Ticket de métro électronique et vie privée

François-Xavier Standaert, François Koeune
UCL Crypto Group, Université catholique de Louvain

Suivant l'exemple d'autres villes européennes, la STIB utilise des tickets de métro électroniques depuis l'été 2008. Leur mise en circulation a donné lieu à différentes réactions de chercheurs, juristes et associations de consommateurs, s'inquiétant des problèmes éthiques soulevés par ce type de technologie. Un an plus tard, l'absence de spécifications publiques et de volonté politique claire entretient toujours le scepticisme d'un certain nombre d'utilisateurs.

La RFID ou identification par radiofréquence permet d'identifier à distance des objets, animaux ou personnes, sans contact physique ni visuel. On la retrouve dans de nombreuses applications: badges ou cartes d'accès à des bâtiments, abonnements à divers services, clés de voitures, étiquettes dans les supermarchés, … En forçant le trait, on peut dire que l'utilisation de RFID s'accompagne de deux risques principaux. D'une part, il existe un problème de sécurité: il s'agit d'éviter l'usurpation d'identité dans un contrôle d'accès ou l'utilisation non autorisée d'un service. D'autre part, il existe un problème de respect de la vie privée: il s'agit d'éviter qu'une puce électronique ne révèle trop d'information sur ses utilisateurs, permette de suivre leurs déplacements, … Ce risque s'illustre facilement avec le compostage d'un titre de transport public: anonyme dans le cas d'un ticket en papier, cette opération ne l'est plus forcément lorsque le ticket est électronique. Si chaque utilisateur conserve la même carte à puce pour valider tous ses déplacements, un numéro d'identification présent dans ces cartes peut permettre d'enregistrer les dates et lieux de compostages. Il en résulte la crainte d'un contrôle accru des citoyens.

En théorie, le développement de tickets de métro électroniques est pourtant encadré par deux principes juridiques rassurants. D'une part, les lois sur la criminalité informatique sont applicables. Elles font d'une carte à puce sans contact l'élément d'un système informatique auquel un accès intentionnel sans autorisation est punissable. D'autre part, les responsables d'une infrastructure (la STIB, par exemple) sont soumis à la législation européenne sur la protection des données à caractère privé. Celle-ci fait appel au principe de proportionnalité: les données recueillies doivent être pertinentes et non excessives. En principe, le consentement préalable des individus est toujours nécessaire à la légitimité du traitement de ces données. En outre, les textes font référence à la notion de *privacy by design*. L'idée est que les développeurs de technologies doivent permettre l'application de ces règles en rendant disponibles les outils adéquats.

Prenant l'exemple des tickets de métro bruxellois, il semble qu'aucune de ces recommandations n'ait été parfaitement respectée. A peine quelques mois après leur introduction, des chercheurs ont constaté que l'identité des propriétaires, leur date de naissance, leur code postal et les lieux et heures de leurs trois derniers compostages étaient facilement accessibles à tout possesseur d'un lecteur de cartes à puces. Par rapport aux règles énoncées ci-dessus, cela implique (1) que n'importe quel « pirate » peut récupérer ces informations, (2) que l'application du principe de proportionnalité est discutable - on peut en effet se demander dans quelle mesure la STIB a réellement besoin de stocker sur une carte de métro des informations personnelles qui étaient absentes des tickets en papier - et (3) que la notion de *privacy by design* n'était pas suffisamment déployée pour assurer un haut niveau d'anonymat dans les transports publics. Ces observations sont aussi en contradiction évidente avec les propos de M. Pascal Smet, alors Ministre en charge de la Mobilité de la Région de Bruxelles Capitale, lorsqu'il déclarait que « *les trajets ne sont pas enregistrés au niveau de la carte Mobib, mais ils le sont au niveau du valideur* ».

Et pourtant, les puces RFID ne sont pas obligatoirement synonymes de contrôle accru. Protéger la vie privée de leurs utilisateurs par rapport à des tiers, ou même par rapport au gestionnaire du réseau, est possible. Des techniques cryptographiques permettent par exemple de réaliser des tickets virtuels anonymes. On peut alors prouver mathématiquement que l'identité de l'utilisateur ne peut être révélée qu'en cas de tentative de fraude. Comme dans le cas d'autres applications potentiellement ciblées par les technologies sans fil (passeport biométrique, carte d'identité, …),

ce n’est pas tant le choix d’une technologie qui menace la vie privée de ses utilisateurs que la façon dont elle est déployée. Mais la présence croissante de puces RFID dans la vie courante va aussi rendre leur régulation plus difficile. Il semble donc important d’entamer une réflexion de fond sur le sujet dès aujourd’hui afin d’instaurer des règles transparentes pour l’avenir.

En pratique, une combinaison de mécanismes juridiques et technologiques pourrait parfaitement répondre aux inquiétudes citoyennes quant à l’impact d’objets électroniques toujours plus nombreux. Mais sa mise en œuvre demande une volonté politique claire car le respect de la vie privée influence aussi le coût du service offert. Il s’agit donc de spécifier les fonctionnalités demandées, par exemple à un ticket de métro. En caricaturant, il faut choisir entre pas d’anonymat, l’anonymat par rapport aux autres usagers ou l’anonymat par rapport aux autres usagers et le gestionnaire du service. Cette décision prise, il faut ensuite mettre en place des critères d’évaluation publics permettant de convaincre le non spécialiste que l’outil technologique qu’il utilise remplit effectivement les fonctions qui lui sont demandées. Cette discussion pose la question de l’expertise scientifique. Elle souligne l’importance d’une recherche libre de contraintes comme contrepoids aux développements industriels. Elle rappelle aussi la nécessité d’associer différentes disciplines à ces développements dans une perspective préventive. Au final, une politique plus restrictive en matière de gestion des informations à caractère personnel n’est pas toujours en contradiction avec les intérêts privés. Une fois établis, des critères de respect de l’anonymat permettent également aux entreprises de valoriser une expertise qu’elles possèdent pour la plupart déjà. Une régulation transparente résultant d’un compromis crédible entre les intérêts en jeu est donc non seulement possible mais souhaitable pour tous.