Le réseau social Facebook a enregistré en avril 2009 son 200 millionième membre dans le monde (près de dix millions d'utilisateurs en France) et enregistrait en janvier 2009 près de 1,2 milliard de visiteurs uniques. Qu'est-ce que l'individu montre de lui sur le Web et quelles sont ses motivations ? Quels moyens techniques lui permettent de gérer ce qu'il publie et qui y a accès ? Quels sont les dérives et les risques, aussi bien pour celui qui diffuse des informations que pour celui qui collecte des données ? Si les faits et gestes de notre existence physique sont déjà repérables depuis longtemps (banque, carte à puce, vidéosurveillance, transport, télécommunication, etc.), ceux de notre existence numérique le sont tout autant et tracent autrement les frontières entre sphère privée et sphère publique du fait du caractère inhérent d'Internet : être un réseau public mondial décentralisé. Mais, comme le rappelle Louise Merzeau, maître de conférence à l'université Paris Ouest-Nanterre La Défense, on est passé de la problématique *« protection des données personnelles/ surveillance » à celle du lien entre « profil et identité / trace et information ».*

Organisés en avril 2009 par l'équipe Prodoper du CNRS (PROtection des DOnnées PERsonnelles), l'ISCC (Institut des sciences de la communication du CNRS), l'AFCDP (Association française des correspondants aux données personnelles), en partenariat avec l'université Paris Ouest-Nanterre La Défense, les états généraux de l'identité numérique furent l'occasion de croiser les approches et points de vue de juristes, d'économistes, d'informaticiens, d'e-commerçants et de représentants de la société civile autour du thème de l'identité numérique.

L'identité numérique concerne à la fois les informations personnelles que nous publions spontanément sur le Web, celles que les autres publient sur nous et les traces que nous laissons sur le réseau, volontairement ou involontairement. L'identité numérique ne peut donc pas être limitée à un identifiant. Frédéric Cavazza, blogueur et consultant, préfère quant à lui parler d'identité aux multiples facettes : identité administrative (civile) comprenant le nom, l'âge, l'adresse ; identité personnelle que seuls les amis connaîtront ; identité restreinte aux proches, à la famille ou à ceux avec qui l'on partage une passion ; identité professionnelle, intra-entreprise, etc. Pour schématiser, nos profils donnent des informations et notre comportement laisse des traces, ces dernières acquérant un caractère personnel par leur rattachement à un profil.

Non seulement les frontières entre toutes ces identités sont désormais de plus en plus poreuses, mais, en outre, les traces que nous laissons dans l'univers virtuel, sont quasiment toutes enregistrées.

Le sentiment pour l'individu d'utiliser des services disparates sur le Web lui fait oublier combien la notion d'espace et de temps diffère sur le réseau. D'une part, il est de plus en

plus aisé, pour tout un chacun, de recouper et d'agréger l'ensemble des traces et des informations personnelles laissées par un individu (comme par exemple sur le moteur de recherche de personne 123people.com). D'autre part, les informations enregistrées sur le Web sont quasiment ineffaçables.

En atteste cet article du magazine *Le Tigre*, qui publiait en janvier 2009 le portrait Google d'un parfait inconnu : « *Bon anniversaire, Marc. Le 5 décembre 2008, tu fêteras tes vingt-neuf ans. Tu permets qu'on se tutoie, Marc ? Tu ne me connais pas, c'est vrai. Mais moi, je te connais très bien. C'est sur toi qu'est tombée la (mal)chance d'être le premier portrait Google du Tigre. Une rubrique toute simple : on prend un anonyme et on raconte sa vie grâce à toutes les traces qu'il a laissées, volontairement ou non, sur Internet. Comment ça, un message se cache derrière l'idée de cette rubrique ? Évidemment : l'idée qu'on ne fait pas vraiment attention aux informations privées disponibles sur Internet, et que, une fois synthétisées, elles prennent soudain un relief inquiétant. Mais sache que j'ai plongé dans ta vie sans arrière-pensée : j'adore rencontrer des inconnus. Je préfère te prévenir : ce sera violemment impudique, à l'opposé de tout ce qu'on défend dans Le Tigre. Mais c'est pour la bonne cause ; et puis, après tout, c'est de ta faute : tu n'avais qu'à faire attention* ». S'ensuivait la vie détaillée de Marc L. avec bon nombre de détails intimes et personnels.

Si depuis toujours, l'identité est une notion qui renvoie en même temps « *à soi et à l'autre* », la numérisation de l'information et sa circulation sur les réseaux bouleversent en profondeur cette double dimension. Il ne s'agit plus de gérer son identité autour de soi, voire sa réputation ou son image, mais également la gérer aux yeux de tous sur un réseau mondial décentralisé. Les pratiques numériques liées aux blogs, aux réseaux sociaux et forums de discussion, aux publications de photos et de vidéos, aux partages de liens, aux votes et commentaires, redéfinissent la notion d'un « moi numérique » ; pour Nicolas Voisin, fondateur de la société 22mars spécialisée dans les médias sociaux et du site owni.fr, « *I am what I share : A "chercher à être ce que je partage", c'est-à-dire à partager ce que je souhaite que l'on pense de moi, ou que l'on associe à qui je suis, j'effectue, spontanément ou de manière consciente et réfléchie, un acte à haute valeur ajoutée. J'associe à un contenu ma réputation, mon identité numérique* ».

