

Nos libertés et le traçage électronique

Le traçage électronique, comme tant d'autres évolutions techniques, peut engendrer le meilleur et le pire. C'est pourquoi il anime un débat de fond entre optimistes, qui y voient un remède à l'insécurité sous toutes ses formes et pessimistes qui y voient un moyen de matérialiser «Big Brother»¹.

Ce traçage peut prendre de nombreuses formes: de l'enregistrement de données personnelles «classiques» à la définition de données biométriques de plus en plus précises (des empreintes digitales aux empreintes génétiques), en passant par le pistage de tous les citoyens grâce aux systèmes de radiolocalisation.

Dans le cadre de ses après-midi «Informatique et société», l'ESI² s'est intéressée en 2007 à l'un des aspects de cette vaste problématique: il s'agissait d'expliquer les techniques disponibles dans le domaine de l'identification électronique et les problèmes liés à leur utilisation.

Les trois exposés du 12 mars 2008, en prolongation de l'après-midi de 2007 (voir Espace de Libertés n° 355), traitaient du traçage électronique proprement dit. En effet, il ne peut y avoir de traçage électronique sans identification préalable de l'élément à tracer (personne, animal ou bien de consommation).

1. Introduction à la technologie RFID par Michaël Hauspie (IUT «A» de Lille):

La technologie RFID (Radio Frequency Identification) permet d'embarquer dans de petits objets des «étiquettes» dont la puce électronique peut communiquer avec l'extérieur à l'aide d'ondes électromagnétiques. Ses ancêtres sont le radar (1920) et les antivols placés sur les marchandises dès les années 1970. Les standards apparus dans les années 1990 ont étendu les possibilités de ces systèmes ainsi que leur champ d'application.

La différence fondamentale entre une étiquette RFID et les systèmes concurrents (codes barre ou carte à puces) se trouve dans la possibilité de lire des informations à distance. Si cette caractéristique facilite de nombreuses démarches, elle fait naître des craintes au niveau de l'identification des personnes. En effet, une carte à puce ne peut être lue à l'insu de son propriétaire. Par contre, les informations d'une étiquette RFID peuvent être lues à distance, sans que son porteur le sache.

L'étiquette RFID comprend une puce électronique jointe à une antenne. La plupart des étiquettes sont passives, l'information qu'elles contiennent ne peut être lue que par un appareillage extérieur relié à un ordinateur qui contrôle le processus. D'autres étiquettes renferment une pile qui leur permet, soit d'alimenter des capteurs qui mesureront certains paramètres d'ambiance (température), soit d'envoyer elles-mêmes des informations à un ordinateur. Ces puces actives ou

¹ Personnage de fiction du roman « 1984 » de George Orwell qui est devenu, surtout dans la culture anglo-saxonne, le symbole de l'état policier. Signalons également, qu'au Pays-Bas d'où elle est originaire, l'émission « Loft Story » s'appelle « Big Brother ».

² Ecole Supérieure d'Informatique

semi-passives sont destinées au suivi de qualité des produits de grande consommation (vérification du respect de la chaîne du froid).

Il est facile de neutraliser une puce RFID en plaçant un écran entre celle-ci et le lecteur (papier aluminium), mais peu d'utilisateurs sont au courant.

Par ailleurs, certaines personnes ne craignent pas de se faire injecter une puce RFID à l'instar d'animaux de compagnie. Parmi les cas actuellement recensés, on trouve des clients VIP de discothèques qui s'identifient directement pour le paiement de leurs consommations (Danemark, Pays-Bas) mais aussi des personnes nécessitant des traitements médicaux lourds qui transportent ainsi sur elles tout leur dossier médical (USA).

Un problème potentiel de l'utilisation des lecteurs RFID a peu été investigué: on ignore à peu près tout de l'impact des rayonnements électromagnétiques sur la santé des personnes qui les côtoient journellement (dans les entrepôts ou les magasins).

2. Etre tracé ou empêcher la traçabilité par Olivier Markovitch (ULB)

L'utilisation des puces RFID dans les passeports belges a soulevé de nombreuses critiques quand des chercheurs de l'UCL ont montré qu'aucun mécanisme de sécurité ne protégeait les informations qui s'y trouvaient. La lecture de telles données à l'insu de leur porteur permet à des personnes mal intentionnées de suivre le porteur, mais encore d'usurper son identité et de commettre des délits en son nom. Pour remédier à cela, un code a été imprimé dans les nouveaux passeports. Il doit être encodé à la lecture de l'étiquette RFID pour accéder en clair aux données. Il semblerait cependant que les algorithmes gérant ces codes ne sont pas très difficiles à «craquer».

Internet représente également une source d'information sur les personnes. La majorité de ses utilisateurs se sent protégée par l'anonymat des échanges sur la «toile». Internet est cependant loin de garantir un tel anonymat.

Si la plupart des systèmes d'exploitation actuels masquent l'adresse du poste de travail d'où sont envoyés les messages, il est possible de retirer de nombreuses informations de l'en-tête des e-mails: qui est en copie, quels ont été les transferts entre boîtes, etc.

