Cycle d'ateliers *Smart Cities*
Quels sont les enjeux de vie privée et les impacts des cyber-risques dans une *Smart City*

Mardi 7 mars 2017

Régis CHATELLIER, chargé d'études innovation et prospective à la Commission nationale de l'informatique et des libertés (CNIL)

Le Laboratoire d'innovation numérique de la CNIL, LINC[1], a pour objet l'étude transversale et prospective des tendances émergentes d'usage du numérique et des données et de leur impact sur la protection des données personnelles et des libertés. À ce titre, le LINC entame une série de réflexions sur la ville numérique, interrogeant la place du citoyen dans la ville connectée.

La ville numérique est une « ville servicielle[2] », dans laquelle s'accumulent des briques de services. La littérature académique a montré que la ville numérique est un concept en construction depuis une dizaine d'années. L'appellation « *Smart City* » émerge en 2008 aux États-Unis et désigne alors la stratégie commerciale d'IBM à destination des collectivités. Ce concept se caractérise par une vision *top down* et technophile, un paradigme qualifié de « tentation néo-cybernétique » par Antoine Picon où « la ville, l'humain et la machine formeraient un système unique dont le gestionnaire pourrait mesurer et contrôler chacun des aspects ». Le projet de la cité-État de Singapour représente un exemple « pur » de cette vision, un modèle non reproductible où tout est contrôlé verticalement, dans une relation directe entre les autorités et les habitants.

Plus tard, l'approche *bottom-up* dite des « Civic hackers », fait place aux développeurs indépendants (les start-ups, les petites et moyennes entreprises), qui utilisent les données pour promouvoir de nouvelles formes de pratiques urbaines, plus collaboratives. Autrement dit, ce sont les contributions des citoyens qui participent à la construction de la ville numérique, à l'image de l'application pour vélo « Strava », qui capte les données des cyclistes et les revend au service d'urbanisme de Seattle.

La connaissance utilisateurs générée par ces *big data* est plus efficace que les données récupérées par des capteurs urbains. Depuis environ deux ans, comme le dit Carlos Moreno, les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) « *prennent leur revanche* ». Forts de leurs données, de leur capacité à opérer techniquement et d'une certaine légitimité liée à la convocation de la multitude, les industriels de la donnée entendent s'imposer aux villes par les usages. Face à la popularité de certaines applications telles que Waze, le service de géolocalisation de Google, les villes se trouvent confrontées à un dilemme, dans lequel les industriels leur proposent des services pour les citoyens, en contrepartie de la fourniture des données.

La généralisation du modèle « données contre services » séduit de nombreuses villes moyennes, qui contrairement aux grandes métropoles, manquent de financement et de conseil et sont attirées par l'apparente gratuité des services offerts par les géants du numérique. Aux États-Unis, 16 villes ont ainsi contracté avec Google. De même, Uber propose de remplacer certains services de transports en commun par sa flotte de VTC, sans pour autant mettre ses données en accès libre (*open data*).

---

[1] https://linc.cnil.fr.
[2] Bruno Marzloff, 2011.

Face à la massification des données, la question de leur traçabilité et de leur anonymisation se pose au fur à mesure de leur réutilisation. Dès lors, le risque de discrimination est amplifié et la frontière entre le service et la surveillance s'amenuise. Le cas des algorithmes prédictifs du crime, de véritables « machines à biais », en est un exemple. Mais l'hyper personnalisation des services ne doit pas prendre la forme d'une surveillance des citoyens.

La CNIL réaffirme l'importance dans le cas de l'*open data* de l'anonymisation complète des jeux de données, qui ne permettent en aucun cas de remonter jusqu'à l'individu. Régis Chatellier rappelle par ailleurs que la question de la protection des données personnelles est distincte des enjeux de propriété, les individus doivent pouvoir faire valoir leurs droits sur les données qui les concernent directement, quels que soient les détenteurs de ces données.

Au-delà de la notion de risque, Régis Chatellier souligne que la protection de la vie privée est une opportunité pour des acteurs qui prendraient en compte ces questions dès la conception de leurs services urbains (*privacy by design*), créant ainsi, dans une période où les individus prennent conscience de l'importance de la protection des libertés, une forme d'avantage concurrentiel par rapport à des acteurs moins soucieux de ces questions. Le règlement européen sur la protection des données personnelles, applicable en 2018, va dans ce sens.

Yves VERHOEVEN, **sous-directeur des relations extérieures et coordination à l'Agence nationale de la sécurité des systèmes d'information (ANSSI)**

Créée en 2009 et placée auprès du secrétaire général de la défense et de la sécurité nationale au sein des services du Premier ministre, l'ANSSI est responsable de la cyber sécurité. Initialement tourné vers la cyber défense des organes régaliens, son rôle s'est élargi à la sécurité numérique de la société de l'économie. Sa mission se traduit par des actions de sensibilisation, de prévention et de réaction face aux cyber-attaques.
Depuis la loi de Programmation militaire (LPM) de 2013 et la Directive européenne sur la sécurité des réseaux et des systèmes d'information (NIS), l'ANSSI endosse des responsabilités à l'échelle nationale sur des opérateurs d'importance vitale (OIV) et des opérateurs de services essentiels (OSE).

