La vie priveÌ•e nâ€™existe pas sur Internet

Description

Quâ€™est-ce quâ€™une donnÃ©e personnelle, une adresse IP, un cookie ou encore Â« les traces Â» circulant sur Internet ? Quels sont les enjeux de lâ€™interconnexion des fichiers comportant des donnÃ©es personnelles Ã lâ€™heure du tout numÃ©rique ?

A lâ€™occasion dâ€™une interview Ã la BBC, Sir Tim Berners-Lee, lâ€™un des fondateurs de lâ€™hypertexte Ã lâ€™origine du World Wide Web sâ€™inquiÃ©tait : Â« *Je veux savoir, si je consulte (sur le Web) des livres sur certaines formes de cancer, que mon assurance ne va pas augmenter de 5 % parce quâ€™ils mâ€™imaginent malade* Â»… Pourquoi pareille inquiÃ©tude ? Quel danger lâ€™informatique peut-elle faire courir aux particuliers ?

Si lâ€™on en croit le professeur Jean Morange, câ€™est le fichage des individus qui se rÃ©vÃ¨le dangereux. En revanche, lâ€™informatisation des fichiers sâ€™avÃ¨re dâ€™une grande efficacitÃ©, Ã condition dâ€™Ãªtre correctement maÃ®trisÃ©e. La France figure parmi les premiers pays Ã avoir pris conscience que la vie privÃ©e pouvait Ãªtre mise en danger par lâ€™informatique : câ€™est le fondement mÃªme de la loi du 6 janvier 1978, modifiÃ©e par la loi du 6 aoÃ»t 2004, qui permet dâ€™assurer cette maÃ®trise de lâ€™informatique lorsquâ€™elle implique des donnÃ©es personnelles.

Pour comprendre les enjeux de lâ€™informatisation des fichiers Ã lâ€™heure du Web 2.0 qui place lâ€™utilisateur au centre du systÃ¨me, il convient dâ€™apporter quelques prÃ©cisions sur le fonctionnement du Web, dâ€™Internet ainsi que le rÃ©gime juridique qui sâ€™y rapporte.

Internet et le Web : fournisseur dâ€™accÃ¨s au rÃ©seau et Ã©diteurs de services du Web

Internet ayant Ã©tÃ© popularisÃ© par l’apparition du World Wide Web, les deux sont parfois confondus. En rÃ©alitÃ©, Internet est le rÃ©seau informatique mondial qui rend accessible au public des services dont le World Wide Web ou le courrier Ã©lectronique, la messagerie instantanÃ©e ou encore les systÃ¨mes de partage de fichiers poste Ã poste (*peer-to-peer*). Le World Wide Web est un systÃ¨me hypertexte public utilisant le rÃ©seau Internet et qui permet de consulter, Ã lâ€™aide dâ€™un logiciel de navigation (Internet Explorer, Opera, Firefox etc.), des services hÃ©bergÃ©s sur des serveurs. Le droit distingue ainsi, parmi les acteurs privÃ©s, ceux dont lâ€™objet est de fournir au public un accÃ¨s au rÃ©seau Internet, comme Orange, Free, Neuf, NumÃ©ricable…, de ceux qui rendent accessibles sur le Web un service, comme Google, Facebook ou Fnac.com Ã©tablissant ainsi la diffÃ©rence entre des prestataires techniques et des Ã©diteurs de contenus.

Le droit impose aux fournisseurs dâ€™accÃ¨s au rÃ©seau de conserver les donnÃ©es de connexion de leurs clients et demande aux Ã©diteurs de services du Web dâ€™effacer les donnÃ©es personnelles de leurs utilisateurs. Pour comprendre ce paradoxe, il faut distinguer les donnÃ©es de connexion des donnÃ©es personnelles et autres types de donnÃ©es informatiques.

