprise, mini MOOC produit par Dô-Khac Decision, 2014.

(...)



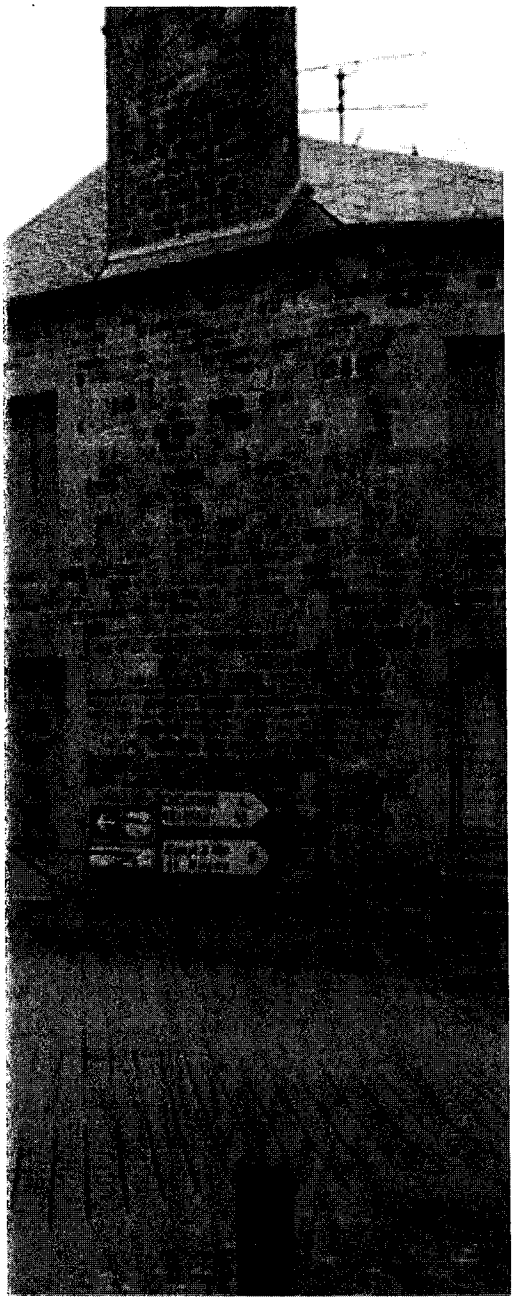
Saint-Sulpice-la-Forêt

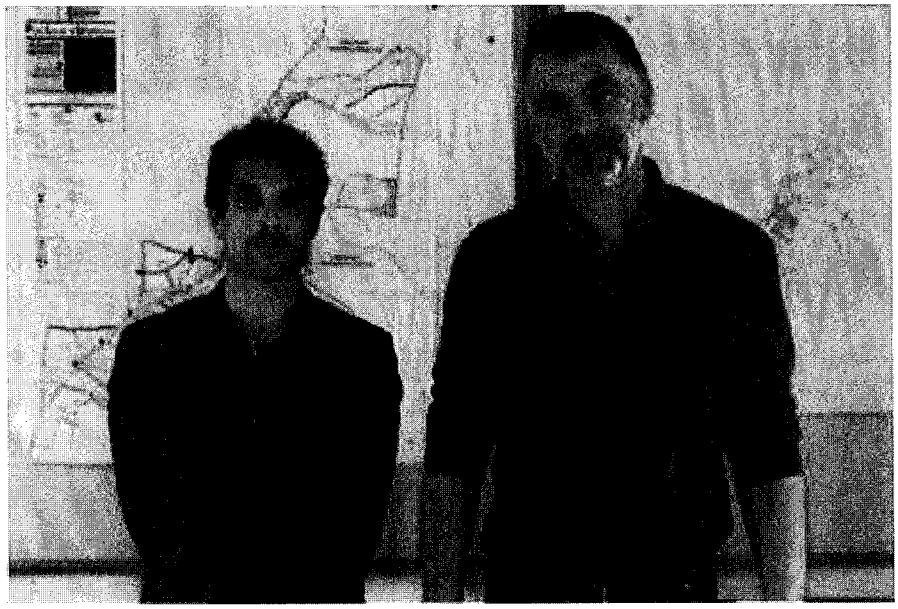
Le village breton devenu smart city

SURNOMMÉE LA « START-UP » DE RENNES MÉTROPOLE, la petite commune de Saint-Sulpice-la-Forêt a lancé un projet d'optimisation énergétique de ses bâtiments municipaux. Grâce aux technologies Cloud et à l'Internet des objets (IoT), la consommation énergétique des bâtiments sera surveillée en temps réel et le chauffage piloté à distance. Un projet qui ne coutera que 20 000 euros à la commune.

« *Il n'y a pas que les grandes villes qui peuvent devenir des smart cities* », lance Yann Huaumé, maire de Saint-Sulpice-la-Forêt. Ce village de 1500 habitants, situé à une quinzaine de kilomètres de Rennes, entend bien s'inscrire pleinement dans la mouvance des villes intelligentes. Son projet *"Smart Saint Sulpice"* attire aujourd'hui l'attention de nombreuses collectivités avoisinantes, à commencer par Rennes Métropole, qui soutient l'initiative.

Ce projet prévoit l'optimisation de la consommation énergétique des six bâtiments communaux, grâce au Cloud et à l'internet des objets. « *Notre volonté politique est de faire participer Saint-Sulpice-la-Forêt aux grands enjeux de société, à commencer par l'écologie. C'est pourquoi nous avons signé la convention des maires pour le climat et l'énergie, dans le cadre de la COP 21. Notre engagement est de faire baisser de 20 % notre consommation énergétique et de nos émissions de CO2 d'ici 2020. Grâce au projet Smart Saint Sulpice nous devrions y parvenir en seulement deux ans* », poursuit ce jeune maire de 39 ans, élu en mars 2014.





Yann Husumé, Maire de Saint Sulpice la Forêt, élu en 2014, et Benoit Vagneur, adjoint en charge des finances, de l'urbanisme et de la communication de la ville.

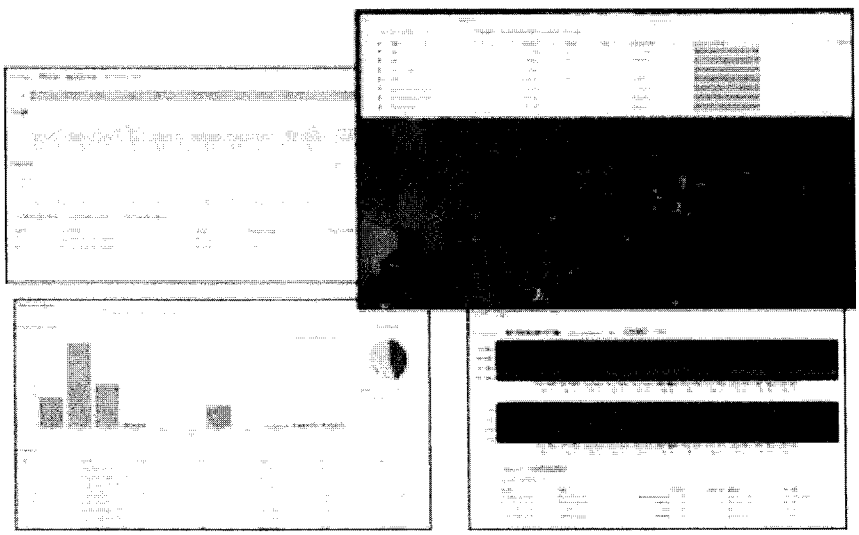
SAINT-SULPICE-LA-FORÊT : CHIFFRES CLÉS

Population 1 483 habitants au 01/01/2015 (source INSEE)	**Superficie** 6,72 km²
Densité 220 hab./km²	**Logements** 98 % en maison (2012-source Insee)
Âge moyen 36 ans	**Revenu moyen** 45 000 euros par ménage

Mais avant de lancer ce projet ambitieux, Saint-Sulpice-la-Forêt a dû commencer par engager une transformation numérique complète de ses services et outils. « *Nous sommes partis de très loin* », se rappelle Benoit Vagneur, adjoint en charge des finances, de l'urbanisme et de la communication. Le système d'information municipal était pour le moins vetuste : les élus utilisaient leurs e-mails personnels pour communiquer ; le site internet de la ville, développé six ans auparavant par un élu et hébergé à Marseille, était totalement obsolète ; le serveur hébergeant les applications métier n'était pas sécurisé et directement connecté à une box grand public ; les accès internet de la municipalité plafonnaient à 2 Mb/s… « *Notre premier travail a été de moderniser le SI de la commune, en nous inspirant de ce nous utilisions au quotidien dans nos différentes activités professionnelles* », poursuit Benoit Vagneur.

Passage à Google Apps for Works

Deux mois après son élection, la nouvelle équipe décide de déployer *Google Apps for Works* afin de disposer d'une messagerie professionnelle. La suite bureautique en ligne de Google intègre les outils classiques : Gmail, espace de stockage Google Drive, visioconférence Hangouts, agenda… complétés par des fonctions de partage entre groupes d'utilisateurs. Si elle offre donc de nombreux avantages techniques, cette solution Cloud est hébergée chez Google, sur des serveurs localisés notamment aux États-Unis. Quid de la protection des données sensibles de la commune ? « *Nous avons débattu de ce sujet. Les données régaliennes, telles que l'état civil ou le budget, restent en dehors du Cloud, et sont hébergées sur un serveur local de la mairie* », précise l'équipe municipale.



Différents tableaux de bord permettent à l'équipe municipale de suivre le fonctionnement et les performances du réseau

Refonte complète du site internet de la commune

Autre modernisation : le site internet de la commune est transformé en « *portail de services* ». « *Une smart city c'est aussi une ville capable d'échanger des infor-*

mations avec les citoyens grâce au numérique. C'est la raison d'être de ce nouveau site », poursuit Yann Huaumé.

Mis en ligne en novembre 2014, *« Saint-sulpice-la-foret.fr »* propose désormais des informations publiées directement par les associations. Le portail intègre également des outils de communication entre citoyens, notamment autour du covoiturage ou du baby-sitting. À la demande des administrés, un dispositif d'inscription en ligne à la cantine et la garderie a été développé. Côté parents, un changement d'inscription peut désormais être réalisé avec un préavis de seulement 24 h pour la cantine et la vielle pour la garderie, contre trois jours auparavant. Côté mairie, ce service web permet une gestion des factures de cantine et de garderie en quelques minutes au lieu de quatre jours au temps du traitement papier. *« Cela paraît anecdotique, mais nous avons de nombreuses demandes d'information autour de ce service de la part d'autres collectivités »*, précise Benoit Vagneur. Pour réaliser ce nouveau site, la collectivité fait appel à deux professionnels indépendants vivant sur la commune. Il repose sur le système de gestion de contenu (CMS) Joomla et a été réalisé avec une architecture en *« responsive design »*, afin de pouvoir s'adapter à une consultation sur tablettes et smartphones.

