Cycle d'ateliers *Smart Cities*
Les enjeux juridiques et la justice dans la *smart city*

Mardi 4 juillet 2017

Nathalie PLOUVIET, avocat à la Cour d'appel de Paris, directeur du département Droit de l'internet des objets au cabinet Alain Bensoussan Avocats

La *smart city* est une ville qui cherche à résoudre des problèmes publics à l'aide des solutions offertes par les technologies de l'information et de la communication, sur la base de partenariats d'initiatives municipales et en mobilisant de multiples parties prenantes. Elle se caractérise selon le Parlement européen par six axes de réflexion : la gouvernance, la population, le mode de vie, la mobilité, l'économie et l'environnement.

De nombreux projets de *smart city* voient le jour, bouleversant à la fois le cadre juridique et les réflexions éthiques. L'arrivée de ces technologies se traduit en effet par une forte perturbation des cadres classiques de la réglementation et des équilibres depuis longtemps établis, entre l'ordre et la liberté, entre le collectif et l'individuel.

La notion de « propriété de la donnée » apparaît essentielle dans la *smart city*. La multiplication des acteurs sur un projet pose la question d'établir pour toutes les parties prenantes (sous-traitants) leur responsabilité dans la conception, la réalisation, l'exploitation et la maintenance du projet. Cette question est d'autant plus importante que les technologies employées sont sujettes à l'obsolescence. Par ailleurs, il semble capital que les collectivités locales prennent conscience de la valeur des données et puissent se forger une « culture de la donnée ».

Nathalie Plouviet attire l'attention sur la loi relative à l'ouverture des données conçue dans le but d'ancrer la France dans l'économie de la donnée. Si la circulation des informations et des savoirs est envisagée dans bien des cas comme une source d'innovation, certaines entreprises ont perçu l'*open data* comme une menace pour leur activité. C'est le cas de l'Insee dont le cœur de métier s'appuie sur le traitement de données. D'autres comme la RATP sont désormais dépendantes des GAFAM[1] qui n'hésitent pas à se servir de ces données pour les revendre aux collectivités locales. Le droit de réutilisation des données procure donc un net avantage concurrentiel aux nouveaux entrants. C'est l'exemple des images prises par Google à travers le monde, qui servent ensuite à valoriser des services.

Le développement des nouvelles technologies dans la ville passe par une meilleure protection des droits des personnes. Si l'anonymisation systématique des données est devenu un acquis juridique avec la Directive européenne 95/46/CE sur la protection des données personnelles, le « droit à l'intimité numérique » équivalent du « droit à la déconnexion » dans la sphère privée est cité comme l'un des piliers d'une meilleure acceptation sociale des nouvelles technologies. De même, des progrès doivent être faits dans la prise de conscience des risques cyber : 80 % des ménages conservent le mot de passe fourni lors de la vente d'un logiciel.

Enfin, une compréhension plus fine des enjeux éthiques par les citoyens est une étape essentielle pour tendre vers une *smart city*. Que signifie par exemple la notion de « consentement » dans le cas de la reconnaissance faciale ou de la géolocalisation ?

Dans ce contexte, l'élaboration de standards de la *smart city* apparaît nécessaire. La norme ISO 37120 a été élaborée avec des indicateurs[2] afin d'évaluer les services urbains et la qualité

[1] Google, Apple, Facebook, Amazon et Microsoft.
[2] Économie, éducation, énergie, environnement, finance, secours incendie et interventions d'urgence, gouvernance, santé, loisirs, sécurité, abris, déchets, télécommunication et innovation, transports, aménagement, eaux usées, eau et services d'assainissement.

de vie d'une ville. Cette norme permet de mesurer la compétitivité territoriale et a pour objectif d'agir comme un levier de transformation des territoires. La charte numérique verte (*Green Digital Charter*) développée par le réseau de grandes villes européennes, *Eurocities*, et initiée par Manchester engage les villes signataires à coopérer pour atteindre les objectifs de l'Union européenne en matière de changement climatique au moyen des technologies numériques. L'amélioration de l'efficacité énergétique et la réduction de l'empreinte carbone sont les grands axes déployés dans les projets pilotes. En France, Roubaix, Rennes, Nice, Nantes et Bordeaux ont adhéré aux principes de cette charte.