DonnÃ©e de connexion, donnÃ©e personnelle, adresse IP et cookie

Pour accÃ©der de chez soi Ã un site Web, chaque ordinateur connectÃ© au rÃ©seau Internet est identifiÃ© par un numÃ©ro unique qui permet de le retrouver parmi lâ€™ensemble des ordinateurs connectÃ©s. Ce numÃ©ro unique sâ€™appelle lâ€™adresse IP (Internet Protocol) et prend la forme dâ€™une suite de chiffres : 212.85.150.134. Celle-ci est attribuÃ©e Ã lâ€™internaute par son fournisseur dâ€™accÃ¨s. A chaque adresse IP correspond un client. Lâ€™adresse IP est donc un peu lâ€™Ã©quivalent du numÃ©ro de tÃ©lÃ©phone pour les ordinateurs connectÃ©s Ã Internet.

Lâ€™adresse IP est-elle considÃ©rÃ©e ou non comme une donnÃ©e personnelle ? En France, une donnÃ©e personnelle est dÃ©finie par loi du 6 janvier 1978 relative Ã l'informatique, aux fichiers et aux libertÃ©s dite Â« Informatique et libertÃ©s Â» comme Â« *toute information relative Ã une personne physique identifiÃ©e ou qui peut Ãªtre identifiÃ©e, directement ou indirectement, par rÃ©fÃ©rence Ã un numÃ©ro d'identification ou Ã un ou plusieurs Ã©lÃ©ments qui lui sont propres* Â». Câ€™est par exemple le nom et le prÃ©nom dâ€™une personne qui permet une identification directe de lâ€™individu ou le numÃ©ro de tÃ©lÃ©phone qui permet lâ€™identification indirecte de son propriÃ©taire.

En France comme en Europe puisque lâ€™adresse IP permet de remonter Ã lâ€™ordinateur dâ€™un internaute grÃ¢ce Ã son fournisseur dâ€™accÃ¨s, il sâ€™agit dâ€™une donnÃ©e Â« indirectement nominative Â», permettant lâ€™identification indirecte dâ€™un individu.

Aux Etats-Unis, en revanche, oÃ¹ les risques dâ€™atteinte Ã la vie privÃ©e peuvent Ãªtre minorÃ©s au profit des enjeux Ã©conomiques du commerce informatique, de la libre circulation des donnÃ©es et la libertÃ© des Ã©changes dont elles sont lâ€™objet, les donnÃ©es informatiques dont les adresses IP ont Ã©tÃ© considÃ©rÃ©es comme les biens dâ€™une Ã©conomie de marchÃ© et ne sont pas considÃ©rÃ©es comme une donnÃ©e personnelle.

Pourquoi la loi impose-t-elle aux fournisseurs dâ€™accÃ¨s Ã Internet (qui ne le faisaient pas avant) de conserver les donnÃ©es de connexion ? Depuis septembre 2001 et les objectifs de sÃ©curitÃ© qui en dÃ©coulent, la conservation des donnÃ©es de connexion fait lâ€™objet de nombreux dÃ©bats. La loi du 21 juin 2004 pour la confiance dans lâ€™Ã©conomie numÃ©rique et la loi du 23 janvier 2006 relative Ã la lutte contre le terrorisme imposent aux fournisseurs dâ€™accÃ¨s la conservation des Â« donnÃ©es de connexion Â», pendant 12 mois, pour diffÃ©rentes finalitÃ©s dont la recherche, la constatation et la poursuite des infractions pÃ©nales ainsi que la lutte contre le terrorisme.

Cette prÃ©occupation sÃ©curitaire est Ã©galement relayÃ©e par la directive europÃ©enne 2006/25/CE du 15 mars 2006 qui prÃ©voit une conservation des donnÃ©es gÃ©nÃ©rÃ©es ou traitÃ©es dans le cadre de la fourniture de services de communications Ã©lectroniques accessibles au public ou de rÃ©seaux publics de communication pendant une durÃ©e allant de 6 Ã 24 mois et dont la finalitÃ© est Â« *la recherche, la dÃ©tection et la poursuite dâ€™infractions graves telles quâ€™elles sont dÃ©finies par chaque Etat membre dans son droit interne* Â». La loi impose ainsi aux fournisseurs dâ€™accÃ¨s au rÃ©seau de conserver les donnÃ©es permettant dâ€™identifier une personne Ã des fins de police prÃ©ventive.