Modernisation de l'infrastructure réseau

Autre étape incontournable pour devenir une smart city : disposer d'une infrastructure réseau digne de ce nom. Le réseau de la mairie était resté en ADSL à 2 Mbit/s. La nouvelle équipe décide donc de passer au VSDL à 20 Mbit/s. *« Nous avons simplement changé d'offre chez Orange »*, confie Benoit Vagneur. Pour résoudre les problèmes de sécurité et ajouter un filtrage de contenu sur les ordinateurs de l'école : une couche VPN (*Virtual Private Network*) est également intégrée au réseau. Enfin, la commune déploie six hotspots WiFi pour que les citoyens et les associations puissent se connecter gratuitement au net. *« Nous avons un gros problème de couverture 3G sur la commune. Un seul opérateur, en l'occurrence SFR, couvre correctement notre territoire. Proposer des accès WiFi était donc une réponse à cette problématique »*, précise Benoit Vagneur. Cette évolution de l'infrastructure réseau a été réalisée entre octobre et décembre 2015, principalement avec l'opérateur télécom Orange. Aujourd'hui, environ 200 utilisateurs par semaine se connectent à ces hotspots WiFi municipaux.

Les locaux et un des capteurs (ci-dessous de Wi6Lab), l'une de s start ups locales, spécialiste de l'Internet des Objets, qui accompagne la commune dans le déploiement de ses dispositifs smart city

Optimisation des dépenses énergétiques

Parallèlement à ces modernisations des principaux outils et services municipaux, la nouvelle équipe décide de s'attaquer à un problème récurrent de la commune : sa consommation énergétique au-dessus de la moyenne. Cette consommation est générée à 80 % par six bâtiments communaux : l'école, la marie, le centre culturel, la salle polyvalente, la salle de sport et le local de services techniques.

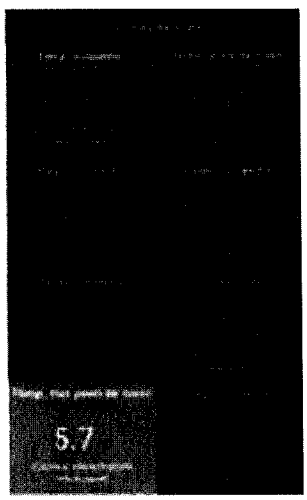
« Nous avons identifié plusieurs défaillances techniques, comme une fuite d'eau à la salle polyvalente correspondant à 26 piscines qui se sont vidées en huit à neuf mois », se rappelle Benoit Vagneur. Autre exemple : le disjoncteur de panneaux photovoltaïques permettant à la commune de produire une partie de son électricité avait sauté pendant six mois, sans que personne ne s'en rende compte.

Mais le principal problème reste la gestion du chauffage de ces bâtiments, qui est très loin d'être optimal. *« Quand ils existent, les équipements ne permettent pas de programmer le chauffage en fonction des besoins »*, observe ainsi l'équipe de Yann Huaumé. L'école est par exemple chauffée à 21°, les jours de classe, la nuit, le week-end… et pendant les vacances.

Un coût trop élevé pour moderniser les équipements existants

« Notre problématique était la suivante : comment réduire notre consommation énergétique de 20 % avec seulement 20 000 euros de budget », résume Yann Huaumé. La commune envisage d'abord de changer certains équipements, notamment les automates de chauffage, afin de pouvoir piloter leur consommation. Mais les tarifs proposés par les équipementiers se révèlent trop élevés. *« Rien que pour l'école, il fallait entre 20 000 et 30 000 euros pour mettre à jour le réseau électrique afin de pouvoir le piloter »*, précise Benoit Vagneur.

L'équipe municipale cherche alors une alternative. Et c'est en rencontrant des représentants d'une start-up locale : Wi6Lab que leur vient l'idée d'exploiter l'internet des objets. Cette jeune pousse, d'une dizaine de personnes, s'est spécialisée dans les réseaux privés pour l'IoT à destination des entreprises. Il s'agit de réseaux radio à longue portée et



Une appli sur smartphone permet aux gestionnaires de la ville de suivre les consommations de la commune, de suivre les différents capteurs et de recevoir des alertes.

à basse consommation (en technologie LoRaWan). Wi6Lab conçoit également les petits capteurs sans fil qui permettent de réaliser les mesures à distance via le réseau IoT. « *Nous nous sommes dit : ces capteurs pourraient être installés dans les bâtiments administratifs de la ville pour collecter des données de consommation en énergie sans devoir déployer une lourde infrastructure de communication* », indique Benoit Vagneur. De plus, d'autres petits modules radio, fonctionnant aussi sur réseau IoT, sont capables d'actionner des équipements à distance. Ces « *actuateurs* » permettraient en l'occurrence de piloter les automates de chauffage.

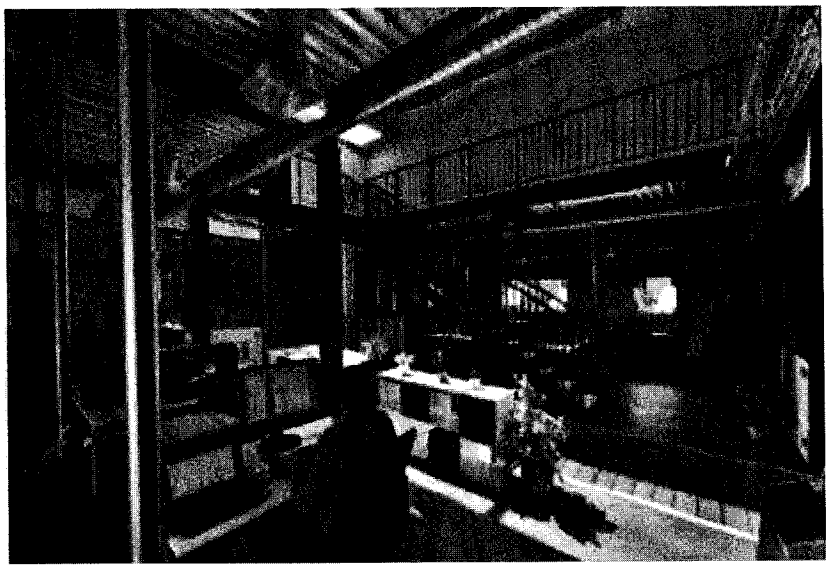
À ce stade, l'équipe municipale semble avoir trouvé une partie de la solution. Reste à développer une solution pour exploiter les données collectées par ces capteurs et piloter à distance les équipements de chauffage. Il se trouve qu'une autre entreprise locale, Alkante, est spécialisée dans le développement de logiciels métier, notamment pour les collectivités. Après une rencontre avec l'équipe municipale, elle confirme être en mesure d'adapter une de ses plateformes logicielle dans le Cloud aux besoins du projet « *Smart Saint Sulpice* ».

Le budget serré de la commune n'arrête pas ces deux entreprises, qui acceptent de financer la majeure partie du projet (lire encadré ci-contre), car elles y trouvent également un intérêt. « *Ce projet va nous permettre de développer nos compétences dans la gestion de données en temps réel sur les systèmes d'information de collectivités* », indique François Leprince, directeur associé d'Alkante. « *Nous allons pouvoir développer une offre pour les collectivités, un marché que nous ne couvrons pas encore* », confie pour sa part Anthony Crolais, COO de la jeune pousse.

L'équipe de Yann Huaumé fait également appel à l'Alec du pays de Rennes (Agence locale de l'énergie et du climat), qui fournira une aide « *pédagogique* » très utile dans la gestion de l'énergie, nouveau domaine pour l'équipe municipale. Enfin, Rennes Métropole est contactée et accepte également de financer une partie du projet sous la forme d'une avance remboursable.

Un réseau IoT privé

Depuis le printemps 2016, une cinquantaine de capteurs sont en cours d'installation dans les six bâtiments de la ville. Durant les mois à venir, ils vont permettre de collecter des informations précieuses sur les consommations en électricité, eau, gaz et fioul. Ils vont également relever les températures et le taux d'humidité dans les locaux. À la fin 2016, le projet passera à la phase de pilotage du chauffage, fort des informations collectées durant les mois précédents. Six « *actuateurs* » seront installés dans les bâtiments pour piloter les équipements de chauffage.



Pour communiquer, ces capteurs utiliseront un réseau radio privé. Pourquoi un réseau privé et non celui de Sigfox, Orange ou Bouygues Telecom, qui déploient chacun leur réseau dédié à l'IoT ? « *Ces réseaux de grands opérateurs ne couvrent pas notre territoire et se concentrent sur les zones urbaines denses* », explique Benoit Vagneur. De plus, Saint-Sulpice-la-Forêt entend rester maître des données collectées dans le cadre de son projet IoT. Un réseau privé est donc la meilleure solution. « *Nous sommes responsables de ces données et nous en sommes propriétaires* », poursuit l'élu. Un partage de ces données en open-data est prévu. Mais il reste encore à définir comment ces données seront partagées afin de leur donner du sens, indique l'équipe municipale.

Déjà un impact « psychologique » de 5 %

Avant même que le système ne soit totalement opérationnel, le projet IoT porte déjà ses fruits. « *Le simple fait de mettre ce projet dans l'agenda a changé certains comportements et nous avons déjà une baisse de l'ordre de 5 % sur nos factures depuis quelques mois* », confie Benoit Vagneur. Pour l'équipe municipale le projet est « *bien engagé* ». Elle table sur un retour d'investissement en moins de cinq ans. « *Les 20 % d'économie attendus représentent un gain de l'ordre de 10 000 euros chaque année. Cette somme, nous allons l'investir pour optimiser encore d'avantage notre consommation énergétique, en réalisant des travaux d'isolation sur nos bâtiments. Et grâce aux données collectées, nous saurons exactement où investir afin que l'isolation thermique soit la plus efficace possible* », conclut Yann Huaumé.

CHRISTOPHE GUILLEMAIN

Alkante, entreprise locale spécialisée dans le développement de logiciels pour les collectivités, a adapté une de ses plateformes logicielles dans le Cloud aux besoins du projet « Smart Saint Sulpice ».