Les «cookies» contiennent des informations déposées par les serveurs web sur les ordinateurs. Ils permettent entre autres d'envoyer à chaque utilisateur des publicités en relation avec ses centres d'intérêt déduits des sites fréquemment visités. Le blocage des cookies est toujours possible, mais au prix d'une limitation d'accès à des services intéressants pour l'utilisateur.

Un grand nombre d'applications Internet, telles que les serveurs de mail ou les moteurs de recherche (dont Google, leader du marché) ne sont gratuits que parce que les publicitaires les financent. Grâce aux cookies, les fournisseurs de ces applications récoltent de nombreuses informations sur les habitudes des internautes. Cela permet de dégager des tendances utiles pour les annonceurs, et de rendre l'utilisation d'Internet parfois très désagréable vu le nombre de publicités non demandées qui s'affichent lors de simples opérations.

En principe, ces informations ne permettent pas d'identifier précisément un utilisateur, mais il n'est pas impossible que, par recoupements, suite aux fusions et acquisitions d'entreprises du secteur, une entreprise comme Google puisse y arriver.

Il existe une panoplie d'outils qui permettent aux internautes d'éviter de recevoir des publicités indésirables ou de transmettre des informations confidentielles à des personnes non concernées.

Les messages peuvent être chiffrés ou masqués à la vue des «espions» du net. Ces outils sont facilement accessibles mais inconnus de la majorité des utilisateurs courants d'Internet.

3. Principes juridiques en lien avec les technologies de traçage par François Dubuisson (ULB)

Les grands principes de protection de la vie privée se retrouvent dans notre Constitution et dans la convention européenne des droits de l'homme.

La loi belge sur le traitement informatique de données touchant à la vie privée des citoyens date de 1992, époque à laquelle Internet était beaucoup moins développé qu'actuellement.

Dès 1995, la Commission Européenne s'est intéressée au problème. Le «groupe de l'article 29» réunit des experts désignés cette même année pour traiter la protection des données informatiques liées à la vie privée.

Le traitement visé comporte la récolte, le stockage, l'utilisation et le transfert de données. Les données à caractère personnel sont les informations permettant d'identifier une personne physique de façon directe (adresse, nom, numéro de téléphone etc.) ou indirecte (appartenance ethnique, genre, religion, etc.)

Malgré la définition de grands principes, il existe une large part d'interprétation de ceux-ci qui conduit à des conclusions contradictoires. Par exemple, une adresse IP³ est considérée en Belgique comme une donnée personnelle: à partir d'une adresse IP, un fournisseur d'accès peut retrouver l'adresse géographique d'une personne. En France, par contre, certains jugements ont conclu qu'il ne s'agissait pas d'une donnée personnelle.

Le traitement de données personnelles visant un but légitime et clairement défini est autorisé. La durée de conservation des données doit être limitée. Le propriétaire des données sera toujours averti de l'utilisation de ses données. La personne concernée doit toujours pouvoir s'opposer à l'utilisation des informations qui le concernent.

Les services publics ont le droit d'utiliser les données personnelles (sécurité sociale par exemple). De telles données peuvent aussi être utilisées dans le cadre d'opérations légales (lutte contre la criminalité).

Il est interdit de se servir de données sensibles, touchant à l'origine ethnique, aux convictions religieuses, ou à toute caractéristique pouvant mener à des discriminations.

Une directive européenne oblige les organismes utilisant des transmissions de données par un moyen de télécommunication autre que la radio à effacer toutes les données de trafic et de communication dès qu'elles ne sont plus nécessaires à leur activité.

En Europe, la firme Google n'est impliquée dans aucune affaire touchant au respect de la vie privée. Le groupe de l'article 29 s'inquiète cependant dans une lettre adressée au président de Google de la durée de conservation des données de recherche des internautes (18 à 24 mois), de la durée de vie de ses cookies (30 ans !) ainsi que des possibilités réelles de profilage des utilisateurs de leurs services.

³ Tout ordinateur ou machine reliée à Internet se voit attribuer une adresse IP. Ces adresses peuvent être fixes ou attribuées à chaque connexion.

Conclusion

Il est très difficile de trouver un équilibre entre l'avancée de techniques qui peuvent faciliter notre vie, parfois même sauver des vies et le contrôle des excès entraînés par un usage abusif. C'est pourquoi une information de qualité sur ces sujets est indispensable, ainsi qu'une incitation à la réflexion sur la question centrale de ce débat : dans quelle mesure les avantages qu'apportent ces nouvelles techniques peuvent-ils contrebalancer les risques qu'ils font courir à notre liberté ? Par ailleurs, nous devons être conscients du fait que la défense de nos libertés passera par la volonté de chacun de nous de rester informé et d'utiliser si cela s'avère nécessaire les moyens techniques et législatifs mis à notre disposition pour protéger nos droits.

Jacqueline DE MESMAEKER, Maître-assistante à l'ESI