Le Point.fr
Mon petit droit m'a dit
Par Laurence Neuer
Publié le 03/11/2017

Ville intelligente : "Le risque est que les données se retournent contre les personnes"

ENTRETIEN. Préserver l'anonymat et protéger les libertés dans la smart city est une lutte de longue haleine. Et la Cnil veille au grain...

Les multiples garde-fous juridiques font-ils le poids face à l'invasion des capteurs, compteurs, caméras, qui collectent des données dans les villes ? © Manuel Cohen /

"L'air de la ville rend libre", disait Hegel.

Cette formule doit-elle désormais s'énoncer au passé ? Du géographe Rob Kitchin et ses prédictions de "surveillance panoptique" à la Cnil qui, dans sa dernière étude La Plateforme d'une ville, pointe les risques de la "datafication" de la ville sur la protection des libertés, il est plutôt question d'asphyxie et de captivité. Les libertés d'aller et venir, la liberté sexuelle, la vie privée, sont-elles solubles dans le numérique ? Les multiples garde-fous juridiques font-ils le poids face à l'invasion des capteurs, compteurs, caméras, qui collectent des données de manière continue et invisible ? Entretien avec Régis Chatellier, chargé d'études prospectives au Laboratoire d'innovation numérique de la Cnil (Linc), qui a publié La Plateforme d'une ville.

Le Point : " Une ville ne saurait devenir pleinement intelligente sans plonger ses capteurs et ses réseaux jusqu'à l'intérieur de nos logements. Si l'optimisation des flux de mobilité pose la question de la liberté d'aller et venir anonymement, la *smart city* pose la question de notre capacité à préserver notre domicile du regard inquisiteur du reste de la société", souligne l'étude de la Cnil. Comment s'expriment ces menaces ?

▶ Régis Chatellier : Aujourd'hui, on veut que l'espace urbain soit le plus fluide possible. Et l'on s'oriente vers une ville "sans couture", dont, pour reprendre une image utilisée pour les réseaux de communication, le dernier mètre de la smart city serait le bâtiment, ou le logement. Autrement dit, cette gestion des flux ignore, si on ne la régule pas, la frontière de l'intime. Un exemple ? Celui des capteurs du Crous de Rennes. Cet organisme qui gère la résidence étudiante avait en septembre dernier décidé d'expérimenter des capteurs sur les lits escamotables pour pouvoir en anticiper la maintenance. Il s'agissait d'un capteur de poids qui permettait de connaître la charge supportée par le lit, mais aussi potentiellement de savoir combien de personnes étaient sur ce lit, et de déduire tout ce qui se passait dans l'intimité de la chambre. La Cnil a été alertée, mais, devant le tollé médiatique qu'il a suscité, le système n'a pas été expérimenté.

Accusé de vouloir espionner les étudiants, le Crous de Rennes retire des capteurs placés ds des lits https://t.co/KWGojBpnWf via @KonbiniFR

— Benjamin Jérôme (@benj_jerome) 24 septembre 2017

Au-delà du foyer, ces questions se posent dans l'espace urbain. C'est l'exemple, entre autres, du wifi tracking. La Cnil s'était opposée à ce que la société JCDecaux comptabilise les flux de piétons en collectant les identifiants des appareils mobiles de tous ceux qui passaient à proximité de ses panneaux publicitaires implantés à La Défense. L'affaire est allée jusqu'au Conseil d'État qui a, en février 2017, confirmé cette position pour deux raisons : la demande de JCDecaux ne prévoyait pas de recueillir le consentement des personnes concernées, et la technique d'anonymisation des données ne présentait pas de garantie suffisante et permettait toujours de re-identifier les individus.

Que pensez-vous de Linky, cette nouvelle génération de compteurs communicants qui renseignent sur nos consommations d'électricité en temps réel ?

▶ La Cnil a travaillé avec tous les acteurs du secteur des compteurs communicants pour élaborer dès 2014 un pack de conformité, un guide, et des recommandations pour qu'ils puissent déployer leurs services conformément à la loi.