Pourquoi la CNIL demande-t-elle alors aux fournisseurs de services du Web (comme Google, Yahoo!, ou Facebook) de ne pas conserver indÃ©finiment les donnÃ©es de connexion ? Le World Wide Web est un service accessible sur le rÃ©seau Internet. Parmi les trÃ¨s nombreux services accessibles sur le Web, les moteurs de recherche, les rÃ©seaux sociaux ou encore les sites de commerce Ã©lectronique sont parmi les plus utilisÃ©s.

La collecte des donnÃ©es effectuÃ©e sur les sites Web est rendue possible grÃ¢ce aux cookies, ces petits fichiers dits Â« texte Â» placÃ©s sur le disque dur dâ€™un ordinateur lorsquâ€™il est connectÃ© pour la premiÃ¨re fois Ã un site Web. Le cookie est installÃ© par le site Web visitÃ©, via le navigateur Internet, sur le disque dur de lâ€™ordinateur. Les cookies permettent au site Web qui les Ã©met de Â« reconnaÃ®tre Â» lâ€™internaute en recueillant un certain nombre dâ€™Ã©lÃ©ments dâ€™identification : lâ€™adresse IP, le systÃ¨me dâ€™exploitation de son ordinateur (Windows, Mac, Linux…), le navigateur utilisÃ©, ainsi Ã©ventuellement que des informations statistiques comme les pages consultÃ©es, le nombre de visites, les actions effectuÃ©es sur le site. Les habitudes de consultation de lâ€™internaute concernÃ© sont ainsi repÃ©rÃ©es.

En France, mÃªme si une entreprise offrant un service sur le Web nâ€™a dâ€™Ã©tablissement ni en France ni en Europe, le fait dâ€™enregistrer un cookie dans lâ€™ordinateur de celui qui sâ€™y connecte, rend le droit applicable puisque lâ€™objet mÃªme dâ€™un cookie est de traiter des donnÃ©es informatiques, dont lâ€™adresse IP qui est une donnÃ©e Â« indirectement nominative Â».

Les donnÃ©es collectÃ©es par les moteurs de recherche

Quand un internaute tape le mot Â« voiture Â» sur un moteur de recherche comme Google ou Yahoo!, la requÃªte est envoyÃ©e de son ordinateur vers les serveurs du site Web qui recherche les rÃ©sultats pertinents et les affiche ensuite sur lâ€™ordinateur de lâ€™internaute. Les moteurs de recherche conservent les traces de ces requÃªtes appelÃ©es Â« logs de connexion Â» et place Ã©galement un cookie dans lâ€™ordinateur de lâ€™internaute.

Ces Â« logs de connexion Â» concernent un certain nombre de donnÃ©es dont lâ€™adresse IP, la requÃªte, le navigateur Internet, et dâ€™autres informations relatives Ã la navigation. Jusquâ€™Ã

rÃ©cemment, Google conservait ainsi ces Â« logs de connexion Â» pendant 24 mois, aprÃ¨s quoi les deux derniers chiffres de lâ€™adresse IP Ã©taient dÃ©truits et un nouveau numÃ©ro de cookie Ã©tait attribuÃ© Ã lâ€™internaute. Puis Google a volontairement ramenÃ© cette durÃ©e de conservation des donnÃ©es personnelles Ã 18 mois. Cependant le droit applicable aux moteurs de recherche Ã©tant celui de la directive europÃ©enne du 24 octobre 1995 relative Ã la protection des personnes physiques Ã lâ€™Ã©gard du traitement des donnÃ©es Ã caractÃ¨re personnel et Ã la libre circulation de ces donnÃ©es, cela signifie quâ€™ils ne sont pas tenus dâ€™enregistrer les adresses IP des internautes qui utilisent leur service.

