Internet, sécurité et libertés

Le modèle financier d'Internet est largement fondé sur la collecte de données personnelles sur les internautes, mais comment permettre à chacun de préserver la part de sa vie privée qu'il ne souhaite pas ouvrir à autrui ? Le désir de se prémunir contre tout risque ne va-t-il pas conduire à mettre la population sous surveillance ? En résumé, comment délimiter les contours d'un nouveau pacte social assurant un équilibre judicieux entre sécurité et liberté ?

par **Isabelle FALQUE-PIERROTIN***

INTERNET EST CONSTRUIT SUR UN PARADOXE !

Internet est né du souci qu'eurent les autorités américaines de garantir les échanges de données entre centres de recherche, en cas de conflit militaire ; cette architecture de réseau sans tête devait pouvoir survivre à une attaque nucléaire. Internet est donc un enfant de la sécurité militaire américaine. Et pourtant, tout son développement, depuis le début des années 90, s'est construit autour d'une idéologie libérale, voire libertaire, mettant en avant les nouvelles libertés offertes par le réseau : liberté d'accéder à un fonds de connaissances élargi, liberté de s'exprimer, liberté d'« aller et de venir » dans le monde entier à partir de son ordinateur… Cette ode à la liberté s'est même traduite, en 1996, par la Déclaration d'indépendance du Cybermonde, dans laquelle John Perry Barlow soulignait la rupture existant entre le monde ancien des gouvernements traditionnels et le cyberspace, celui-ci se développant à l'instar d'un « acte de nature » et tirant sa légitimité et ses règles de la seule « nétiquette », c'est-à-dire des règles collectives établies par les internautes eux-mêmes. L'auteur déclarait : « *In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace.* »

L'univers numérique nourrit donc des relations, anciennes et complexes, avec les principes de sécurité et de liberté et cet équilibre instable est inscrit au cœur même de la biologie du réseau.

Cet équilibre a, jusqu'à présent, permis un développement continu du réseau et de ses usages, conduisant plus d'un milliard d'individus à devenir internautes.

Il semble que ce pacte social fasse aujourd'hui l'objet d'un réexamen, suscitant même des inquiétudes chez certains. Le groupe des autorités européennes de protection des données, le G29, alerte ainsi l'opinion publique sur la mise en place d'une « société de surveillance », dénonçant, en vrac, la biométrie, la vidéosurveillance et la traçabilité croissante des individus en ligne. La presse grand public se fait régulièrement l'écho de la possibilité qu'a chacun d'entre nous d'être mis à nu, à travers toutes les données personnelles que nous laissons en ligne et que les différents moteurs de recherche permettent d'agréger. En s'élargissant à de nouveaux usages, en entrant dans la sphère du grand public, il semble que, progressivement, Internet change de nature et que, de libérateur, il soit en train de devenir notre nouveau maître. Est-ce l'effet d'une idéologie nouvelle, ou est-ce l'expression d'un principe de réalité ?

La situation, même si elle n'est pas justifiée, est relativement explicable. L'on assiste, en effet, à une offensive, croisée mais non coordonnée, des acteurs publics et privés en faveur d'un resserrement du contrôle de l'univers numérique et, cela, au moyen des technologies numériques elles-mêmes.

* Conseiller d'Etat, Présidente du Forum des droits sur l'Internet.

Depuis le 11 septembre 2001, les Etats sont engagés dans une « croisade » contre le terrorisme et les réseaux numériques sont un élément clé de leur vigilance, en raison de la volatilité extrême des contenus qui y circulent et de l'anonymat qui semble y régner. Les lois se sont ainsi succédées, dans tous les pays, qui renforcent les moyens de surveillance par les autorités. En France, les textes suivants ont été adoptés en moins de 8 ans : la loi sur la sécurité quotidienne (2001), la loi sur la sécurité intérieure (2003), la loi pour la confiance dans l'économie numérique (2004), la loi de transposition du paquet télécoms (2004), la loi de lutte contre le terrorisme (2006), la loi sur la prévention de la délinquance (2007), la loi de programmation pour la sécurité intérieure (LOPSI) I, et bientôt II (2009)… Au total, ce sont plus de huit textes législatifs, qui visent à règlementer la conservation des données de connexion, les nouveaux moyens d'enquête en ligne des forces répressives, etc. L'Internet fait peur, de par le potentiel de dissimulation qu'il recèle, et la traque menée dans cet *underground* fait désormais partie du quotidien de la surveillance policière. Le débat, qui a été vif, ces dernières années, sur la nécessité de demander ou non l'identité des internautes se connectant à partir d'un cybercafé, illustre bien cette crainte.

