Catherine Forget, Avocate, Chercheuse au CRIDS

L'art du détournement des objets à des fins de surveillance

Géolocalisation, vidéosurveillance, authentification, biométrie... les outils de surveillance s'invitent de plus en plus régulièrement dans les gadgets de notre quotidien. Sans en être forcément conscients, nous sommes l'objet voire les objets d'une surveillance globale constante.

La révolution informatique a eu pour incidence d'apporter un champ nouveau à la surveillance. Que cette dernière soit commerciale ou sécuritaire, les technologies permettent d'initier et de récolter une quantité incroyable de données grâce à des méthodes particulières. La géolocalisation d'une personne, c'est-à-dire la localisation d'une personne avec précision et en temps réel, peut s'effectuer au moyen d'un téléphone portable. En cherchant le réseau, l'appareil se connecte à des antennes relais déterminables, permettant de situer avec précision la personne et d'analyser ses déplacements. De même, le wi-fi permet de géolocaliser une personne. Un Smartphone se connecte à différentes bornes wi-fi, permettant de suivre les déplacements de l'individu. Les Global Positioning System (GPS) permettent eux aussi la géolocalisation des automobilistes, toutefois moins précisément car elle s'effectue par satellites. Soulignons cependant que ce « problème » sera résolu à bref délai. En effet, dès octobre 2015, les voitures vendues dans l'Union européenne seront équipées de « l'eCall », une petite boîte noire permettant d'alerter manuellement ou automatiquement les services d'urgence en cas d'accident localisant ainsi directement la voiture. L'objet a suscité certaines craintes, néanmoins l'Union européenne tente de rassurer, le système devrait rester « dormant » et ne s'activera qu'en cas d'incident évitant ainsi le « traçage » des automobilistes.

Transports peu privés L'eCall n'est pas le seul dispositif susceptible de surveiller les automobilistes, nos routes pullulent de caméras Automatic Number Plate Recognition (ANPR). Ces caméras détectent d'éventuelles infractions et reconnaissent automatiquement les plaques d'immatriculation. Elles peuvent également, sur base d'une liste noire, alerter les services de police si telle voiture n'est pas en ordre de contrôle technique. En outre, les piétons ne sont pas en reste. Dans un avenir proche, si ce n'est pas déjà le cas, d'autres caméras terniront encore nos rues. Par exemple, des caméras thermiques sont au point, détectant les changements de chaleur, et dès lors les corps humains. D'autres caméras intelligentes détectent les mouvements physiques ou les bruits suspects. Les utilisateurs de la Société de Transports Intercommunaux Bruxellois (STIB) munis d'une 'carte Mobib' ne sont également pas à l'abri d'un éventuel traçage. Cette carte de la STIB est en effet équipée d'une puce Radio Frequency Identification (RFID), permettant l'identification d'une personne à distance et l'enregistrement de ses données de déplacement. Les passeports biométriques comprennent également des puces RFID contenant des empreintes digitales et une photo. La biométrie s'appuie en effet sur des données biologiques ou physiologiques d'une personne pour permettre son identification.

Profilages Indépendamment de nos déplacements, notre vie intime, nos opinions politiques et culturelles sont dorénavant encodées au départ de notre ordinateur personnel. Outre une quantité incroyable de données révélées volontairement par les utilisateurs des réseaux sociaux, les opérateurs de télécommunication ont l'obligation d'enregistrer l'ensemble des métadonnées, c'est-à-dire toutes nos données générées par nos communications électroniques (liste de contacts, date, heure des échanges...), à l'exception du contenu des messages envoyés. En accédant à ces différentes données, les services répressifs peuvent établir des profils très précis des utilisateurs, leurs déplacements, leurs centres d'intérêts, etc... Les utilisateurs des smartphones étant en permanence connectés, les applications en ligne, agendas, plans des villes, réseaux sociaux sont autant d'informations collectées par les opérateurs télécoms et accessibles (sur demande) pour les autorités judiciaires.

Les nouvelles technologies sont nombreuses et la liste est encore longue... Admettant que le domaine sécuritaire « ne connaît pas la crise » et fait fi des études relatives aux risques pour la santé des mesures précitées – l'impact des ondes électromagnétiques sur notre santé...- le développement des gadgets sécuritaires n'en est qu'à ses débuts. Même si l'article 8 de la Convention européenne des droits de l'homme garantit le droit à la vie privée, et l'article 8 § 1 de la Charte des droits fondamentaux de l'Union européenne la protection des données à caractère personnel, ces droits ne sont pas absolus et le combat est ardu dans un domaine où les fantasmes sécuritaires et commerciaux ont le vent en poupe.