L'Internet des objets est-il compatible avec la vie privée ?

Publié le 01 juillet 2014, à 12h06

Les experts du numérique, Objets connectés, Internet

L'Internet des objets est-il compatible avec la vie privée ? © DR

Déjà les objets communiquent de plus en plus entre eux. Demain, ils seront des milliards à échanger des informations. Autant de données captées, souvent à notre insu, sur notre vie privée. Résistera-t-elle à cet Internet des objets ?

En septembre 2013, aux Etats Unis, des dysfonctionnements dus à des mesures de confidentialité et de sécurité inappropriées ont porté atteinte à la vie privée de centaines d'Américains.

La société Trendnet commercialise des caméras de surveillance connectées à Internet (*SecurView*), permettant d'assurer la sécurité d'une habitation ou la vidéosurveillance de bébés. Suite à une faille logicielle, toute personne en possession de l'adresse IP d'une de ces caméras a pu visualiser, et dans certains cas écouter, les informations transmises en ligne. Des pirates ont ainsi publié en ligne, en direct, les signaux émis par près de 700 caméras de particuliers, dévoilant en temps réel les activités de leurs utilisateurs (bébés endormis, adultes vaquant à leurs occupations quotidiennes...). Trendnet avait en outre transmis les identifiants des utilisateurs en texte clair et lisible sur le net.

La Federal Trade Commission (FTC), chargée aux Etats Unis de la protection des consommateurs et de la concurrence (équivalent de notre DGCCRF), a jugé que les pratiques de sécurité laxistes de Trendnet ont violé la vie privée de centaines de consommateurs, en rendant possible la consultation publique de leurs données sur Internet, et que les pratiques de Trendnet étaient trompeuses et déloyales.

Elle a imposé à Trendnet d'établir un programme exhaustif de sécurité de l'information, de se soumettre à un audit tiers tous les deux ans pendant les vingt prochaines années, d'informer les clients sur les questions de sécurité soulevées par ses caméras ainsi que sur la disponibilité de mises à jour logicielles destinées à les corriger, et de fournir une assistance technique gratuite pour les deux ans à venir pour aider ses clients à mettre à jour ou désinstaller les caméras.

Cette affaire a des retombées aux Etats-Unis et en Europe (notamment en France) pour toutes les entreprises commercialisant des appareils connectés à Internet, qui doivent assurer la sécurité et la confidentialité des données personnelles que ces appareils collectent, stockent et échangent entre eux.

COMMENT ASSURER LA SÉCURITÉ ET LA CONFIDENTIALITÉ DES DONNÉES PERSONNELLES ?

Les opérateurs télécoms et les fournisseurs d'accès à Internet sont soumis à certaines obligations :

- depuis 2004 (CPCE art. L 34-1) : garantir la confidentialité et l'intégrité des données à caractère personnel collectées, conservées et traitées,

- depuis 2011 (dir.2009/136/CE, 25-11-2009 et ord. 2011-1012, 24-8-2011), en cas de vol, de destruction ou d'accès à ces données par des personnes non autorisées : notifier toutes les failles de sécurité la Commission nationale de l'informatique et des libertés (art. 34 bis loi 6-1-1978) et informer les personnes concernées par cette faille, victimes actuelles ou potentielles, sauf s'ils prouvent avoir mis en œuvre les mesures de protection technologiques appropriées, rendant les données incompréhensibles à toute personne non autorisée à y avoir accès.

Au-delà des opérateurs télécoms et fournisseurs d'accès à Internet, depuis juin 2013, la Commission européenne a publié un règlement (UE 611/2013, 24-6-2013) obligeant l'ensemble des acteurs collectant, conservant ou traitant des données à caractère personnel, à prendre des mesures concrètes en matière d'information des autorités et du public en cas de faille de sécurité.

Objectifs : assurer un traitement similaire aux individus situés à travers l'Union européenne et simplifier la tâche des entreprises actives dans différents Etats membres de l'Union, pouvant désormais appliquer le même protocole d'actions en cas de brèche de données, quelle que soit la loi nationale applicable. S'agissant d'une réglementation européenne applicable en France depuis le 25 août 2013, les fournisseurs de services de télécoms doivent contrôler la conformité de leurs pratiques et procédures de sécurité existantes.

Pour éviter d'éventuelles sanctions, notamment pénales pouvant atteindre 300 000 euros d'amende et 5 ans de prison (art. 226-16 à 226-24 et R 625-10 à R 625-13 du Code pénal), et davantage dés l'adoption du projet de règlement européen, les fournisseurs de services télécoms ont tout intérêt à :

- établir un programme complet en matière de protection, de sécurité et de confidentialité de la vie privée
- se soumettre périodiquement à un audit indépendant.

Frédéric Forster et Edouard Lemoalle, Alain Bensoussan Avocats