Plutôt que chercher à la dissimuler, maîtriser son identité numérique devient alors l'un des enjeux majeurs des utilisateurs du Web. De là provient le décalage entre le système de protection des données personnelles pensé dans les années 1970 et ce qui se passe aujourd'hui sur le Web. Il ne s'agit plus de protéger des données personnelles, mais d'accompagner l'individu dans la maîtrise de son identité numérique. Le groupe « identités actives 2.0 ? » de la FING (Fondation Internet nouvelle génération) ne s'y trompe pas en avançant que « *la protection de la vie privée, conçue comme un édifice juridique*

fonctionnant par défaut et pour tous, doit désormais se compléter de dispositifs de "maîtrise", plus complexes et mouvants, qui permettent aux individus – dans des limites à mieux définir – d'organiser à leur manière ce qu'ils veulent défendre, ce qu'ils veulent exposer et ce qu'ils sont prêts à négocier».

Si l'identité numérique est devenue une question clé de la société de l'information, c'est parce que les données personnelles si l'on en croit Louise Merzeau, sont le pivot d'une nouvelle économie des savoirs et des interactions, révélant au passage que l'identité et l'anonymat ne sont pas qu'une question numérique.

Pour la communauté informatique, « *on n'a pas toujours besoin d'avoir une identité* ». L'identité et l'authentification sont deux fonctions différentes. Si l'identité est la représentation d'une personne dans un système d'information, l'authentification sert à vérifier l'identité de cette personne. Et Yves Deswarte, directeur de recherche au CNRS au sein de l'unité de recherche LAAS (Laboratoire d'analyse et d'architecture des systèmes) nous a présenté un projet de carte d'identité blanche, une carte d'identité sans photo ni nom, dans laquelle seraient contenues les informations d'état civil et de preuve de droits. Cette carte fonctionne selon le principe du « oui/non », la réponse étant, par définition, contenue dans les questions, c'est-à-dire qu'il y aurait déjà au préalable une sélection de l'information pertinente contenue sur la carte. La carte ne répondrait qu'en fonction de la question posée, ce qui ne nécessiterait que l'utilisation minimale d'informations concernant l'individu. Pour Yves Deswarte, le concept de carte d'identité blanche vise avant tout à pointer du doigt « *les questions de sécurité individuelle et contrôle de la vie privée, en donnant la possibilité de pouvoir prouver ses droits sans avoir à dévoiler son identité.* »

Au demeurant, les visions juridiques et informatiques se rejoignent lorsqu'il s'agit de différencier l'identité de l'authentification. Pour Eric Brabry, directeur du pôle « droit du numérique » du cabinet Alain Bensoussan et membre du Conseil d'administration de l'AFCDP (l'Association française des correspondants aux données personnelles), ce n'est pas tant l'identité qui est en jeu mais la *désidentité*, c'est-à-dire le droit de ne pas être identifié. Il s'agit en effet de faire face à de nouveaux risques liés la circulation sur le Web des identités et des données rattachables à une personne : vol d'identité, usurpation d'identité, *phishing*… Le *phishing*, appelé en français l'hameçonnage, est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance… L'hameçonnage peut se faire par courrier électronique, par des sites Web falsifiés ou autres moyens électroniques.

En droit français, l'usurpation d'identité concerne le vol d'identité dont les agissements ont des incidences pénales. S'il n'y a pas d'incidences pénales, l'usurpation ne sera pas caractérisée. Depuis 2005, Tristan Mendès France, blogueur, propose de pénaliser l'usurpation de l'identité numérique.

Les risques liés à l'identité numérique sont essentiellement le fait d'utilisateurs peu avertis. Les travaux de Jean-Marc Manach, journaliste spécialisé, coorganisateur des Big Brother Awards consistent à informer les internautes sur les manières de contour- ner soi-même les systèmes de traçabilité et de sécuriser ses communications. Il s'agit principalement de « *technologies de protection de la vie privée* » (*PETs*, pour *privacy-enhancing technologies*) qui restent cependant peu utilisées par les individus. Pour Jean-Marc Manach, « *Le moins que l'on puisse dire est qu'il existe en effet "deux poids, deux mesures" : vous êtes un industriel/chercheur/"start-upeur" travaillant sur un domaine sensible ? L'Etat vous protège et vous explique comment vous protéger, sur le Net, au nom du contre-espionnage. Vous êtes un citoyen lambda ? L'Etat ne vous explique rien, mais fait au contraire tout pour s'autoriser le fait de vous espionner.* » A l'appui de sa démonstration, un texte émanant de la DST, l'ex- service de contre-espionnage français, qui révèle que « les attaques arrivent rarement par hasard : 95 % des vols d'ordinateurs sont ciblés ». L'espionnage est à 60 % économique, scientifique et industriel, et à 40 % politique, diplomatique ou de défense…

Les risques peuvent aussi provenir d'organismes publics : en mai 2009, un « pirate informatique » a dérobé les données médicales de 8 millions de patients de l'Etat américain de Virginie et menace de les divulguer si une rançon de 10 millions de dollars ne lui est pas versée. Des affaires de ce genre se multiplient un peu partout dans le monde.

