

La protection de la vie privée au défi de l' «Internet des objets ».*

Conçues au départ pour faciliter la gestion des stocks dans le secteur de la distribution, et donc pour suivre un produit en ne révélant qu'indirectement les comportements des consommateurs, les applications de la technologie RFID (dispositifs qui combinent des puces électroniques stockant des données à des lecteurs capables de capter celles-ci à distance) tendent à se diversifier. Elles veulent répondre à des objectifs de surveillance (filtrage de l'accès à certains lieux, contrôle des identités à distance,...), d'efficacité (adaptation de l'offre de transport public aux flux de passagers) ou de marketing (profils d'utilisateurs,...). Mais le suivi et le profilage des personnes qu'elles permettent posent de nombreuses questions en matière de respect de la vie privée.

Les enjeux pour la protection de la vie privée découlent principalement de l'invisibilité à la fois des transferts de données opérés par les systèmes RFID, et des contrôleurs de ces systèmes (à défaut de voir ceux qui nous observent, nous avons l'impression de n'être pas observés). Ils résultent aussi du défi que représente la sécurisation des systèmes RFID : si elle fait défaut, les « données RFID » que nous transportons peuvent être interceptées, sans même que nous nous en apercevions, par des tiers équipés d'un lecteur.

Pourquoi donc est-ce un problème, que nos objets « parlent de nous » ? C'est qu'une condition essentielle au développement de nos relations sociales, que protège le droit à la protection de la vie privée, est la possibilité que nous avons, en tant qu'individus, de choisir quelle information à propos de nous-mêmes nous voulons communiquer, à qui, et en quelles circonstances. Il est bien évident que les puces RFID, qui peuvent révéler le contenu des sacs, la marque des sous-vêtements, les voyages effectués en transports en commun,... peuvent en dire long à propos de leurs propriétaires, et il importe que ces derniers puissent choisir à qui ces objets racontent leur vie. À défaut, dans la mesure où ces objets racontent certains détails de nos modes de vie, indiquent nos préférences sexuelles, politiques ou religieuses, nous sentirions-nous encore libres dans nos choix si ceux-ci risquent de nous valoir d'être montrés du doigt par la majorité ? Au-delà d'une inquiétude formelle pour le respect des normes de protection des données, c'est donc de la possibilité pour l'individu de s'auto-déterminer et de définir ses relations sociales qu'il s'agit.

D'ores et déjà annoncée, l'invasion des puces, vouées à contaminer tous les objets de notre quotidien (GSM, cartes de transport, d'identité, véhicules, vêtements,...) a donc de quoi mettre mal à l'aise quiconque se soucie non seulement du droit à la protection de la vie privée, mais aussi, et surtout, des dynamiques sociales, culturelles et démocratiques auxquelles ce droit est indispensable.

Au vu de l'imprévisibilité et de la rapide diversification des scénarios d'utilisation, ainsi que de l'invisibilité des flux de données, les instruments juridiques actuels risquent fort d'être inadéquats pour prévenir les atteintes à la vie privée.. À l'aube du développement de l' « Internet des objets », le temps est venu pour le droit et la technologie d'entrer en dialogue afin que, dès le stade de la conception des dispositifs RFID, des garanties pour l'utilisateur soient intégrées à la *technologie elle-même*. C'est dans cet esprit que le Centre de recherche informatique et droit de l'Université de Namur et l'équipe de cryptographie de l'UCL travaillent sur le projet E.USER (financé par la Région wallonne) qui vise à développer des systèmes RFID répondant aux impératifs de protection de la vie privée.¹

Dr Antoinette Rouvroy, chercheuse qualifiée FNRS, Centre de Recherche Informatique et Droit (CRID), Université de Namur.

¹ Pour tout renseignement concernant ce projet, contacter Antoinette Rouvroy (antoinette.rouvroy@fundp.ac.be), François Koeune (francois.koeune@uclouvain.be) ou François-Xavier Standaert (fstandae@uclouvain.be).