Le risque cyber est un risque spécifique et peut être défini comme la rencontre entre des vulnérabilités, un scénario de menace et les impacts de l'exploitation de ces vulnérabilités, entendus comme l'effet recherché de l'acteur malveillant.

Par nature, le risque cyber est un risque généré par un agent malveillant et ne repose pas sur la prise en compte statistique d'un aléa. Trois axes de travail permettent de limiter ces risques :

- diminuer les vulnérabilités ;
- réduire le nombre d'acteurs malveillants ;
- travailler avec les porteurs de systèmes d'information pour maîtriser et limiter les impacts potentiels des atteintes à ces systèmes.

La menace se classe en quatre catégories :

- les attaques relevant de la cybercriminalité, qui visent l'enrichissement de l'attaquant ;
- les atteintes à l'image visant la déstabilisation (par exemple : piratage de sites internet de collectivités ou d'acteurs privés et entreprises lors des attaques terroristes djihadistes) ;
- l'espionnage (captation d'informations potentiellement à caractère stratégique) ;
- le sabotage, entendu comme la volonté de nuire sur une partie ou sur la totalité d'un système (par exemple : ville, usine).

Parmi ces différentes types de menaces, Yves Verhoeven remarque que, dans le cas des villes intelligentes, c'est bien le risque de sabotage qui est le plus préoccupant. En 2015, l'ANSSI a traité 20 attaques majeures de niveau stratégique contre la France (exemple : TV5 Monde).

La maîtrise des risques cyber est un processus continu d'évaluation et de réduction de ces risques, et d'acceptation par la maîtrise d'ouvrage du niveau de risque résiduel. L'homologation de la sécurité est un réel enjeu pour les villes connectées.

L'ANSSI aborde la question de la ville numérique à travers deux « tiroirs » :

- le premier est relatif à la sécurité individuelle de chacun des services. Ainsi, nombre de ceux-ci interagissent avec des personnes, notamment au niveau des objets connectés (IOT). C'est le cas des capteurs qui collectent les données, mais aussi des objets dits « actionneurs », tels les véhicules autonomes, qui interagissent avec l'homme dans le monde physique. Avec ces objets connectés du type actionneur, la sûreté des personnes peut donc être en jeu. Aujourd'hui, la cyber sécurité de chaque service est un sujet de préoccupation ;
- le second est l'interconnexion des services qui fait émerger de nouveaux risques, à la fois parce qu'elle augmente la surface d'attaque sur chaque service et qu'elle génère des risques nouveaux par la mise en relation des systèmes entre eux. À l'heure actuelle, les villes ne sont pas intégralement connectées, elles se limitent le plus souvent à la connexion de trois, voire quatre systèmes entre eux – cela pousse les méthodologies actuelles de maîtrise des risques à leur limite. L'ANSSI attire l'attention sur le fait que les risques d'une interconnexion de nombreux systèmes ne peuvent pas être maîtrisés avec les outils existants.

De manière générale, les *Smart Cities* posent le problème du « cyber-risk management » pour les « systèmes de systèmes » (S2S). En effet, la gestion décentralisée des risques ne permet pas d'appréhension globale. De surcroît, un système décentralisé et interconnecté est par principe complexe et son évolution n'est pas prévisible si on connaît seulement les briques de base.

L'ANSSI alerte donc sur le fait que la généralisation rapide des villes intelligentes ne pourra, à court terme, qu'engendrer des catastrophes. Outre les enjeux de sécurité, des questions de souveraineté se posent. Yves Verhoeven prend l'exemple du recours massif au *cloud computing,* dont il rappelle que le risque de captation ou d'altération des données est possible dans la mesure où l'opérateur qui héberge les données peut, en dépit de ses obligations de transparence et de neutralité, avoir intérêt à prendre connaissance de leur contenu, ou être soumis à des réglementations nationales donnant à des tiers accès à ces données.

S'agissant du conseil à apporter aux métropoles, l'ANSSI s'attache à son rôle de sensibilisation auprès de celles-ci. Elle a ainsi, depuis un an, initié le déploiement d'agents dans les territoires pour porter ces messages.

L'agence alerte sur le fait qu'aucune ville ayant une démarche Smart City ne présente une approche innovante de la gouvernance du risque cyber. Il s'agit d'un véritable défi à relever.

Il se pose donc la question de la mise en place d'une structure qui permettrait de partager l'expérience entre métropoles sur le sujet spécifique des *Smart Cities*.

Christine Raynard et Camille Boulenguer