Cette directive est dâ€™ailleurs applicable Ã tous les sites Web, soit du fait de leur Ã©tablissement dans lâ€™un des pays de lâ€™Union europÃ©enne, soit parce quâ€™ils ont recours Ã des moyens de traitement des donnÃ©es personnelles comme les cookies. Or, comme les moteurs de recherche amÃ©ricains ne considÃ¨rent pas lâ€™adresse IP comme une donnÃ©e personnelle, ils estiment que la durÃ©e de conservation des Â« logs de connexion Â», dont lâ€™adresse IP, ne rentre pas dans le champ de compÃ©tence de la protection des donnÃ©es personnelles, mais dans celui de la sÃ©curitÃ© informatique.

En rÃ©ponse, le G29, un groupe de travail regroupant les 27 Â« CNIL Â» europÃ©ennes, a adoptÃ© Ã lâ€™unanimitÃ©, le 4 avril 2008, un avis prÃ©cisant les rÃ¨gles applicables aux moteurs de recherche. Cet avis prÃ©cise notamment que les donnÃ©es personnelles enregistrÃ©es en Europe par les moteurs de recherche, doivent Ãªtre effacÃ©es au plus tard au bout de 6 mois. Lâ€™avis prÃ©cise Ã©galement les conditions dâ€™application des rÃ¨gles juridiques communautaires et formule des recommandations susceptibles dâ€™amÃ©liorer la protection et le droit des utilisateurs des moteurs de recherche. Le G29 a rappelÃ© Ã cet Ã©gard que les moteurs de recherche, Ã©tant des Â« services de la sociÃ©tÃ© de lâ€™information Â», ne sont pas concernÃ©s par la directive 2006/24/CE du 15 mars 2006 relative Ã la conservation des donnÃ©es, contrairement aux fournisseurs dâ€™accÃ¨s au rÃ©seau Internet ou aux opÃ©rateurs de tÃ©lÃ©communications.

Cela signifie que les moteurs de recherche ne sont pas lÃ©galement obligÃ©s de conserver des informations sur les connexions des utilisateurs. En pratique, un moteur de recherche comme Google ou Yahoo ne devrait donc pas conserver indÃ©finiment lâ€™historique des requÃªtes effectuÃ©es et des sites consultÃ©s par un internaute. Cet historique peut contenir des informations trÃ¨s intimes, comme des problÃ¨mes conjugaux, une opinion politique, Ã partir desquelles il est possible de dÃ©duire des habitudes de vie supposÃ©es ou un certain comportement.

Si les moteurs de recherche invoquent un certain nombre dâ€™arguments pour conserver ces donnÃ©es, arguments liÃ©s Ã la meilleure efficacitÃ© du service pour lâ€™utilisateur ou Ã la sÃ©curitÃ© informatique, leur finalitÃ© est avant tout de pouvoir dresser un profil trÃ¨s prÃ©cis des utilisateurs du service, essentiellement Ã des fins commerciales.

Les donnÃ©es collectÃ©es par les rÃ©seaux sociaux

Un site Web dit Â« de rÃ©seau social Â» est un service du Web dont lâ€™objet est de permettre Ã ses membres de publier des informations personnelles et de se Â« connecter Â» Ã ses amis ou relations professionnelles. Rien de plus utile pour retrouver un ancien camarade de classe, constituer un rÃ©seau professionnel, garder le contact avec des personnes dissÃ©minÃ©es aux quatre coins du monde. Sur le principe et dans le souci de sauvegarder les droits individuels, la loi du 6 janvier 1978 interdit de mettre ou de conserver en mÃ©moire informatisÃ©e, sauf accord exprÃ¨s de lâ€™intÃ©ressÃ©, des donnÃ©es nominatives qui, directement ou indirectement, font apparaÃ®tre les origines raciales, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales dâ€™une personne.