Deux visions liées à l'architecture du réseau semblent se dessiner : celle d'éduquer et de sensibiliser le grand public aux risques, afin que chacun puisse maîtriser lui-même son identité numérique, ou celle de protéger le grand public « *malgré lui* », grâce à des dispositifs comme celui que propose Michel Arnaud, professeur à l'université Paris Ouest-Nanterre La Défense, avec une « banque centrale des identités » fonctionnant avec un tiers de confiance et le correspondant informatique et libertés. Le correspondant informatique et libertés est l'interlocuteur, dans l'entreprise, de la protection des données à caractère personnel au sens de la loi du 6 août 2004. Il tient la liste des traitements à l'intérieur de l'organisme privé ou public et il a également un rôle essentiel dans la diffusion de la culture « informatique et libertés » au sein de l'organisme l'ayant désigné ; il sera l'interlocuteur privilégié non seulement de la CNIL, mais également celui des personnes concernées par les traitements soumis à la loi du 6 janvier 1978 : conseil en amont, pédagogie, audit et médiation, rôle d'alerte du responsable de traitement sur les irrégularités constatées.

Cette architecture ne semble malheureusement pas prendre en compte la nature décentralisée du réseau. Sur un réseau décentralisé, sans tête, il s'agirait plutôt de sécuriser chaque extrémité plutôt qu'un organe central, cible parfaite de piratage informatique.

Cette approche, du reste, existe déjà comme l'atteste le passage de la tachygraphie analogique à la chronotachygraphie électronique dans le domaine des transports routiers en Europe, rendu obligatoire à la suite des règlements européens n°2135/98 du 9 octobre 1998 et du 20 avril 2006, dont les objectifs étaient à la fois d'améliorer la sécurité routière, d'harmoniser dans tous les pays les temps de conduite et de lutter contre la fraude des anciens systèmes. Les camions sont équipés d'une boîte noire et les chauffeurs sont munis d'une carte électronique professionnelle. Lors d'un contrôle, il s'agit de vérifier les autorisations du porteur de la carte électronique. Ce « *réseau social professionnel* » fonctionne techniquement sur un mode décentralisé où l'interrogation des autorisations se fait par requête auprès des autorités de délivrance. Comme le souligne Gilles Taïb, directeur général de Chrono- services, le système d'information devient un « *organisme vivant* » qui ne s'arrête jamais de vivre.

Tous s'accordent donc pour affirmer que l'ennemi public numéro un n'est pas tant le « *pirate informatique* », voire le « *corsaire* », que l'utilisateur lui-même. Pour l'instant, cet utilisateur ignore les enjeux liés à la protection de ses données personnelles et joue sous de multiples identités en acceptant la prise de risque. L'objectif n'est donc pas tant de protéger les personnes que de les équiper d'outils appropriés et de les responsabiliser.

La mise en adéquation d'un cadre juridique propice au développement des services du Web avec ces nouvelles pratiques sociales est d'autant plus urgente que la question de « l'identité numérique » ne concerne actuellement que les connexions à Internet à partir d'un ordinateur. Or, le développement croissant des terminaux mobiles connectés à Internet fait surgir de nouveaux défis comme celui de la géolocalisation qu'il conviendra de relever. Le défi juridique est donc double puisqu'il s'agit d'harmoniser mondialement des législations hétérogènes et de prendre en compte la circulation mondiale des données sur le réseau.

Relever ce défi passe par une mobilisation effective de tous les acteurs concernés et d'un véritable engagement politique nourri de réflexions telles que celles qui ont été évoquées par le Prodoper lors ces états généraux de l'identité numérique. Le livre blanc sur « l'identité numérique » qu'ils doivent publier avant la fin de l'année 2009 est attendu avec impatience.

Sources :

- « *Les états généraux de l'identité numérique* », conférence organisée par l'équipe Prodoper du CNRS (PROtection des DOnnées PERsonnelles), l'ISCC (Institut des sciences de la communication du CNRS), l'AFCDP (Association française des correspondants aux données personnelles), en partenariat avec l'université Paris Ouest Nanterre la Défense, le 27 avril 2009.
- « *Vol de données médicales : un pirate demande une rançon* », Christophe Auffray, zdnet.fr/actualites, 6 mai 2009.
- prodoper.fr
- bugbrother.blog.lemonde.fr/
- *Traçabilité et réseaux*, Revue Hermès, numéro 53, coordonné par Michel Arnaud et Louise Merzeau, CNRS Editions, avril 2009.

N°10-11 Printemps - été 2009