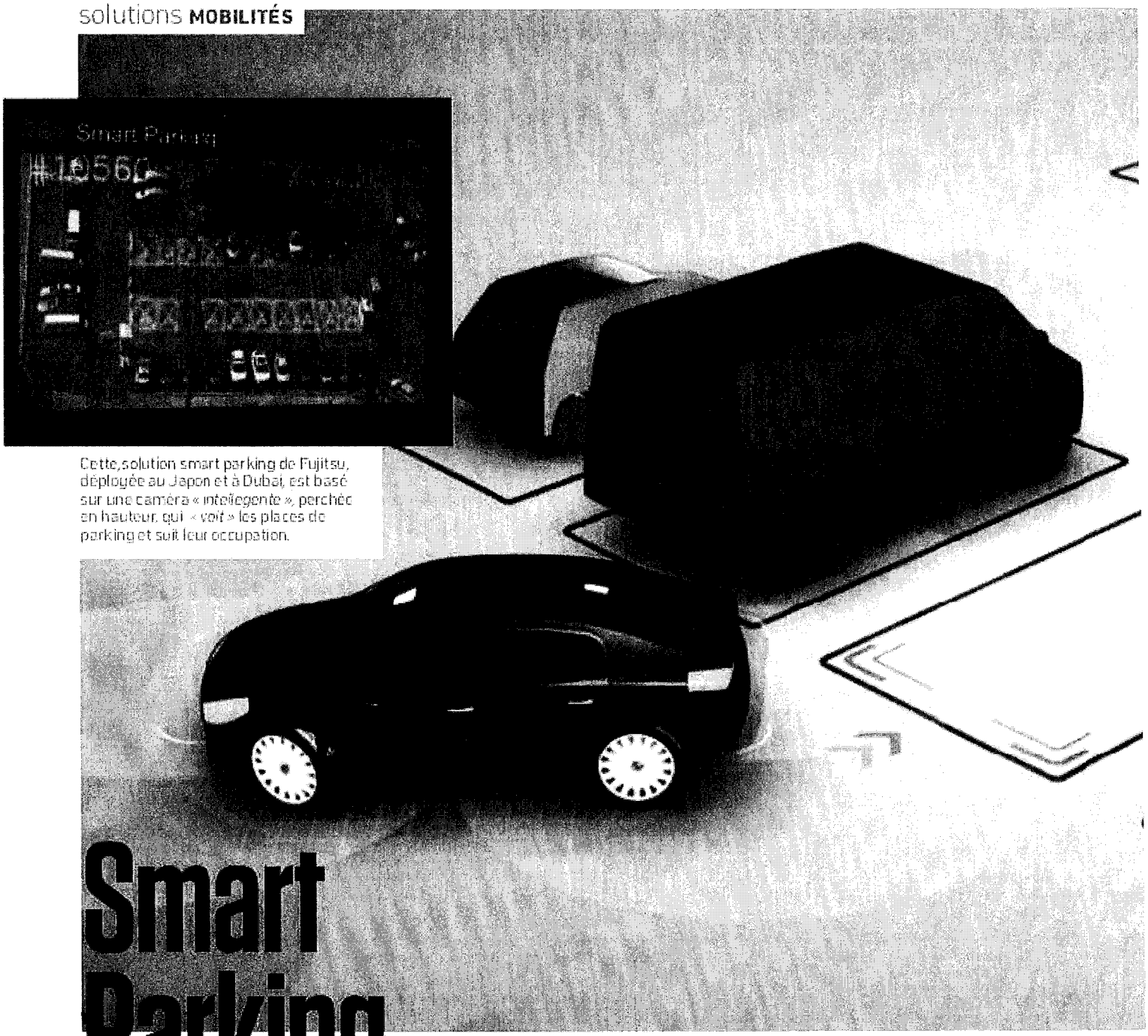
BUDGETS DES PROJETS

Passage à Google Apps for Works
3 400 €
au départ (formation des 25 agents et élus + une première année d'accès aux services), puis 1000 euros par an

Refonte du site internet
11 000 €
au départ, dont 3 000 euros pour le module de gestion de la cantine et garderie, puis 1500 euros par an de maintenance et 200 euros d'hébergement chez OVH

Modernisation du réseau
9800 €
dont 2800 euros pour le déploiement des six hot-spot WiFi, puis 1800 par an (accès 20 Mbit/s)

Smart Saint Sulpice
110 000 €
dont 20 000 euros financés par la commune par l'achat des capteurs. Les 90 000 euros restant sont pris en charge par Wi6Labs (50 000) et Alkante (40 000) avec une aide de Rennes Métropole sous la forme de 45 000 euros d'avance remboursable (dispositif d'aide à l'innovation Rennes Saint Malo Lab)



Cette solution smart parking de Fujitsu, déployée au Japon et à Dubai, est basé sur une caméra « intelligente », perchée en hauteur, qui « voit » les places de parking et suit leur occupation.

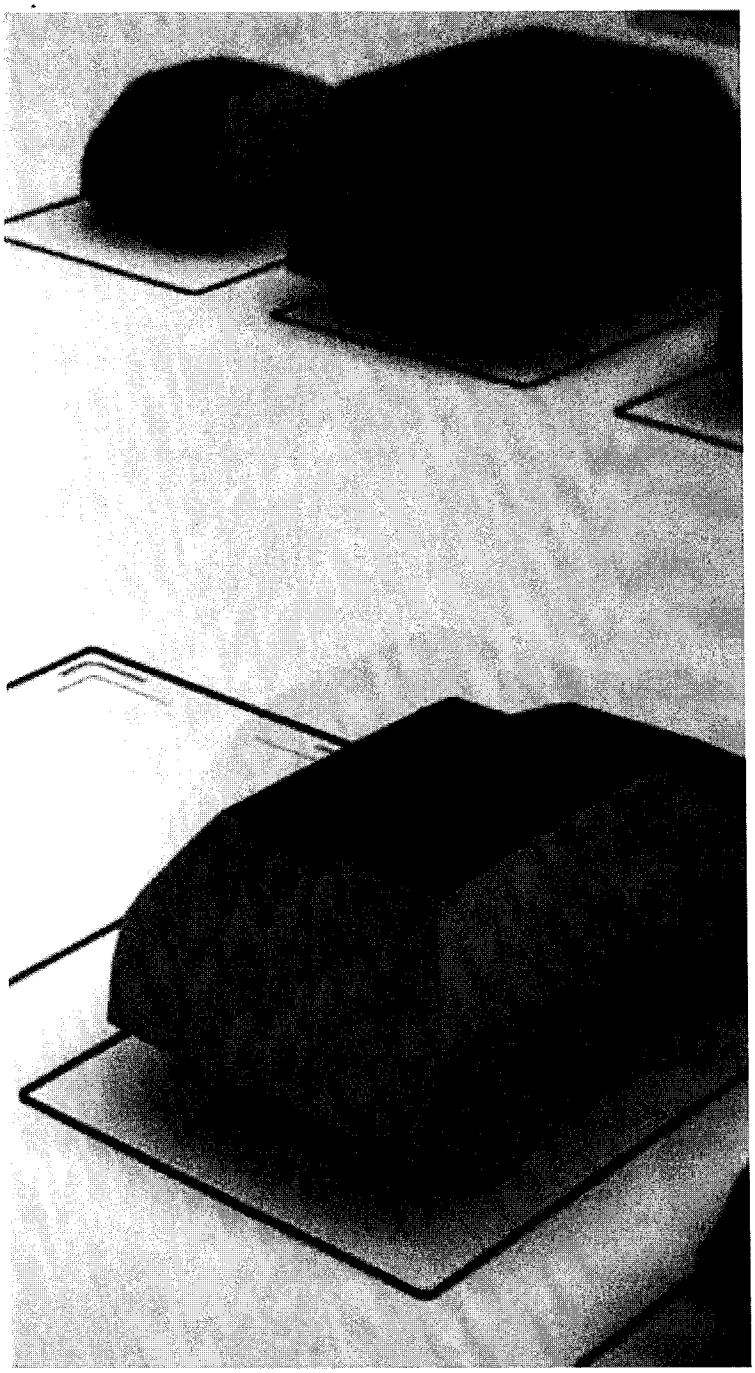
Smart Parking

18 mois pour ré-inventer le stationnement

PLUS DU QUART DE LA CIRCULATION AUTOMOBILE DANS LES VILLES EST À METTRE SUR LE COMPTE DES AUTOMOBILISTES QUI CHERCHENT À SE GARER. Une quête qui provoque encombrements, pertes de temps colossales et pollution. Or, en apportant un peu d'*« intelligence »* aux systèmes de stationnement, on peut limiter ce temps de recherche et ses nuisances, facilitant par la même occasion la vie des citoyens. Mais les solutions de *« smart parking »* qui s'offrent aux collectivités diffèrent tant pour leur approche technique que pour leur coût, très variable. Dès lors, alors que la réforme du stationnement entrera en vigueur en 2018, vers quelle(s) solution(s) s'orienter ? Suivez le guide.

Centres villes saturés, amendes de stationnement distribuées à tour de bras mais rarement payées, agents municipaux massivement mobilisés à faire la police du stationnement… Autant de maux dont souffrent les villes françaises et auxquels la *« réforme du stationnement payant sur voirie »*, adoptée en 2014 dans le cadre de la loi de modernisation de l'action publique territoriale et d'affirmation des métropoles (Mapam), vise à apporter des réponses.

Cette disposition, qui consacre la décentralisation de la gestion du stationnement public, vise aussi à *« dépénaliser »* la question du stationnement payant en supprimant l'amende forfaitaire de 17 €. Les élus locaux disposeront de davantage de latitude pour piloter leurs politiques de stationnement, tant sur le plan des modes de gestion que de la stratégie tarifaire. Et dans ce nouveau cadre, la plupart des collectivités moyennes et petites peuvent s'attendre des recettes potentielles non négligeables. Initialement programmée pour s'appliquer le 1er janvier 2016, la



Les capteurs placés dans le sol détectent la présence (ou l'absence) d'une voiture au dessus d'eux et communiquent l'information par radio bas débit (via des réseaux de type LoRa, Sigfox...) au serveur qui gère le système. L'historisation de ces données permet au système d'« apprendre » quels sont les jours et les heures récurrents d'occupation des places et de communiquer à l'utilisateur l'information.