Or, lâ€™objet des rÃ©seaux sociaux est de sâ€™appuyer sur cet accord exprÃ¨s des internautes pour collecter et conserver en mÃ©moire ce type de donnÃ©es. En se basant sur le cÃ´tÃ© ludique, social, voire utile du service, les rÃ©seaux sociaux permettent aux internautes de se Â« ficher eux-mÃªmes Â». Le modÃ¨le dâ€™affaire de ce type de site est fondÃ© sur la gratuitÃ© du service pour lâ€™internaute en Ã©change de lâ€™utilisation Ã des fins publicitaires de ses donnÃ©es personnelles et ses interactions sociales.

Mais combien, parmi les 70 millions dâ€™inscrits sur Facebook, sont informÃ©s quâ€™ils ne peuvent plus supprimer leur compte mais simplement le Â« dÃ©sactiver Â», ce qui permet Ã Facebook de tracer les connexions entre les diffÃ©rents membres, y compris avec ceux ne souhaitant plus utiliser le service ? En sâ€™inscrivant sans vraiment lire les conditions gÃ©nÃ©rales dâ€™utilisation du site Web, les utilisateurs de Facebook ont acceptÃ© le transfert et le traitement de leurs donnÃ©es personnelles aux Etats-Unis en leur confÃ©rant un droit perpÃ©tuel et irrÃ©vocable dâ€™utiliser, de copier ou de distribuer toutes les donnÃ©es communiquÃ©es.

De plus, Facebook se rÃ©serve le droit de collecter et de compiler autour dâ€™un internaute toutes les informations publiques que ce dernier pourrait avoir publiÃ© sur dâ€™autres services du Web comme les blogs, les forums, les sites participatifs ou les plates-formes dâ€™Ã©change pour enrichir son profil, toujours Ã des fins publicitaires. Il y a donc une certaine contradiction entre lâ€™objet du service, constituer un rÃ©seau de relations sur Internet, et lâ€™encadrement juridique des pratiques commerciales qui en dÃ©coulent : dresser le profil publicitaire des membres de la maniÃ¨re la plus dÃ©taillÃ©e possible Ã partir des tous les Ã©lÃ©ments disponibles sur le Web pour offrir Ã un annonceur un ciblage prÃ©cis.

Le groupe de travail G29 publiera avant lâ€™Ã©tÃ© 2008 un avis et des recommandations Ã lâ€™attention des sites Web exploitant un rÃ©seau social comme celui adressÃ© le 4 avril 2008 aux moteurs de recherche.

Risques dâ€™usurpation dâ€™identitÃ©

L’usurpation d’identitÃ© (ou vol dâ€™identitÃ©) consiste Ã prendre dÃ©libÃ©rÃ©ment l’identitÃ© d’une autre personne, gÃ©nÃ©ralement dans le but de rÃ©aliser une action frauduleuse, comme

dâ€™accÃ©der aux comptes bancaires de la personne usurpÃ©e, ou de commettre un dÃ©lit ou un crime de maniÃ¨re anonyme. Un sondage, effectuÃ© pour le compte de la campagne britannique Get Safe Online de sensibilisation Ã la sÃ©curitÃ© informatique, avance que 15 % des utilisateurs des sites de rÃ©seaux sociaux Â« *nâ€™utilisent aucune des possibilitÃ©s pour rendre confidentielles leurs informations sur ces sites et 24 % des internautes utilisent le mÃªme mot de passe pour tous les sites* Â», que 27 % des 18-24 ans ont postÃ© des photos de tiers sans leur consentement et que 34 % des 18-24 ans, et 30 % des 25-34 ans, Â« *rÃ©vÃ¨lent des informations susceptibles dâ€™Ãªtre utilisÃ©es Ã des fins criminelles* Â».

Pour Ã©viter ces risques, lâ€™application des principes prÃ©conisÃ©s par la CNIL (et plus largement en Europe) conduit Ã recommander dâ€™effacer les donnÃ©es personnelles le plus vite possible, Ã rendre anonymes les traces et Ã refuser lâ€™interconnexion des fichiers qui ne sâ€™appuie pas sur le consentement exprÃ¨s de lâ€™utilisateur.