Pour des raisons évidemment très différentes, les entreprises souhaitent également renforcer leur emprise sur les réseaux, et, en particulier, sur le consommateur. Pour elles, l'enjeu est de sécuriser leurs revenus en ligne, mais aussi, dans un contexte économique toujours plus concurrentiel, où le consentement à payer diminue, de mieux « profiler » l'internaute, afin de lui proposer une offre toujours plus personnalisée. Cette dernière tendance est d'autant plus forte que les modèles économiques les plus innovants de l'Internet sont construits à partir des ressources publicitaires susceptibles d'être retirées de la valorisation de gigantesques bases de données personnelles. Publicité ciblée, publicité contextuelle ou comportementale… : les techniques publicitaires se diversifient, mais toutes se nourrissent de données à caractère personnel, collectées sur chaque internaute.

Le dispositif est particulièrement attractif pour ce dernier : les ressources, les services d'une entreprise de dimension mondiale sont, en quelque sorte, à sa disposition pour satisfaire ses propres besoins, à condition qu'il abandonne un peu de lui-même, un peu de son identité. L'engouement planétaire pour des « réseaux sociaux », tels que Facebook (140 millions d'utilisateurs) ou Myspace (230 millions), en témoigne.

Tous ces éléments vont dans le sens d'une traçabilité croissante des individus au nom de l'Etat, de la vie des affaires ou, tout simplement, de la facilité. Traçabilité dans le temps, traçabilité dans l'espace : l'individu est désormais sous surveillance.

QUE PENSENT LES INDIVIDUS DE CES ÉVOLUTIONS ?

Force est de reconnaître qu'ils sont assez ambivalents. D'une part, ils expriment une certaine inquiétude par rapport à cette situation, comme en atteste le dernier sondage Eurobaromètre (Janvier 2008), où plus des deux-tiers des internautes européens se déclarent préoccupés par le fait de laisser des données personnelles sur Internet.

Mais, d'autre part, cela ne les empêche nullement de mettre leur vie privée en ligne. Marc L., portraituré dans l'article du Tigre, avait ainsi diffusé plus de 17 000 clichés et l'ensemble de ses traces numériques permettait de dresser un profil, aussi inquiétant que complet, de sa vie personnelle et professionnelle. Cette scénarisation de l'individu, de sa vie et de ses proches, semble témoigner d'un nouveau rapport à soi et à l'intimité : je me donne en spectacle, donc j'existe ! Ce comportement est particulièrement répandu chez les jeunes, qui font l'amalgame entre une certaine culture du partage et de la communauté et une surexposition individuelle de nature narcissique. En cela, l'Internet prolonge, en quelque sorte, la culture de la Star Academy. Pour certains sociologues, cette situation n'est pas réellement préoccupante, dans la mesure où l'individu est un acteur éclairé, qui fait ses choix, en matière de vie privée, en fonction des compensations ou des services qui lui sont offerts.

Mais les arbitrages sont parfois délicats. D'une part, parce que les individus sont, en général, assez peu conscients des risques auxquels leurs usages peuvent conduire ; ils sont peu informés des pratiques des entreprises et valident, par exemple, souvent, des conditions générales d'utilisation sans même les avoir lues.

Et d'autre part, parce que le modèle social dominant les entraîne à participer à ces plateformes communautaires, à ces nouveaux lieux de socialisation, même s'ils ne le souhaitent pas vraiment. Peut-on être jeune, en 2009, sans être sur Facebook !

Certains excès les conduisent cependant à se mobiliser. Ainsi, la récente volonté de Facebook de modifier unilatéralement ses conditions générales d'utilisation, dans le sens d'une appropriation définitive par la société de tous les contenus déposés par ses abonnés, et ce, même pour ceux ayant supprimé leurs profils, a suscité une véritable opposition de la communauté, qui a contraint cette société à revenir aux conditions antérieures.

De même, l'emprise de l'Etat sur la vie privée des citoyens fait, en général, plutôt l'objet d'une contestation active de la part des internautes. Très récemment, la mise en place du fichier Edvige, succédant à l'ancien fichier des Renseignements Généraux, a relancé la polémique et les défenseurs des libertés se sont mobilisés, conduisant finalement le Gouvernement à revoir son projet.

Ces derniers exemples montrent que la situation actuelle est assez confuse et que la dialectique entre sécurité et liberté s'enrichit sans cesse de nouvelles dimensions.

© Jean-Claude Moschetti/REA

« Tous ces éléments vont dans le sens d'une traçabilité croissante des individus au nom de l'Etat, de la vie des affaires ou, tout simplement, de la facilité. Traçabilité dans le temps, traçabilité dans l'espace : l'individu est désormais sous surveillance ». *Site Internet de la CNIL (Commission nationale de l'informatique et des libertés), lors de la journée européenne pour la protection des données personnelles et de la vie privée.*

Trouver un sens aux évolutions est dès lors complexe et le manichéisme n'a pas lieu d'être ici, en dépit des apparences.