L'application Parker, qui permet de guide l'automobiliste vers des places de stationnement disponibles.

réforme du stationnement, a été reportée de deux ans au 1er janvier 2018. Un délai que les collectivités pourront mettre à profit pour explorer de nouveaux concepts de « *parking intelligent* ». L'ère du digital ouvre en effet la voie à de nouvelles formes d'organisation et de gestion du stationnement, public comme privé, qui combinent la mise en oeuvre de capteurs connectés à internet, l'usage d'applications mobiles, et le traitement des données générées par les outils du Big Data.

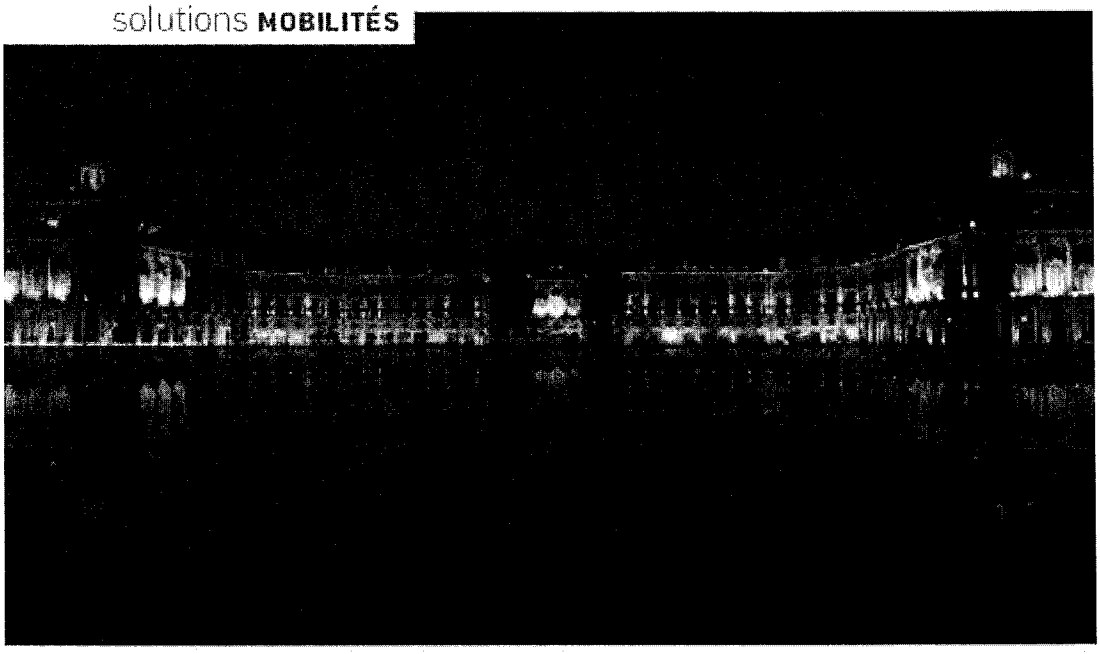
Avec ou sans capteurs ?

L'option « *avec capteurs* » est une possibilité à étudier. Ces dispositifs qu'on implante dans le sol permettent de détecter la présence ou non d'un véhicule sur une place de stationnement. Les offres industrielles existent : Orange Labs a repéré ceux de la société californienne StreetLine, un des leaders mondiaux du secteur.

Aximum, filiale de Colas, a conçu des capteurs de nouvelle génération : directement associables au paiement, avec suivi d'une politique de tarification, ils peuvent contribuer à gérer des places spécifiques (PMR, Véhicule électrique, etc..) ainsi que divers services (calcul d'itinéraire de porte à porte en multimodal, réservation de place, gestion de statistiques, etc).

Bosch a également présenté un modèle de capteur basse consommation adapté aux places de stationnement. Lui aussi transmet des informations en temps réel à des serveurs. On peut y accéder via une application mobile. Le système peut être couplé à un dispositif de géolocalisation d'intérieur à base de 'beacons' pour orienter les véhicules dans les parkings couverts.

Signalons au passage que le prix de ces capteurs est extrêmement variable : celui d'Aximum est de l'ordre de 50 € l'unité, mais on trouve aussi ceux du chinois Huawei qui devraient arriver sur le marché à moins de 5 euros. Les prix des capteurs ne représente de toutes façons qu'une partie de l'investissement nécessaire.



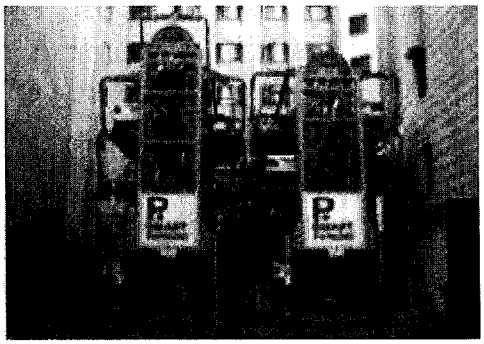
Bordeaux mise sur le « tout numérique »

Bordeaux Métropole s'est substitué au 1er janvier 2015 à la Communauté Urbaine, qui exerce depuis 1968 la compétence de gestion et d'exploitation des parcs de stationnement hors voirie. Bordeaux compte 17 750 places en ouvrage exploitées par Bordeaux Métropole et 12 300 par d'autres gestionnaires. « Depuis plusieurs années, la fréquentation des parcs publics s'est stabilisée après la mise en service du tramway (3 lignes totalisant 60 km) et le report modal induit, et ce malgré des tarifs restant supérieurs à ceux du stationnement de surface », explique Eric Monceyron, chef de mission ITS, direction du pôle Mobilité. L'apport du numérique permet désormais d'élargir leur application au stationnement en voirie : l'utilisateur peut payer son stationnement occasionnel à partir de son téléphone mobile, et prolonger la durée à sa guise après réception d'une alerte. Ce service est opéré par Urbis Park et Mobile City (5 parkings délégués)

Des applications innovantes : Citypark et Parking Facile

Le démonstrateur Citypark développé par la société Qucit4, est un exemple récent de gestion dynamique. Il utilise des algorithmes d'intelligence artificielle (machine learning et Big data) et offre ainsi des capacités de calcul prédictif : temps nécessaire pour stationner selon différentes options (en surface ou en ouvrage, avec parcours final à pied) et comparaison de coûts. Des historiques de données sont exploitées pour calibrer le lien entre les variables contextuelles (météo, circulation, événements, ...) et le temps de recherche optimisé. Il vise à intégrer le stationnement dans la chaîne de déplacement, soit en rabattement soit à destination, avec un temps estimé complet. Le consortium conduit par Qucit comprend les opérateurs du stationnement, Parcub et Urbis Park, ainsi que la start-up Parking Facile. Cette dernière, à partir d'une plateforme mobile, gère un portefeuille de places de parkings – notamment auprès de bailleurs sociaux ou d'institutionnels, avec des tarifs incitatifs. Des boîtiers émetteurs/récepteurs, pilotés par la plateforme, opèrent l'ouverture et la fermeture des parkings.

> « Les capteurs sont une solution parmi d'autres technologies possibles. On voit se profiler des systèmes avec radars ou scanners embarqués qui collectent la plupart des données utiles ».
>
> **Eric Monceyron,** chef de mission ITS direction du pôle mobilité de Bordeaux Métropole



Une approche « smart » pour gagner de l'espace : garer les voitures dans des carrousels qui les stockent en hauteur.

L'intérêt des capteurs, c'est surtout celui des données qu'ils génèrent et qui sont mises en valeur à l'aide de solutions du type Big Data ou BI (*Business Intelligence*, comme Cognos d'IBM). Ainsi retraitées, les données permettent par exemple de prédire, en fonction des horaires, à quel endroit les automobilistes sont susceptibles de trouver des places de stationnement libres.

A Troyes (cf encadré ci contre), les 220 capteurs installés avec Orange, en centre-ville, sont couplés à un logiciel (Parker) de gestion des places de stationnement. A St-Amand-Montrond (Cher), les données issues des capteurs permettent d'alerter les autorités sur la présence de véhicules « *ventouse* », qui restent immobilisés à la même et nuisent ainsi entre autres à dynamique du commerce des centres ville.

Mais tout n'est pas parfait avec les capteurs. A Nice, par exemple, on s'est rendu compte que les véhicules ne se rangent pas sur des places fixes, marquées au sol. Et donc que le capteur indique une place libre alors qu'il se trouve entre deux véhicules...

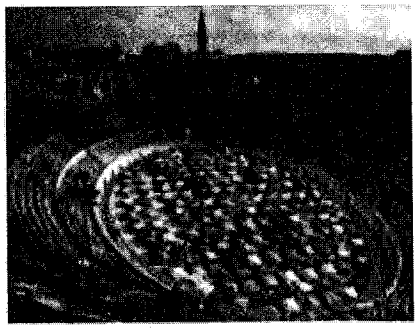
« *Les capteurs sont une solution parmi d'autres technologies possibles*, commente Eric Monceyron, chef de mission ITS direction du pôle mobilité de Bordeaux Métropole. *On voit se profiler des systèmes avec radars ou scanners embarqués qui collectent la plupart des données utiles* ».

La profusion des applications mobiles

En fait, les capteurs et les données qu'ils génèrent prennent réellement leur dimension lorsqu'ils sont relayés par des applications mobiles. 'Path to park' (de Parkeon, fabricant de parcmètres) est une solution prédictive, avec des algorithmes du type

Nîmes Un observatoire du stationnement pour mieux piloter

Nîmes possède une offre de stationnement relativement bien dimensionnée pour une ville de 150 000 habitants, avec 10 000 places publiques dans le centre-ville - soit environ 30 places à l'hectare - se répartissant entre 3 200 places payantes et 2 000 places gratuites sur voirie, et 4 800 places dans 9 parkings en ouvrage. Le paiement dématérialisé a été mis en place avec le système Pay by phone. Un observatoire du stationnement a été institué en 2013, véritable outil de suivi du stationnement basé sur la collecte de données de terrain et de statistiques d'exploitation de la voirie payante et des parkings. Au regard du faible taux de rotation des véhicules sur voirie, des bornes arrêt minute ont été implantées à l'intérieur du périmètre payant. Le stationnement y est gratuit et limité à 15 minutes, après quoi la police municipale est alertée par email. Les résultats sont spectaculaires : le taux de rotation atteint 20 à 25 véhicules par place et par jour. La deuxième étude extraite de l'observatoire a trait au contrôle du stationnement. Les enquêtes annuelles de terrain ont révélé que le niveau de respect à Nîmes est très hétérogène et en baisse depuis 2010. La valeur de cet indicateur à Nîmes reste toutefois comparable à la moyenne nationale, soit 30 %. Le suivi des résultats permet de vérifier l'action du contrôle et de l'adapter en appliquant un contrôle géographique ciblé si besoin. En outre, la



verbalisation électronique a été mise en place en 2014, et de nouvelles perspectives sont également ouvertes par la vidéo-verbalisation, notamment pour les arrêts gênants.