Les acteurs de la publicitÃ© en ligne, la publicitÃ© comportementale, le consentement de lâ€™utilisateur, lâ€™interconnexion de fichiers

Mais les fournisseurs dâ€™accÃ¨s, les sites Web et, dâ€™une maniÃ¨re gÃ©nÃ©rale, les entreprises de lâ€™informatique et des tÃ©lÃ©communications nâ€™appartiennent jamais quâ€™Ã une seule catÃ©gorie dâ€™acteurs. La sociÃ©tÃ© Google propose de trÃ¨s nombreux services sur le Web, moteur de recherche, plate-forme dâ€™Ã©change de vidÃ©os, de photos, systÃ¨me de messagerie etc. et elle a participÃ© dÃ©but 2008 aux enchÃ¨res organisÃ©es par la Federal Communications Commission (FCC) pour l'attribution de frÃ©quences, afin de devenir opÃ©rateur de tÃ©lÃ©communications aux Etats-Unis. Microsoft est Ã la fois un Ã©diteur de logiciels pour la micro-informatique, la tÃ©lÃ©phonie mobile et propose Ã©galement de nombreux services sur le Web. La CNIL demande que ces entreprises ne puissent pas systÃ©matiquement interconnecter les donnÃ©es personnelles dâ€™un service Ã lâ€™autre, Ã la suite dâ€™un rachat ou dâ€™une prise de participation, sans demander lâ€™accord explicite de lâ€™intÃ©ressÃ©.

Lâ€™Ã©lÃ©ment le plus important que les Anglo-Saxons semblent systÃ©matiquement oublier, est le consentement de la personne. En Grande-Bretagne, trois opÃ©rateurs rassemblant les deux tiers des abonnÃ©s Ã Internet, British Telecom, Carphone Warehouse et Virgin Media, ont utilisÃ©, entre septembre et octobre 2007, les services et le logiciel espion (*spyware*) de Phorm, alias 121Media, pour Ã©pier les agissements de 18 000 internautes clients de leur prestation d'accÃ¨s Ã Internet. Une surveillance qui s'est effectuÃ©e sans l'accord des personnes concernÃ©es.

Ce qui est confidentiel, ce nâ€™est pas tant notre identitÃ©, dÃ©jÃ accessible par bien dâ€™autres moyens que le Web, mais notre comportement et les liens qui rattachent ces Â« traces Â» Ã notreidentitÃ© personnelle. Si hier, la publicitÃ© sâ€™adressait Ã lâ€™audience la plus large possible ensâ€™affichant dans la rue, les magazines et dâ€™autres supports fixes, le rÃ©seau Internet offre lapossibilitÃ© de personnaliser les annonces publicitaires en les adressant Ã des publics ciblÃ©s etaisÃ©ment identifiables.

Mais quâ€™elle soit Â« contextuelle Â» ou Â« comportementale Â», cette publicitÃ© personnalisÃ©e devrait reposer sur le consentement exprÃ¨s de lâ€™utilisateur. Les grands acteurs du Net profitent actuellement du vide juridique international pour collecter un maximum de donnÃ©es Ã lâ€™insu de lâ€™utilisateur, ne sachant dâ€™ailleurs pas toujours quoi faire de cette masse dâ€™informations.

Une Ã©tude sur le sujet menÃ©e par ComScore pour le *New York Times* rÃ©vÃ¨le que Yahoo! rÃ©colte 811 informations sur chaque internaute qui visite lâ€™un de ses sites alors quâ€™il fait une recherche, un achat ou regarde une vidÃ©o. MenÃ©e en dÃ©cembre 2007 sur le trafic des sites des quinze gÃ©ants amÃ©ricains du Web (Yahoo!, Google, Microsoft, etc.), lâ€™Ã©tude montre jusquâ€™Ã quel point ces sociÃ©tÃ©s collectent les donnÃ©es gÃ©nÃ©rÃ©es par les internautes. A eux seuls, Yahoo!, Google, Microsoft, AOL et MySpace ont enregistrÃ© pas moins de 336 milliards de transmissions de donnÃ©es, le but Ã©tant dâ€™affilier chaque internaute Ã un profil publicitaire.

