Protection de la vie privée sur Internet

Yves Deswarte, LAAS-CNRS

Dans notre civilisation, la protection de la vie privée est considérée comme l'une des libertés individuelles fondamentales. Dans le monde « réel », cette protection repose à la fois sur des lois et sur les difficultés matérielles et le coût de la collecte d'informations qui porteraient atteinte à la vie privée des individus. En revanche, dans le monde virtuel de l'Internet, une telle collecte est à la fois facile et peu coûteuse.

Ainsi, une adresse électronique (au même titre qu'une adresse postale ou qu'un numéro de téléphone) permet bien souvent d'identifier un utilisateur et de le localiser. De même l'adresse électronique d'un service permet dans de nombreux cas d'identifier un contenu d'information sensible. Par exemple, si quelqu'un consulte une « page sur la toile » contenant des informations sur les traitements du SIDA, il est possible d'identifier cette personne simplement en analysant les données techniques de la connexion, en particulier les adresses électroniques. Or ces données techniques sont connues de tous les opérateurs impliqués dans la connexion, en particulier les fournisseurs de service Internet. Ces opérateurs sont d'ailleurs tenus de conserver ces données pendant une durée pouvant aller jusqu'à un an (article 32-3 du code des postes et télécommunications).

Les opérateurs ne sont pas les seuls à pouvoir obtenir de telles informations. Ainsi tout site sur la toile peut enregistrer l'adresse électronique de toute demande de consultation de chacune de ses pages. Ces serveurs accumulent souvent beaucoup d'autres informations personnelles. S'il s'agit d'un service payant, le serveur peut demander au client de remplir un formulaire avec ses nom et prénom, son adresse postale, son numéro de carte de crédit, etc. En général, le serveur enregistrera aussi automatiquement d'autres informations, comme la date, l'heure et l'objet de la transaction, l'adresse électronique de la connexion du client, et toute autre information susceptible d'aider à résoudre d'éventuels conflits. Au-delà de la simple transaction, ces informations sont souvent utilisées par les serveurs pour des desseins légitimes, comme une meilleure gestion des relations avec la clientèle, ou pour d'autres moins avouables, comme la diffusion massive de publicité ou la constitution d'un profil pour chaque acheteur (en recoupant les informations de diverses transactions) pour mieux cibler des actions publicitaires. Les bases de données contenant ces informations sont un patrimoine précieux pour ces entreprises et peuvent faire l'objet d'un commerce lucratif.

Il est donc relativement facile et peu coûteux de collecter de nombreuses informations personnelles sur Internet, et de les conserver très longtemps. C'est aussi ce qui distingue ce monde virtuel du monde réel : votre marchand de journaux aura vite oublié vous avoir vendu un exemplaire du Figaro, alors qu'un serveur comme celui du New York Times pourrait identifier quel utilisateur a consulté telle page, il y a quatre ans.

Face à ces dangers, il existe une protection légale, au niveau français par la loi « Informatique et libertés », le code des postes et télécommunications ou la nouvelle loi pour la confiance dans l'économie numérique, et au niveau européen par les directives 95/46/EC sur la protection des données à caractère personnel et 2002/58/EC sur la vie privée et les communications électroniques. Mais cette législation est peu connue et mal appliquée : elle est souvent considérée comme difficile à mettre en œuvre par les entreprises et il est difficile de vérifier si elle est respectée.

Il faut donc aussi développer des technologies de préservation ou d'amélioration de la vie privée, ce qu'on appelle en anglais les *Privacy-Enhancing-Technologies* ou *PETs*. Il est ainsi possible de couper le lien entre adresse électronique et individu, par l'utilisation de relais d'anonymat ou l'utilisation d'adresses dynamiques. Il est également possible de gérer des identités virtuelles multiples, par exemple par l'utilisation de pseudonymes ou de plusieurs boîtes aux lettres. Des recherches en cours tendent à minimiser la distribution d'informations personnelles. Ainsi dans le cadre d'une transaction de commerce électronique, le marchand doit être assuré de la validité du paiement, mais il n'a pas besoin de connaître l'identité ni l'adresse de l'acheteur ; la banque de l'acheteur a besoin de connaître l'identification du compte du marchand, pas son identité ni l'objet de la transaction ; l'entreprise de livraison ne doit connaître que l'adresse de livraison et les caractéristiques physiques de l'objet à livrer, mais pas l'identité de l'acheteur ni le montant de la transaction, etc. On peut aussi concevoir des mécanismes permettant d'autoriser ou d'interdire l'accès à un service ou à une information en fonction de caractéristiques de l'utilisateur, comme le fait qu'il soit majeur ou qu'il soit à jour de ses cotisations, sans qu'il n'ait besoin de dévoiler son identité. Enfin, des relations contractuelles entre client et serveur devraient permettre au client de négocier l'utilisation des données personnelles qu'il transmet au serveur, en imposant par exemple que cette utilisation soit limitée à une seule transaction et que ces données soient effacées sous huitaine. Ceci suppose le développement de mécanismes de sécurité capables de garantir le respect de telles exigences.

Bien sûr, ces technologies de préservation de la vie privée doivent être compatibles avec les besoins des organisations chargées légalement de la lutte contre la criminalité ou le terrorisme. Il faut donc privilégier des solutions basées sur des tiers de confiance, capables à la fois de protéger les individus et de fournir à la justice les preuves dont elle aurait besoin.

La protection de la vie privée sur Internet nécessite donc des recherches et développements nouveaux, mais aussi une motivation accrue des citoyens et des entreprises pour que soient mis en place des moyens efficaces et économiquement viables.