'machine learning', travaillant à partir des données des horodateurs ; elle oriente les automobilistes vers des zones de stationnement disponibles. 'Parker' (utilisé à Troyes) recense également les parcs enclos ou ouvrages et permet de consulter les tarifs en vigueur avant de déclencher le guidage vocal. La ville de Lyon fait figure de précurseur avec la mise en place de deux projets logiciels d'envergure Optisur et Optimod (sur horodateurs Parkeon), pour améliorer la gestion du stationnement. Le premier assure la surveillance et le contrôle du stationnement de voirie (sur une base Prédit et Parkeon) ; et le second évalue la fiabilité et la pertinence des informations remontées par les capteurs. Il en est résulté que les capteurs ne sont pas parfaits pour un service de guidage vers des places libres.

Brassage avec l'Open Data

D'autres données peuvent avantageusement alimenter ce genre de *'smart'* applications : ce sont celles de l'Open Data, c'est à dire, celles qui constituent un « *intérêt public général* ». Dans le cas des délégations de service public (DSP), la responsabilité des autorités concédantes doit être établie en matière de diffusion des données, dès lors qu'elles sont à la fois propriétaires des données et des parcs. Cette ouverture des données publiques doit être neutre, sans risquer de privilégier certains acteurs. « *Le parking est une dimension de la mobilité, au sens global. Et il ne peut pas y avoir de stationnement intelligent sans ouverture des données* », souligne Mathieu Caps, responsable Public affairs chez OpenDataSoft. « *L'enjeu est le même : gérer des applications qui vont faciliter la vie des usagers. Donc, la data est cruciale.*

« Le paiement mobile arrive, mais aussi le modèle économique des parkings fermés, avec forfaits, abonnements. Et à partir du moment où ces services existent en mobilité, on dématérialise totalement le paiement et cela implique que le contrôle de paiement soit effectif »

François Duquesnoy, directeur Smart Cities d'Orange Business Services

Troyes Le choix d'un capteur interactif

Pour sa solution pilote de parking intelligent, Troyes a retenu, avec Orange, la solution StreetLine. Les automobilistes peuvent connaître en temps réel la disponibilité des places de stationnement libres et être guidés jusqu'à celles-ci. Cette solution de parking intelligent permet de mieux réguler le stationnement et de réduit la congestion en centre-ville. Le projet, qui a été lancé à l'automne 2015, porte sur 215 places de stationnement en voirie. Chaque place est équipée d'un capteur sans fil, autonome, qui permet d'identifier les places libres.

Le dispositif utilise les technologies radio de basse consommation. Orange a opéré le pilotage du déploiement et a fourni les cartes SIM M2M (machine-to-machine). Les informations de disponibilité sont remontées de façon très régulière vers un serveur central. La solution fonctionne en couplage avec une application sur smartphone, Parker, développée par StreetLine. Elle permet de visualiser la cartographie des rues de Troyes, enrichies en temps réel. L'utilisateur voit apparaître un plan lui indiquant les places disponibles à proximité.

Ainsi, quel que soit son opérateur mobile, l'utilisateur peut visualiser en temps réel la cartographie des places disponibles dans un lieu donné, consulter les tarifs mis à jour en permanence et se faire guider vocalement jusqu'à la place de son choix.

Le contrôle du paiement du parking est effectué à partir de la plaque d'immatriculation par des agents circulant en voiture ou en deux-roues équipés de caméras qui scannent les plaques à distance. Un agent peut gérer à lui seul près de 2 000 places.

Amsterdam Un modèle entièrement dématérialisé

Depuis 2010, dans la ville d'Amsterdam, le paiement et le contrôle du stationnement est possible à travers plusieurs applications mobiles sur smartphone. L'automobiliste saisit son numéro d'immatriculation sur l'application de son choix et il est traité automatiquement et enregistré sur un serveur central. Pas besoin de ticket, car le contrôle est effectué à partir de la plaque d'immatriculation par des agents circulant en voiture ou en deux-roues équipés de caméras qui scannent les plaques à distance. Le contrôle auprès du serveur central est instantané. Un agent peut gérer à lui seul près de 2 000 places (soit 5 à 8 fois plus que dans un mode opérationnel non dématérialisé). « Le modèle d'Amsterdam est particulièrement novateur, dans la mesure où il propose une gestion entièrement dématérialisée du contrôle au stationnement », souligne Rik Joosten, dg d'Egis Projects. « Notre but est d'atteindre un taux maximum de paiement du stationnement en voirie. Pour y parvenir, nous visons une meilleure rotation des véhicules de résidents et un respect plus important du paiement du stationnement en voirie », ajoute-t-il. Les droits de stationnement de chaque véhicule sont vérifiés auprès de l'opérateur en coopération avec les autorités locales (police et services financiers de la ville). Ce système performant limite considérablement la présence d'agents dans la rue. Le montant est débité et un justificatif électronique est automatiquement envoyé. Si l'enregistrement n'a pas été fait sur le serveur central, l'image scannée, géolocalisée, est sauvegardée pour attester que le paiement n'a pas été effectué. C'est un agent assermenté qui confirme et enregistre l'infraction ultérieurement, au vu du cliché. L'infraction est validée au bout de 15 minutes, après une relance pour régularisation. Après 5 infractions consécutives, un sabot est posé sur le véhicule. Le système, opéré par le français Egis (Caisse des Dépôts & Consignations), a permis de diviser par trois le nombre des horodateurs (environ 2 500). Plus de 60 % des paiements sont effectués de cette façon à partir d'un mobile. A ce jour, 150 000 places sont ainsi gérées. D'autres applications pourraient en découler, comme le relevé de positions ou le calcul de taux d'occupation, qui pourrait être effectué par les véhicules de contrôle, de façon automatique. A noter que la ville de Paris est intéressée par des expériences de lecture automatisée des plaques d'immatriculation (LAPI), sur le modèle d'Amsterdam.

Rik Joosten, Directeur Général d'Egis Projects

« Aujourd'hui, raisonner en termes de places libres, cela ne fait pas un 'business model'. A l'inverse, on voit bien un ou des modèles qui se construisent autour de la « market place » du parking intelligent. Il y a encore beaucoup de données qui restent à exploiter et des services à inventer ».

Khalil Laaboudi, consultant Smartcity chez Ericsson

Cette ouverture des données redonne du lien entre délégants et délégataires. Ils se comprennent mieux. Et c'est là que se trouve la dynamique de l'innovation ». L'application Citymapper est un bon exemple: elle permet d'organiser le déplacement multi-modal en rapprochant les opérateurs du transport via des API.

Question sur le 'business model'

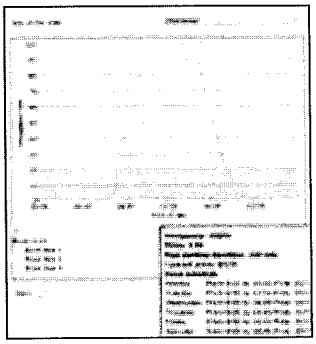
« Le vrai frein dans le domaine du parking, c'est le risque de bouleversement du 'business model' : les opérateurs de parking craignent d'être pillés par les géants du web. Mais cela ne doit pas les empêcher de construire une stratégie digitale », ajoute Mathieu Caps

Khalil Laaboudi, consultant Smart city chez Ericsson constate un « *changement de paradigme* » : « *Aujourd'hui, raisonner en termes de places libres, cela ne fait pas un 'business model'. A l'inverse, on voit bien un ou des modèles qui se construisent autour de la « market place » du parking intelligent. Il y a encore beaucoup de données qui restent à exploiter et des services à inventer ».*

Ailleurs dans le monde

A San Francisco (Etats-Unis), 7 000 capteurs relèvent en permanence l'occupation des places de stationnement sur la voirie. Plus original, un projet de gestion dynamique des prix a été mis sur pied en partenariat avec Xerox. Il vise à fixer les prix dynamiquement, rue par rue, bloc par bloc, de sorte que le taux d'occupation de chaque bloc reste entre 70 et 80 % durant toute la journée. « Dynamiquement' signifie en fait que les prix sont établis à l'avance mais peuvent être changés toutes les 2 ou 3 semaines, ou une fois par mois, explique Matthew Darts, chef de projet auprès de Xerox. Imaginez que vous vous garez habituellement au tarif de 5 $ par heure, et vous constatez en sortant de la voiture que le tarif a grimpé à 15 $. L'explication est qu'à cette heure-là, ce jour-là, vous aviez très peu de chance de trouver une place dans cette rue - à moins d'y mettre le prix... Le but ici est de vous garantir de trouver cette place, mais comme elle est rare, c'est à vous de vous la payer ou non ».

En Finlande, une expérimentation est menée sur le campus de l'université d'Aalto. Elle utilise la géolocalisation des smartphones et les données de ses capteurs pour distinguer si la personne est dans sa voiture ou à pied : c'est le 'crowdsensing'. Par rapprochement avec les plans des lieux et la géolocalisation, un algorithme fait des recoupements entre plusieurs 'inputs' et peut déterminer qu'il y a eu déplacement d'un véhicule et que, donc, une place s'est libérée ou l'inverse. Une application d'assistant au stationnement communique avec un serveur en réseau ; et donc les utilisateurs, fournissent également des données. Il y a donc combinaison de 'crowdsensing' et de 'crowdsourcing'.



A San Francisco, le système mis en place en partenariat avec Xerox permet de fixer les prix du stationnement de manière dynamique, rue par rue, bloc par bloc, de sorte que le taux d'occupation de chaque bloc reste entre 70 et 80 % durant toute la journée. Pour cela, les prix fluctuent à la hausse comme à la baisse.

« Le parking est une dimension de la mobilité, au sens global. Et il ne peut pas y avoir de stationnement intelligent sans ouverture des données »

Mathieu Caps, responsable Public affairs chez OpenDataSoft

Pose d'un capteur sur une place de parking (à Londres).