Des chiffres qui expliqueraient, entre autres, pourquoi Microsoft Ã©tait encore prÃªt, fin avril 2008, Ã dÃ©bourser 47 milliards de dollars pour mettre la main sur Yahoo!. Â« *Beaucoup de contrats visent en fait ces donnÃ©es* Â», explique David Verklin, directeur gÃ©nÃ©ral de lâ€™agence publicitaire Carat Americas. Croiser et compiler les donnÃ©es rÃ©coltÃ©es sur le rÃ©seau et les sites Web permet de dresser une Â« identitÃ© numÃ©rique Â» trÃ¨s prÃ©cise de lâ€™internaute. Or, si ce croisement de ces donnÃ©es est fait sans lâ€™accord de lâ€™intÃ©ressÃ©, il sâ€™agit bien lÃ dâ€™une atteinte au respect de la vie privÃ©e, puisque ces pratiques rendent possibles lâ€™identification des utilisateurs Ã leur insu pour des finalitÃ©s autres que celles pour lesquelles ils ont, dâ€™une part, signÃ© un contrat avec un fournisseur dâ€™accÃ¨s et, dâ€™autre part, acceptÃ© les conditions gÃ©nÃ©rales des sites Web quâ€™ils utilisent.

Le caractÃ¨re mondial du rÃ©seau Internet rend le contexte juridique particuliÃ¨rement complexe car lâ€™une des principales caractÃ©ristiques dâ€™une rÃ¨gle de droit est dâ€™avoir un champ dâ€™application prÃ©cis, limitÃ© Ã un territoire et suivant un champ de compÃ©tence ordonnÃ©. Or puisque les Ã©changes de donnÃ©es sur le rÃ©seau Internet sont par nature transfrontaliers et que, comme le rappelle Gustave Le Bon, Â« *le droit ne commence Ã dater que du moment oÃ¹ l'on dÃ©tient la force nÃ©cessaire pour le faire respecter* Â», toutes les pratiques sont actuellement possibles.

Pourtant, le succÃ¨s des services du Web repose Ã la fois sur la confiance de lâ€™utilisateur et sur une personnalisation des services toujours plus rÃ©ussie. A cette personnalisation doit correspondre une rÃ©flexion de fond quant au respect de sa vie privÃ©e que le doyen Carbonnier dÃ©finissait comme

Ã©tant Â« *la sphÃ¨re secrÃ¨te dâ€™oÃ¹ lâ€™individu aura le pouvoir dâ€™Ã©carter les tiers* […] *, le droit dâ€™Ãªtre laissÃ© tranquille* […] Â».

Aujourdâ€™hui, les identitÃ©s de chacun sont accessibles de plus en plus facilement sur le rÃ©seau public et de maniÃ¨re de plus en plus dÃ©taillÃ©es. FrÃ©dÃ©ric Cavazza et RaphaÃ«l Lefear, deux blogueurs ayant analysÃ© les diffÃ©rents types de donnÃ©es personnelles laissÃ©es sur le Web par les internautes en dÃ©nombrent douze : ce que je dis, ce que je partage, ce que jâ€™apprÃ©cie, ce qui me passionne, ce que je sais, ce qui me reprÃ©sente, ce que je fais, ce qui se dit sur moi, ce que jâ€™achÃ¨te, qui je connais, comment et oÃ¹ me joindre et qui atteste de mon identitÃ©… Ce sont tout Ã la fois, lâ€™identitÃ© personnelle et professionnelle, les habitudes de consommation, de jeux, le contenu gÃ©nÃ©rÃ© ou publiÃ© par lâ€™utilisateur, ses rencontres et ses rÃ©seaux dont il est question. Autant dâ€™informations privÃ©es qui, regroupÃ©es, constitueraient notre identitÃ© numÃ©rique que certains appellent aussi lâ€™empreinte numÃ©rique.

