Avancé des travaux de la CNIL sur les objets connectés

[DONNEES PERSONNELLES]
Communiqués de la CNIL des 23 septembre et 3 octobre 2016

Le marché des objets connectés connait actuellement un fort développement en France, accompagné par celui des réseaux dédiés à la communication entre ces objets où la concurrence entre les différents prestataires s'accentue. Dans ce contexte, les différentes autorités nationales de protection des données réunies au sein du « GPEN » (*Global Privacy Enforcement Network*) ont lancé en avril dernier un audit international portant sur l'internet des objets [Netcom juin 2016 : « *Lancement d'un audit international consacré aux objets connectés* », communiqué de la CNIL] sur son site internet.

Fin septembre, la CNIL a dressé un bref bilan de ces opérations. Ainsi, elle rappelle tout d'abord que les contrôles, qui ont portés sur 300 objets, se sont concentrés sur trois aspects : (i) l'information des utilisateurs ; (ii) la sécurité des données ; et (iii) le niveau de contrôle des utilisateurs sur l'exploitation de leurs données.

Au niveau international, les autorités ont principalement relevé que l'information des utilisateurs était insuffisante. Ainsi, la majorité des objets testés ne fournissait pas suffisamment de détails en ce qui concerne les modalités de suppression des données, les conditions de stockage ainsi que la collecte et l'exploitation des données.

La CNIL livre également ses propres conclusions, portant sur les douze objets qu'elle a pu tester, dans les domaines de la domotique, de la santé et du bien-être. Pour l'autorité française, la principale critique au regard des pratiques actuelles est que l'information livrée, bien qu'accessible et claire, n'est pas suffisamment spécifique aux objets effectivement utilisés et ne permet pas de savoir ce qu'il adviendra exactement des données. Sur les deux autres aspects des contrôles, en revanche, la CNIL ne relève pas de manquement particulier. Elle estime en effet que les utilisateurs ont un contrôle satisfaisant sur leurs données et que les mesures de sécurité mises en place étaient adéquates. Les observations des autorités nationales concernant la sécurité doivent cependant être mises en perspective avec l'attaque du système de nom de domaine « Dyn » du 21 octobre 2016, ayant conduit à l'inaccessibilité de nombreux sites internet pendant plusieurs heures. En effet, il apparaît que cette attaque par « déni de service distribué » d'une ampleur sans précédent a été perpétrée au moins en partie à l'aide de milliers d'objets connectés, préalablement piratés afin de pouvoir être pilotés à distance (c'est-à-dire dans ce cas précis, afin d'envoyer des milliers de requêtes aux serveurs de Dyn pour provoquer une surcharge). La CNIL et ses homologues se réservent néanmoins la possibilité de procéder dans le futur à de véritables contrôles si cela était nécessaire.

Enfin, quelques conseils d'ordre général sont distillés aux utilisateurs. Ainsi, la CNIL rappelle la nécessité de choisir un mot de passe « fort », d'utiliser un pseudonyme lorsque cela est possible, de limiter le partage de ses données et de les supprimer lorsqu'elles ne sont plus utiles.

Cet audit doit être mis en parallèle avec la préparation par la CNIL de son sixième « pack de conformité » dédié aux véhicules connectés. La CNIL a en effet entamé ces travaux en mars 2016, et propose aujourd'hui un point d'étape. Trois scénarios sont étudiés par la CNIL : à la suite de la collecte dans le véhicule, les données peuvent en effet : (i) y rester ; (ii) être transmises à l'extérieur pour les besoins d'un service donné (ex : les contrats d'assurance de type « *pay as you drive* ») ; ou (iii) être transmises à l'extérieur pour ensuite déclencher une action automatique dans le véhicule (ex : infotrafic). A ce stade, la CNIL rappelle seulement quelques points. Tout d'abord, elle réaffirme le caractère personnel de certaines données traitées dans le cadre des véhicules connectés (ex : données relatives aux trajets rattachées à une personne physique, notamment à l'aide du numéro d'immatriculation ou de série du véhicule). Ainsi, le pack aura notamment pour objectif de sensibiliser les acteurs sur les obligations générales liées aux traitements de données personnelles, et notamment à adopter le principe d'une protection dès la conception (« *privacy by design* », principe contenu expressément au sein du Règlement Général sur la Protection des Données).

Sylvain NAILLAT