François Duquesnoy, directeur Smart Cities d'Orange Business Services, estime pour sa part qu'on est au coeur du débat, à commencer par l'aménagement des tarifs. « *Non seulement le paiement mobile arrive (cf. Pay by phone), mais il y a aussi le modèle économique des parkings fermés, avec forfaits, abonnements. C'est moins visible mais cela arrive. Et à partir du moment où ces services existent en mobilité, on dématérialise totalement le paiement et donc, cela implique que le contrôle de paiement soit effectif. Il n'y a plus de ticket, donc les agents municipaux doivent pouvoir vérifier que l'usager a bien payé. Cela rejoint l'actualité sur la dépénalisation du parking* ».

Effectivement, dans moins de deux ans, ce sont bien les collectivités qui auront cette responsabilité.

PIERRE MANGIN

Une puce radio (RFID) placée sur chaque poubelle revient à environ 2 euros l'unité et permet d'identifier le titulaire du contrat pour le facturer en conséquence.

Réduire les ordures ménagères grâce à la tarification incitative

Comment inciter les citoyens à réduire leurs déchets et à mieux les trier ? Première solution : les faire payer au volume de déchets ménagers qu'ils produisent. Autre solution : miser sur le dialogue et l'interactivité, via le web et les applications mobiles, afin de favoriser une prise de conscience.

La « tarification incitative » repose sur le principe du « pollueur/payeur » et consiste à faire payer aux citoyens le service de gestion des déchets, en fonction de la quantité d'ordures ménagères qu'ils produisent. Ce dispositif est devenu monnaie courante au Japon, en Corée ou en Suisse. En France, il se généralise depuis 2010, avec une mise en place dans quelque 200 collectivités, soit environ 5 millions d'habitants.

Comment sont comptabilisés ces déchets ? Dans la majorité des cas (80 % en France*), la mesure s'effectue sur le « nombre de levées », c'est-à-dire le nombre de fois où la poubelle a été présentée à la collecte. Pour 11 % des cas, un système de pesée est ajouté, intégré au niveau du camion de collecte. Le volume du sac peut également servir de critère (6 %), et environ 2 % des collectivités ont simplement mis en place un système de sacs payants.

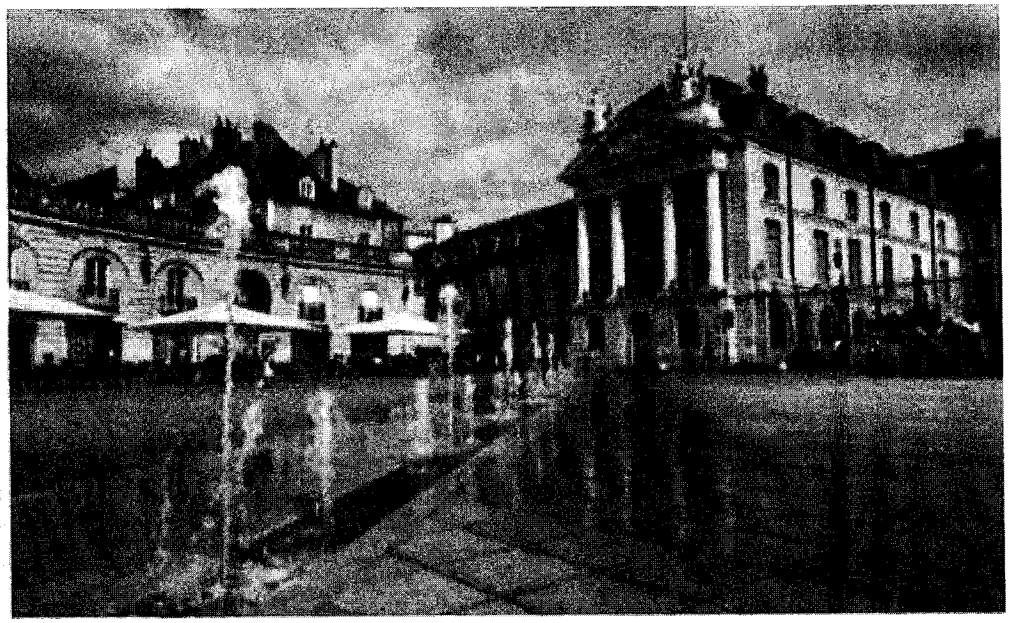
Quelle que soit la formule choisie, la tarification intègre toujours une part fixe, qui correspond à l'abonnement au service public d'élimination des déchets, à laquelle s'ajoute une part variable, qui dépend donc du volume de déchets produits. Il en coûte en général un peu moins de 100 euros par an et par habitant, à payer en deux ou trois fois.

Moins de déchets et davantage de tri sélectif

Les résultats de ce dispositif sont, a priori, plutôt encourageants. « *Il s'avère très efficace pour inciter au tri et à la réduction des déchets : dans les collectivités où il est appliqué, les quantités d'emballages et papiers triés augmentent d'un* »

Grand Besançon -28 % de déchets grâce à la tarification incitative

Le Grand Besançon a été la première - et la seule - agglomération de plus de 100 000 habitants à avoir mis en place la tarification incitative. Le dispositif a permis une réduction de 28 % des déchets ménagers. Cela représente une baisse annuelle de 66 kg en moyenne par habitant. Et le recyclage a aussi progressé : la collecte sélective du verre a notamment augmenté de 3 %. Le système retenu tient compte du poids et du nombre de levées. Pour l'habitat collectif (68 %), le syndic ou le gestionnaire de l'immeuble reçoit la facture et la répercute dans les charges, au tantième de chaque logement. Enfin, chaque habitant peut suivre sa production de déchets sur un portail web. « Les habitants ont réduit leur production de déchets, notamment avec la pratique du compostage qui a été largement promue par la communauté de d'agglomération. Par ailleurs, ils ont sensiblement développé le tri sélectif », indique Yves Jeannerod, responsable de la relation usagers du Grand Besançon. « Nous sommes satisfaits de ce dispositif qui a eu un impact significatif sur la réduction des déchets et sur l'augmentation du tri. De plus, il a été plutôt bien vécu par les usagers », confie pour sa part François Lopez, vice-président du Grand Besançon en charge de la gestion des déchets.



Jean-Patrick Masson, délégué à l'environnement à la communauté urbaine du Grand Dijon

Dijon mise sur l'interactivité avec les citoyens

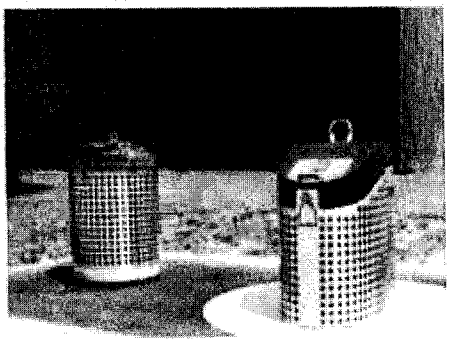
Pas de conteneurs connectés ou de tarification incitative à la communauté urbaine du Grand Dijon. « Nous misons sur un maximum de communication et d'interactivité avec les habitants pour favoriser l'action citoyenne », confie Jean-Patrick Masson, délégué à l'environnement, au patrimoine, à l'énergie et aux déchets du Grand Dijon. Le principal canal de communication est aujourd'hui le site web de la communauté urbaine. Il offre de nombreux services autour des déchets, comme par exemple la localisation des collecteurs à proximité en fonction du type de déchet. Le site permet également de prendre rendez-vous pour la collecte d'encombrants et de noter l'intervention des agents. Enfin, il intègre également un annuaire de professionnels et d'associations qui peuvent réparer ou redistribuer des objets, du textile aux ordinateurs, pour donner une seconde vie aux produits plutôt que de les jeter. « En 2017, ces services seront disponibles sur smartphone et tablette via des applications dédiées intégrant la géolocalisation. Cela augmentera encore l'interactivité avec les citoyens », indique Jean-Patrick Masson. Depuis un an, une dizaine d'agents de la communauté urbaine vont également à la rencontre des citoyens pour les sensibiliser. Avec cette politique de dialogue, le Grand Dijon entend réduire ses déchets de 10 % d'ici 2020.

tiers et les quantités de déchets non triés sont aussi réduites d'un tiers », indique une communication récente du Ministère de l'environnement*. Les collectivités observent un transfert d'une partie des déchets, auparavant jetés dans les poubelles d'ordures ménagères, vers le recyclage. Par ailleurs, le comportement des citoyens change. Ils vont par exemple privilégier l'achat d'un produit avec moins d'emballage. « *Les comportements des usagers commencent à changer dès l'année précédant l'entrée en vigueur de la tarification incitative* », observe la note ministérielle.

Techniquement, ce dispositif est assez simple à mettre ne place. Il faut ajouter une puce radio (RFID) aux poubelles afin d'identifier le titulaire du contrat, ce qui revient à environ 2 euros l'unité, et déployer un logiciel de gestion du service dont le prix oscille entre 10 000 et 60 000 euros.

Une solution efficace surtout en zone rurale

Parmi les principales collectivités à avoir déployé la tarification incitative figure le Grand Besançon. Mise en place dès 2012, elle a permis une réduction du nombre de déchets ménagers de 28 % (lire encadré). La communauté de commune de Ribeauvillé a, pour sa part,



La « tarification incitative » consistant à faire payer aux citoyens le service de gestion des déchets en fonction de la quantité d'ordures ménagères qu'ils produisent, se généralise depuis 2010, avec une mise en place dans quelque 200 collectivités, soit environ 5 millions d'habitants.

déployé ce dispositif depuis 2002, avec un système mixte au poids et au nombre de levées. « *Les résultats ont dépassé nos espérances. Nous sommes passés de 5900 tonnes de déchets ménagers en 1999 à 2500 tonnes en 2015. Il y a eu un transfert vers le tri sélectif, en passant de 730 tonnes pour le papier/cartons à 1500 tonnes, 85 à 215 tonnes pour le plastique et 850 à 1300 tonnes pour le verre* » confie Michael Gruny, responsable du service environnement.

Reste que ce système possède tout de même une limite : il est surtout efficace en milieu rural ou du moins en zone pavillonnaire. Il est en effet plus complexe de comptabiliser les volumes de déchets dans le cas de logements collectifs où chaque ménage n'a pas sa propre poubelle. Mais de nouvelles solutions technologiques arrivent sur le marché. Suez, Véolia comme Ecowaste proposent des conteneurs intégrant un système de badges qui permet ainsi de comptabiliser les levées pour chaque ménage. « *Nous réfléchissons au déploiement de ce type de solution* », indique Michael Gruny.