Si aujourdâ€™hui, la majeure partie des connexions Ã Internet se fait encore Ã partir dâ€™un ordinateur, fixe ou portable, il faut anticiper une sociÃ©tÃ© oÃ¹ le tÃ©lÃ©phone portable, Ã la fois objet intime et fenÃªtre sur le monde, permettra Ã©galement de sâ€™y connecter. Demain, la majoritÃ© des objets de la vie courante seront Ã©galement reliÃ©s au rÃ©seau Internet par frÃ©quence radio via des puces invisibles (*Radio Frequence IDentification*). Nous laisserons alors infiniment plus de traces sur Internet et rares seront nos dÃ©placements, nos habitudes, nos prÃ©fÃ©rences qui pourront Ã©chapper Ã un systÃ¨me informatique oÃ¹ les identitÃ©s circulent de maniÃ¨re aussi fluide et transparente quâ€™aujourdâ€™hui.

Plus la collecte massive de donnÃ©es sera rendue possible et mÃªme encouragÃ©e par certains, plus la protection des libertÃ©s individuelles, le droit au respect de la vie privÃ©e et de lâ€™intimitÃ© sera difficile Ã protÃ©ger. Câ€™est la raison pour laquelle Sir Tim Berners Lee sâ€™inquiÃ©tait dÃ©jÃ en 1997 de la finalitÃ© pour laquelle nos donnÃ©es personnelles peuvent Ãªtre collectÃ©es, compilÃ©es et analysÃ©es par des acteurs privÃ©s. A la mÃªme Ã©poque, un banquier amÃ©ricain du Maryland avait obtenu une liste de personnes atteintes dâ€™un cancer qui, croisÃ©e avec celle de ses clients, lui permettait de rejeter systÃ©matiquement les malades candidats Ã un emprunt.

Et câ€™est bien ce genre de pratiques qui rendent le travail du G29 et de la CNIL dÃ©terminant pour lâ€™avenir des services du Web et dâ€™Internet dont le succÃ¨s repose avant tout sur la confiance.

Sources :

- www.cnil.fr
- Â« Informatique, servitude ou libertÃ©s ? Â», colloque organisÃ© au SÃ©nat par la Commission nationale de l’informatique et des libertÃ©s, CNIL, 7-8 novembre 2005.
- Â« Le systÃ¨me franÃ§ais de protection des donnÃ©es personnelles Â», Annie Gruber, Les Petites Affiches,Â LPA, nÂ° 90, 4 mai 2007.
- Â« La publicitÃ© en ligne mise sur lâ€™intime Â», CÃ©cile Ducourtieux et Laurence Girard, *Le Monde*

, 11 novembre 2007.
- Â« RÃ©seaux sociaux : quand les utilisateurs sâ€™en fichent Â» Arnaud Belleil et Hubert Guillaud, Internet Actu, 20 novembre 2007.
- Â« Mais oÃ¹ va donc le Net Â», Guerric Poncet, *Le Point*, 14 fÃ©vrier 2008.
- Â« Facebook, la CNIL appelle Ã la vigilance Â», Antoine Gendreau, Anne- Laure Villedieu, *Les Echos*, 27 fÃ©vrier 2008.
- Â« Phorm and ISP Business Models Â», Ian Fogg, Jupiter Resarch, avril 2008.
- Â« Recherches en ligne : dÃ©lai maximal de 6 mois en UE pour garder donnÃ©es Â», AFP, 11 avril 2008.
- Â« Les secrets de lâ€™ogre du Net Â», Quentin Domart, Jean-Baptiste Su,Â *Lâ€™Expansion*, mai 2008.
- Â« Pas de confidentialitÃ© sur Facebook, selon la BBC Â», *Le Nouvel Observateur*, 5 mai 2008.

Categorie

1. Articles & chroniques

date crÃ©Ã©e
20 mars 2008
Auteur
jacquesandrefines