Le Royaume-Uni a, quant à lui, développé son propre standard afin « d'aider le marché à mettre en place les conditions propices à l'innovation ». Ainsi, le *Cities Standards Institute*, mis en place par la *British Standard Institution* (BSI) et le *Future Cities Catapult*, regroupe les villes, les principaux leaders de l'industrie et de l'innovation, afin d'identifier les défis auxquels sont confrontées les collectivités, d'apporter des solutions aux problèmes communs et de définir l'avenir des normes d'une *smart city*.

La dernière partie de l'exposée est consacrée à la responsabilité et à l'encadrement contractuel.
Nathalie Plouviet dresse une typologie des tendances de partenariat réalisé dans le cadre de projets de *smart city*. Elle souligne le développement des partenariats entre opérateurs privés et collectivités à l'instar du partenariat *smart water* conclu en 2014 entre Veolia et IBM. Cette solution couple l'expertise métier de Veolia dans le domaine de l'eau, des déchets et de l'énergie à celle d'IBM, spécialiste du traitement et de l'analyse d'information.

Myriam QUEMENER, **magistrat, détaché au ministère de l'Intérieur, conseiller juridique, Mission de lutte contre les cybermenaces**

Un des objectifs de la *smart city* est d'augmenter le niveau de sécurité dans la ville, qui peut devenir par voie de conséquence une *safe city*, comme en témoigne par exemple la ville de Mexico où la délinquance a baissé de 50 % environ. Paradoxalement, l'arrivée des technologies numériques est source de menaces, comme le montre la hausse des cyberattaques. Face à ces mutations, le cadre juridique doit se renouveler rapidement, afin de pouvoir assurer la protection des citoyens, des collectivités locales et des pouvoirs publics.

L'émergence d'une cybercriminalité à grande échelle (« *ransomware* » ou « *rançongiciel* ») soulève plusieurs enjeux, avec en premier lieu celui de la reformulation de la protection de la vie privée. En témoigne l'apparition dans le droit de la notion de « vol des données » reconnue en 2014 pour la première fois, par l'article 323-1 du Code pénal : désormais, la notion de « vol » et plus précisément d'extraction de données s'applique dans l'espace virtuel. Par ailleurs, les indices dans les enquêtes pénales sont désormais numériques comme les données de géolocalisation, les systèmes de vidéosurveillance ou toutes autres informations contenues dans les objets connectés qui peuvent être utilisés dans les investigations pénales.

En second lieu, les technologies numériques redessinent la géographie du droit : les frontières juridiques tendent à disparaître. Le caractère extraterritorial du droit invite à davantage de coopération entre services de police nationaux, d'une part, et entre services de police et acteurs privés, d'autre part. Le recueil des preuves (vidéosurveillance par exemple) s'effectue désormais auprès d'acteurs économiques. Un travail de coopération a été amorcé dans ce sens avec les géants américains du net en vue de retirer plus rapidement les contenus illicites sur des sites, par exemple à caractère terroriste ou portant atteinte à la dignité humaine.
Une réflexion sur la conservation des données a également débuté. Actuellement de 30 jours pour la vidéoprotection, le délai d'archivage devrait s'allonger et s'étendre à toutes les données, afin de facilité le recueil de preuve.

Débat avec la salle

Le débat a été centré sur les solutions à fournir aux collectivités territoriales pour qu'elles se prémunissent contre les risques de captation de leurs données par des acteurs économiques, d'une part, et les cybermenaces, d'autre part.
À l'heure actuelle, le travail de sensibilisation est réalisé auprès des institutions territoriales par les pôles de compétitivité et les CCI, tandis que l'ANSSI s'adresse en priorité aux organismes d'importance vitale (OIV).
Si les villes moyennes prennent progressivement conscience de la valeur de leurs données qui représentent leur patrimoine informationnel, elles ignorent jusqu'où le droit les autorise à les commercialiser et elles semblent freinées par un manque d'expertise juridique en interne.

Christine Raynard et Camille Boulenguer