IL FAUT DISTINGUER LES QUESTIONS

En premier lieu, il est clair que le respect, sur Internet comme ailleurs, des règles de droit est une priorité. Il ne saurait exister un espace de société dépourvu de règles, connues et respectées par tous. Or, dans l'univers numérique, les risques d'actions malfaisantes contre les Etats, les sociétés ou les individus ne doivent pas être minimisés. Cyber-délinquance, escroqueries, nouvelles formes de guerre ou d'espionnage industriels… : tous ces nouveaux maux nécessitent que la police se dote de moyens d'action et de surveillance efficaces, afin que le monde numérique, qui rassemble non pas des êtres virtuels, mais bien des individus réels, reste un espace de droit. Le plan de lutte contre la cybercriminalité annoncé par la ministre de l'Intérieur, en février 2008, s'inscrit dans cette préoccupation légitime. De même, au niveau international, il est fort probable que les préoccupations de sécurité déboucheront, à plus ou moins long terme, sur la signature d'accords internationaux *ad hoc* ; les Etats et les entreprises ont trop à perdre, en terme de vulnérabilité, pour ne pas intervenir. Et cela pose nécessairement la question de la protection des données personnelles et du maintien d'une zone de liberté autour de chaque individu.

On a vu que la collecte des données personnelles participe du modèle « gratuit » actuel de l'Internet. Ce n'est pas au législateur, ni aux autorités publiques, de juger de sa pertinence, dès lors que ces informations sont collectées de façon loyale. Le respect absolu de la législation européenne relative à la protection des données s'impose donc à ces entreprises, et cela doit les conduire à des réajustements de leurs pratiques. Les sociétés elles-mêmes ne s'y sont pas trompées : ce sont elles qui, face à la montée des craintes des internautes, ont été à l'initiative, depuis deux ans, de la réflexion autour de standards mondiaux de protection des données personnelles. L'enjeu, aujourd'hui, est de déterminer à quel niveau vont se tenir les négociations entre les Etats-Unis, l'Europe et les autres pays du monde, ainsi que le caractère, contraignant ou non, de ces standards. Le G29 travaille activement à alimenter cette discussion mondiale de ses propres propositions. L'enjeu sera, le cas échéant, d'inscrire cette préoccupation dans le cadre de la réflexion sur la sécurité, au moyen, par exemple, de la définition de standards pour la conservation des données de connexion.

Enfin, les individus doivent réaliser qu'ils sont les co-constructeurs de l'univers numérique et qu'ils risquent de se faire les fossoyeurs de leur propre vie privée, s'ils n'adoptent pas des usages plus respectueux de leurs données personnelles. En France, tout particulièrement, cela doit conduire à un changement de culture. La protection de la personne y est, traditionnellement, comprise comme un enjeu collectif reposant surtout sur l'intervention de l'Etat. Cette situation ne correspond plus au monde numérique, éminemment décentralisé et ouvert. Les individus doivent participer, eux aussi, à la protection de leurs libertés : ils ne doivent pas s'endormir dans le confort du service qui leur est proposé, mais réfléchir activement au périmètre de leur vie privée qu'ils souhaitent ouvrir aux autres ou, au contraire, préserver.

Un dernier élément doit être évoqué, dans le cadre de cette analyse sur la recherche d'un équilibre optimal entre sécurité et liberté. Il y a un danger, qui se cache derrière les constatations faites plus haut sur les usages de l'Internet, et qui va bien au-delà d'un simple réajustement du curseur sécurité/liberté. C'est celui de la mise en place d'une « société de précaution ». Ce n'est pas Internet et les outils numériques qui créent cette situation, mais ils la rendent possible. Un enfant risque-t-il de se perdre, en rentrant de l'école ? Vite : il convient de le « taguer » (cette solution est effectivement pratiquée, au Japon). Des voitures volées circulent-elles ? Surveillons toutes les plaques d'immatriculation ! (cette solution, après une expérimentation concluante en Ile-de-France, va être généralisée). Il y a des risques de délinquance sur Internet ? Alors, il faut conserver toutes les données de connexion, afin, le cas échéant, de pouvoir remonter jusqu'aux coupables et de savoir ce qu'ils ont fait…

En d'autres termes, un risque, certes existant et bien réel (mais un risque, seulement) conduit à placer toute une population sous surveillance. Et cela est désormais réalisable, à la fois à cause et grâce aux nouvelles technologies ! Ainsi, s'instaure une société de gestion préventive du risque.

Cette société est celle de la peur, celle qui veut prévenir le risque, plutôt que de l'assumer. Une telle société ne doit pas être la nôtre ! En effet, elle pourrait conduire à l'enfermement ou, chez certains, à une réaction de rejet les menant à se réfugier dans l'anonymat et la dissimulation. Il ne faut certes pas négliger les dangers, mais, face à chacun d'entre eux, arbitrer, réellement et collectivement, la stratégie de réponse adaptée, le recours à des solutions techniques n'étant qu'une voie parmi d'autres.

En conclusion, la délimitation des nouveaux contours du pacte social assurant l'équilibre entre sécurité et liberté n'est donc pas simplement une nécessité conjoncturelle, liée à des variables qui se modifient : c'est une exigence fondamentale d'une société connaissant une réelle mutation de ses valeurs et de ses modes de fonctionnement. Les acteurs, tant privés que publics, en sont collectivement responsables.