Par exemple, dans le cas de Linky, ce compteur de la société Enedis (ex-ERDF), la Cnil a été consultée en amont sur la conformité du système aux règles de protection des données, et plus particulièrement sur la courbe de charge qui permet de savoir en temps réel quelle est consommation d'électricité dans le foyer. Celle-ci pourrait en effet permettre de déduire des informations sur la vie privée, notamment le nombre de personnes présentes dans le logement et leurs activités. La Cnil a demandé que cette courbe ne soit remontée à Enedis que par tranche d'une heure, après consentement explicite de l'abonné qui peut à tout moment s'opposer au stockage de ses données dans son compteur ou chez Enedis.

Ce qui caractérise ces nouvelles formes de surveillance et de contrôle de la population, c'est leur côté indolore et sournois. Qu'il s'agisse de capteurs ou de caméras, tout est miniaturisé, les objets connectés sont partout, avec nous… Ce paysage urbain "idéal" nous conduit-il à une société totalitaire où toute forme d'anonymat serait bannie ?

▶ Le risque, c'est en effet l'interconnexion totale de toutes les données sans que les personnes aient la capacité de faire valoir leurs droits. La ville est une société où cohabitent la vidéosurveillance, les réseaux sociaux, les aspirateurs intelligents, les compteurs connectés, etc. Autant de collecteurs de données qui tissent la smart city. Le plus grand risque serait que les données se retournent contre les personnes qui les mettent à disposition pour des services, privés et publics. D'où l'importance, pour un régulateur comme la Cnil, de faire en sorte que chacun de ces acteurs pris individuellement respecte le cadre légal. L'idée d'une "tour de contrôle numérique" qui gérerait l'ensemble des activités

de la ville symbolise ce risque, un système qui potentiellement mettrait fin à toute idée d'anonymat dont la ville était jusque-là le rempart. Comment s'en prémunir ? En faisant respecter le cadre applicable à la protection des données par chacun des acteurs, notamment en garantissant que la collecte des données est compatible avec les finalités de leur traitement ; et en certifiant les techniques d'anonymisation, notamment pour les données ouvertes en open data (par exemple les données de transport). Il faut aussi encourager le développement des technologies protectrices de la vie privée. Il n'y a pas une solution unique, mais un faisceau de réponses.

Comment concilier la nécessaire protection des individus telle qu'elle ressort du Règlement européen sur la protection des données et les promesses d'une meilleure qualité de vie dans la ville de demain ?

▶ Au niveau de la collectivité, l'obligation à partir du mois de mai 2018 d'avoir un DPO (délégué à la protection des données) qui est chargé de mettre en œuvre la conformité des traitements au RGDP (Règlement général de la protection des données) est une garantie importante. Cette personne sera notre interlocuteur privilégié. Par ailleurs, pour des services qui sont proposés par des acteurs non européens, le nouveau règlement pose un principe de "territorialité de la personne". Dès lors qu'un service s'adresse à des Européens, les autorités européennes de protection se considéreront comme légitimes à répondre à une plainte. Si, par exemple, une personne se plaint d'une violation de sa vie privée par un réseau social situé hors UE (qui s'oppose, par exemple, à l'effacement de ses données...), la réponse sera européenne. Jusqu'à présent, il était difficile de toucher ces acteurs. Désormais, le "bloc" européen de protection des données s'impose sur le plan tant juridique que politique, car c'est tout un marché qui est concerné et son poids économique ne manquera pas de peser sur le respect du droit par les acteurs concernés.

LIRE aussi

➤ AU TRIBUNAL DE L'INTERNET #62 ! Aurons-nous encore une vie privée dans la ville intelligente de demain ?

Sur le même sujet

➤ AU TRIBUNAL DE L'INTERNET #62 ! Aurons-nous encore une vie privée dans la ville intelligente de demain ?