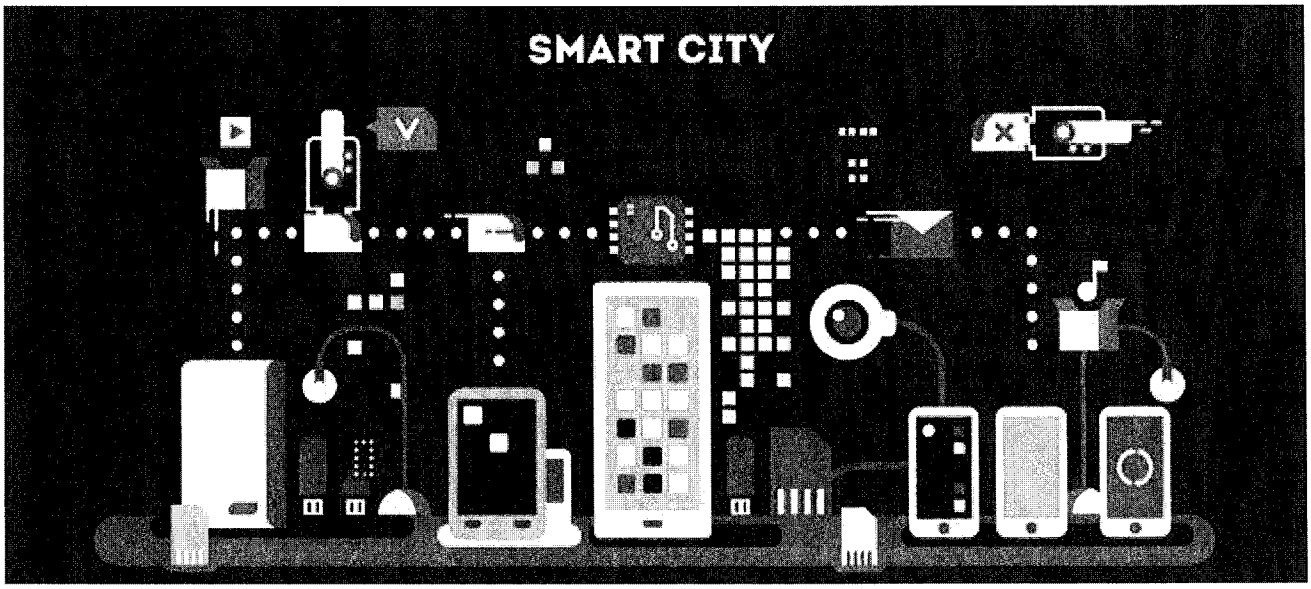
Malgré ce bémol autour de l'habitat collectif, la mise en place de la tarification incitative devrait largement se généraliser dans l'Hexagone durant les années à venir. Elle est ainsi promue par la loi relative à la transition énergétique pour la croissance verte («LTECV ») de 2015. Objectif du texte : que la tarification incitative concerne 15 millions d'habitants en 2020 et 25 millions en 2025. ■

* *chiffres issus de la note du Commissariat général au développement durable : « Déchets ménagers : Efficacité de la tarification incitative », parue en septembre 2016*

DOCUMENT 9

Smart city et citoyen

strategie.gouv.fr



Crédit : DR

Smart city et citoyens

Mercredi 11 mai 2016

Compte rendu - Le 11 mai 2016, France Stratégie, associé au think tank « Objets connectés et intelligents France », a organisé un débat d'experts associant start-up, grands groupes et pouvoirs publics, pour confronter les visions de la smart city.

Morceaux choisis

Le développement des objets connectés est un enjeu de société, de compétitivité et d'attractivité des territoires. Les innovations attendues vont engager les villes dans une transition qui doit permettre d'optimiser la mobilité, de réaliser des économies d'énergie, de mieux gérer la pollution… Et donc d'améliorer la qualité de vie dans la ville.

De nouveaux modes de consommation vont émerger, ainsi que de nouvelles façons de vivre au quotidien, de partager des intérêts communs autour d'événements culturels, sportifs, éducatifs... Grâce à la connectivité en mobilité et en temps réel, ces objets permettent le partage sur les réseaux sociaux mais aussi l'optimisation grâce au traitement des big data.

Mais jusqu'où les objets connectés vont-ils se développer dans la ville ? Comment favoriser et réguler leur développement pour qu'ils soient le plus favorables au citoyen ?

Telles étaient les questions posées lors de ce débat.

La qualité de l'air : un cas d'école

Le sujet de la qualité de l'air peut être considéré comme un cas d'école pour la smart city. Un exemple des potentialités des objets connectés dans un domaine qui représente un véritable enjeu pour les collectivités.

« *Les citoyens de la ville intelligente de demain devront respirer un air de qualité* », affirme Thomas Kerting, fondateur d'Aircology (open innovation). « *La qualité de l'air est une ressource à protéger mais aussi un vecteur d'attractivité du territoire, de bien-être et de santé*

pour les citoyens. C'est également une source de nouvelle économie, à la convergence du numérique et de l'environnement. La France doit prendre le leadership sur l'air comme elle l'a pris sur l'eau ».

« *Au-delà de la technologie, la question posée est celle de l'analyse des quantités phénoménales de données collectées par ces objets connectés* », souligne Cyrille Najjar, co-fondateur de White Lab, une start-up qui développe un capteur capable de détecter et de qualifier les particules dans l'air à l'échelle de l'usager. « *Les gouvernements et les collectivités doivent utiliser ces données, pour bâtir à terme un algorithme du confort respiratoire et du bien-être des citoyens* ».

« *La lutte contre la pollution est une opportunité unique de tester la puissance des objets connectés*, estime Eve Tamraz, docteure de l'ENS de Paris et co-fondatrice de White Lab. *La connaissance de la qualité de l'air va permettre à chacun de mener des actions simples au quotidien pour contribuer à l'amélioration de la santé globale et de la qualité de vie dans la ville. Ce nouveau savoir donne le pouvoir aux citoyens de prendre en charge leur santé* ».

« *Il faut changer les habitudes des usagers et les habituer à mesurer la qualité de l'air*, suggère Cyrille Najjar. *La complémentarité entre puissance publique et sociétés privées doit s'organiser autour du travail sur les données, qui permettront aux collectivités de disposer d'un diagnostic précis par quartier et par type de polluant* ».

Le déploiement d'objets connectés dans la ville

Au-delà des détecteurs de pollution, de nombreux objets connectés vont se déployer dans la ville.

Cécile Maisonneuve, présidente de La Fabrique de la Cité, think tank créé à l'initiative du groupe Vinci, cite l'exemple de Google Sidewalk Labs à New York. « *Considérant que le trottoir est l'espace le plus intéressant dans la ville, ils vont y installer du mobilier urbain intelligent, avec un relais Wifi qui va capter une grande quantité de données. Ce partenariat permettra à la ville d'engranger d'importantes recettes publicitaires... Mais l'idée est surtout de faire de ces mobiliers urbains intelligents des points relais des services publics de la ville : 7 500 points de connexion et de dialogue entre l'habitant et les pouvoirs publics. C'est un exemple intéressant de réconciliation entre la temporalité très rapide du citoyen connecté et de la start-up et la temporalité beaucoup plus longue de la ville et de l'aménagement urbain* ».

« *À New York, Sidewalk Labs réhabilite également les anciennes cabines téléphoniques pour les transformer en kiosques numériques délivrant de l'information contextualisée de proximité. Lorsqu'on avance de 200 mètres, on n'a pas la même information sur le quartier, les commerces, les transports, l'activité culturelle... C'est en combinant la géolocalisation et la contextualisation que l'on peut pousser la bonne information au bon moment* », ajoute Sandrine Murcia, directrice générale de Connecthings. Cette société travaille avec une vingtaine de villes en Europe et avec Rio au Brésil pour déployer des balises Bluetooth sans contact – ou *beacons* – capables d'interagir depuis les espaces urbains et les lieux publics avec les applications mobiles des citoyens. Des balises qui peuvent notamment être installées sur des abribus ou des totems.

« *Les* beacons *sont de plus en plus perfectionnés et intègrent de plus en plus de capteurs. Ils peuvent être fixes ou portés par une personne dans son smartphone. On est loin d'avoir défini*

tous les usages de ces objets », confirme Max Tessier, gérant de la société Ubi Dreams, start-up spécialisée dans les applications mobiles.
« *Les collectivités doivent faire attention avant de déployer massivement des infrastructures qui seront obsolètes d'ici cinq à dix ans* », prévient néanmoins Xavier Darrigol, co-fondateur de Retency, une société qui vise à adapter aux commerces physiques des outils marketing du e-commerce. « *Le premier smartphone digne de ce nom date seulement de neuf ans alors que la restructuration d'un quartier prend quinze ans. Une application mobile comme Waze a rendu obsolète les capteurs et les panneaux mis en place il y a dix ans sur le périphérique. Avec ces nouvelles applications, le coût en infrastructures pour la ville est nul. Laissons les utilisateurs apporter eux-mêmes les infrastructures ! S'il y a un intérêt réel pour les utilisateurs, pas besoin d'infrastructure physique : l'infrastructure, c'est le logiciel !* ».

Le rôle moteur du citoyen

« *Nous en sommes au début de la ville durable. Il ne faut pas croire que le capteur ou l'application ou l'infrastructure fera tout*, explique Sandrine Murcia. *Il faut penser les conditions dans lesquelles ces changements peuvent se faire et donner la possibilité aux citoyens de s'emparer, de tester, d'utiliser ces nouveaux services. La ville intelligente est une ville apprenante et programmable* ».
« *L'empowerment des citoyens est un enjeu majeur de la smart city* », confirme Anne-Sophie Bordry, fondatrice du think tank « Objets connectés et intelligents France ». « *Ce sont les citoyens qui bénéficieront des nouveaux services nés de l'innovation dans le domaine des objets connectés* ».
« *La pression des citoyens sur les réseaux sociaux a de plus en plus d'impact. Les utilisateurs des services ne sont plus de simples usagers mais deviennent des acteurs* », souligne Guillaume Buffet, président-fondateur de U, une plateforme de transformation digitale qui accompagne les très grandes organisations. « *Demain, avec la blockchain, les grandes organisations se feront doubler par leurs utilisateurs si leurs services ne sont pas à la hauteur* ».

À la recherche d'un modèle économique

Selon Max Tessier, « *le modèle économique doit associer toutes les problématiques de la ville : la mobilité, la gestion de la pollution, le commerce, l'énergie... Il faut par exemple récompenser l'action citoyenne de participation à la prise d'information sur la pollution par des réductions dans les transports ou les commerces* ».
« *Le modèle économique peut passer par l'*incentive, *il faut récompenser le citoyen pour ses bonnes pratiques*, abonde Anne-Sophie Bordry. *Il peut également passer par la location anonymisée des données* ».
« *Depuis notre création, nous avons piloté deux milliards d'euros d'investissements dans des infrastructures numériques pour les collectivités : un milliard de subventions publiques et un milliard de fonds privés* », précise Nicolas Potier, directeur associé de Tactis, cabinet de conseil en aménagement numérique du territoire. « *Nous privilégions cette articulation public / privé : il s'agit de faire du business qui corresponde à un service d'intérêt général. Nous travaillons sur les futurs modèles économiques de la smart city, notamment sur les socles techniques des infrastructures de données qui vont permettre d'interconnecter des bâtiments*

stratégiques, de superviser des réseaux de caméras et de radios, mais aussi d'alimenter une politique de service public de la donnée. La question est celle de la valeur de ces données. Nous cherchons des modèles durables fondés sur des co-financements public - privé ».

Le rôle de la puissance publique

Dans ce contexte, quel doit être le rôle de la puissance publique, des collectivités territoriales et de l'État ?

« *Beaucoup de décisions vont se prendre au niveau local et nous allons sans doute voir fleurir de nombreuses initiatives disparates. L'État central a un rôle essentiel à jouer d'information et de suivi* », prévient Xavier Darrigol.

« *L'État doit guider les choix technologiques destinés à offrir de meilleurs services*, estime Anne-Sophie Bordry. *Il doit accompagner les collectivités dans la rédaction des appels d'offres, le choix des infrastructures, la récolte et l'utilisation des données. L'État et les collectivités doivent aussi réinventer le service public de demain pour rester en phase avec les utilisateurs de services connectés* ».

« *Pour éviter les effets de mode, il faut parvenir à distinguer les technologies dont la durée de vie sera de trois ou quatre ans de celles appelées à se développer sur plusieurs décennies*, souligne Nicolas Potier. *Le point d'équilibre pour la puissance publique est difficile à trouver ; le temps de prendre la décision, la technologie peut devenir obsolète* ».

« *Le cœur du sujet est celui de l'appel d'offres*, estime Guillaume Buffet. *Quand on fait un appel d'offres, on sait ce que l'on cherche et par conséquent, on a défini un cahier des charges. Ici, personne ne sait. Il s'agit donc de créer les conditions de l'émergence de services innovants qui trouvent l'intérêt du citoyen et non pas de parier sur le succès de demain* ».

« *La vraie rupture du big data par rapport à l'informatique classique, c'est qu'il va chercher des modèles dans les données. Il est donc difficile de savoir a priori où l'on va* », souligne Pierre Delort, président de l'association nationale des DSI et enseignant à Mines ParisTech.

« *L'État doit favoriser l'émergence de sociétés privées, si possible françaises, qui vont vendre de nouveaux services aux collectivités ou protéger les données personnelles – un domaine où l'Allemagne est en train de prendre le leadership. Le sujet de l'éducation est également essentiel. En France, nous sommes bons en mathématiques théoriques mais un rapport de l'OCDE place la France au 27e rang pour l'emploi des* data specialists – *associant les maths appliquées et l'informatique* ».

L'Arcep, autorité de régulation des communications électroniques, travaille sur l'Internet des objets avec l'objectif d'aboutir à un livre blanc sur le sujet. Une consultation publique va être lancée d'ici l'été.

« *L'Arcep concentre son attention sur deux sujets*, explique Guillaume Mellier, directeur de l'accès fixe et des relations avec les collectivités territoriales. *Le premier est de construire les réseaux à haute capacité de demain, les réseaux en fibre optique, mais aussi toute l'ossature des réseaux mobiles. Le deuxième concerne le réseau mobile : il s'agit d'assurer la disponibilité en fréquences pour les acteurs privés. Jusqu'où devons-nous amener les réseaux dans les espaces publics pour assurer la connectivité (trottoirs, abribus) ? Quelle doit être notre action en matière de réseaux radio pour les objets connectés ? Ce sont aujourd'hui deux sujets d'interrogations pour l'Arcep* ».

Un enjeu de souveraineté

« *Des normes internationales commencent à apparaître, constituant des bases de travail intéressantes pour les territoires intelligents, qui peuvent ainsi s'appuyer sur l'expérience d'autres villes* », explique Jean-François Legendre, responsable développement de l'Afnor et rapporteur du comité stratégique Information et communication numérique. « *Il existe aussi des normes d'organisation et de management pour définir la stratégie pour aller vers la ville durable. Qui détiendra le pouvoir du futur ? Tel est le véritable enjeu. Si on ne participe pas aux négociations de ces normes internationales, on ne pourra pas par exemple défendre l'intérêt d'une gouvernance équilibrée ou introduire des notions de tiers de confiance pour protéger les données personnelles* ».

« *Comment les collectivités peuvent-elles accepter le déploiement d'infrastructures réseaux dans l'espace public ? Quid de la souveraineté avec les services connectés ?* s'interroge Anne-Sophie Bordry. *Et comment les collectivités, qui ont besoin de nouvelles sources de financement, peuvent-elles monétiser par exemple les data de mobilité dans la ville ?* »

« *La protection de la vie privée va-t-elle nous empêcher d'avoir accès à ces données ? Si des sociétés étrangères mettent des capteurs un peu partout, à qui sont ces data qui nous permettent de construire la ville ? Les politiques publiques devront se doter d'un pilotage avec des données souveraines* », préconise Tomas Kerting.

Voir plus loin

Le développement de la smart city n'en est encore qu'à ses débuts.

Les questions abordées lors du séminaire, qu'il s'agisse du rôle moteur du citoyen et de sa participation, des modèles d'affaires à construire autour des données et des services personnalisés, des complémentarités nouvelles public / privé et du rôle de la puissance publique, ont des résonnances qui s'étendent au-delà du champ de la smart city : l'enjeu est bien de « tirer parti de la révolution numérique ».

France Stratégie continuera à approfondir ces questions dans le cadre de son projet « 2017-2027 » visant à élucider les enjeux de la décennie, dans la perspective de la prochaine élection présidentielle.

Michel Bazan

Les choix technologiques de développement des objets connectés vont être un enjeu de société, de compétitivité et d'attractivité des territoires. Les innovations vont engager les villes dans une transition qui doit permettre d'optimiser les transports, de favoriser l'intermodalité et de réaliser des économies d'énergie. De nouveaux modes de consommation, de nouvelles façons de vivre au quotidien, de partager des intérêts communs autour des évènements culturels, sportifs, éducatifs, vont s'imposer.

De nouveaux objets connectés apparaissent tous les jours, d'autres le deviennent. Présents partout, du capteur élémentaire à la robotique, ces objets vont organiser la ville autrement. Grâce à la connectivité à internet en mobilité et en temps réel, ils permettent l'ouverture, le partage autour des réseaux sociaux, l'optimisation grâce aux traitements des big data et, par conséquent, une multiplication des usages.

Imaginons la ville intelligente demain, pour construire dans nos territoires une vision citoyenne des usages.

Thèmes de discussion

Smart City : une opportunité

- La multiplication des services : le développement d'une nouvelle économie grâce à la connectivité permanente en mobilité des citoyens.
- Smart City et bien vivre ensemble : les services connectés du « quantified self », du bien-être et les réseaux sociaux d'échanges et de partages ; l'explosion des plateformes collaboratives et de la « sharing economy » ; les apports des objets connectés au développement durable.

Smart City et souveraineté

- Quels sont les liens entre secteur public et secteur privé pour l'aménagement numérique du territoire urbain ? L'ouverture des politiques publiques et la coordination des services urbains au service des usagers ?
- Comment soutenir des services et territoires connectés pour faire de nos villes européennes des champions de la transition vers la connectivité permanente ?

ANNEXE A

Extrait de « Présentation de la stratégie globale smart city » par le Président d'INGECO lors de la cérémonie des vœux à la presse – Janvier 2017

Confrontée à une compétition nationale et internationale, la métropole d'INGECO doit relever le défi de l'attractivité de son territoire. Elle doit pour cela dépasser la simple notion d'aménagement numérique de son territoire pour mettre en œuvre une stratégie globale visant à la placer dans le top 10 des smart city mondiales.
Cette stratégie s'impose pour relever le défi des enjeux de société, de compétitivité et d'attractivité de notre métropole. Elle se fixe trois axes majeurs :

- Améliorer la gestion de notre territoire
- Réaliser des économies
- Créer de nouveaux services innovants pour le citoyen

Dans un domaine où les technologies évoluent constamment à un rythme soutenu, il serait délicat et inapproprié de planifier d'ores et déjà un portefeuille de projets numériques pour les cinq ans à venir. Il est préférable de fixer des principes d'action et une approche nouvelle pour les services de la collectivité.
Cette approche reposera sur les principes suivants :

- L'innovation numérique et les opportunités qu'elle porte doit devenir un marqueur fort de la réflexion et de l'action des services. Chaque projet identifié, dans quelque domaine que ce soit, devra être conduit en intégrant cette dimension digitale
- Une veille technologique permanente
- Un respect absolu des règles juridiques, notamment dans la collecte et l'exploitation de données sur les citoyens
- Un souci constant de la sécurité des données

Certains projets peuvent cependant être d'ores et déjà planifiés. Il s'agit notamment du projet « Smart parking », qui sera lancé dans les prochains jours et fera l'objet d'une consultation dédiée, destinée à mettre en concurrence les acteurs potentiels.
Ce projet majeur et innovant a pour objectif de limiter les pertes de temps et la pollution associée à la recherche de places de stationnement disponibles. Le citoyen doit disposer d'outils numériques lui permettant de connaître à tout moment les places de stationnement disponibles et d'être guidé en temps réel vers l'emplacement qui lui convient. Ce projet porte une forte valeur ajoutée :

- Efficacité économique en optimisant le temps de transport
- Respect de l'environnement avec la réduction des émissions de gaz à effet de serre
- Innovation numérique au service du citoyen

Le projet est global et concernera les 10 000 places de stationnement en surface ou souterraines qui sont actuellement proposées sur notre territoire. Il permettra également d'anticiper et préparer la réforme du stationnement qui confèrera une autonomie nouvelle à la collectivité dès le 1er janvier 2018.
Il sera complété au cours des prochaines semaines par d'autres initiatives majeures, visant à améliorer le dialogue entre la collectivité et le citoyen, favoriser la qualité de notre environnement et développer l'économie de notre territoire.