Présence numérique : les médiations de l'identité

Louise Merzeau

Présence numérique : les médiations de l'identité

Article inédit.

Louise Merzeau

Louise Merzeau est maître de conférences en sciences de l'information et de la communication à l'université Paris Ouest Nanterre La Défense et membre du CRIS. Ses travaux portent principalement sur les rapports entre mémoire et information, examinés sous l'angle médiologique des interactions entre technique et culture dans différents dispositifs (photo, TV, hypermédias, musée, Web…) . Récemment, ses recherches se sont focalisées sur la question de l'identité numérique et de la traçabilité sur les réseaux.

Plan

INTRODUCTION

L'essor des réseaux numériques donne lieu à des interprétations divergentes. Les unes soulignent l'emprise d'un individualisme croissant, désagrégeant les anciennes cohésions politiques. Les autres y voient le vecteur d'une sociabilité renouvelée. Les deux lectures se retrouvent cependant sur un point : dans le développement des systèmes de communication, la question de l'identité numérique représente désormais un enjeu central, sur les plans techniques, économiques et juridiques aussi bien que sociétaux.

Cette convergence témoigne de l'importance prise par les procédures de traçabilité dans l'ensemble des transactions – commerciales, administratives ou relationnelles. Après avoir été pensée comme une cible, qui venait *après* une information déjà constituée, la personne est devenue une ressource, un agent de pertinence et un opérateur de liens entre les informations.

Cette évolution coïncide avec l'émergence de nouveaux comportements, eux-mêmes portés par des dispositifs inédits, qui modifient les périmètres de l'identité. Décomposée en traces, exposée, indexée, recyclée, la présence numérique fait l'objet de traitements qui désagrègent la personne et mobilisent du même coup des aspirations à maîtriser son identité.

Après avoir été appréhendée sous le seul angle de la protection, la gestion des données personnelles se pose donc de plus en plus en termes de réappropriation. Par un mouvement de balancier qu'on a déjà pu observer dans d'autres médias, l'acculturation progressive aux dispositifs techniques déporte ainsi les questions vers des problématiques d'ordre politique. À l'instar du multimédia ou de l'informatique, à mesure que la communication en réseau se banalise, elle se problématise : derrière les problèmes d'équipement, d'apprentissage procédural et de standardisation industrielle, se dégage peu à peu la question des arbitrages et des choix de société. Avec cette différence qu'il faut désormais penser des systèmes techniques qui évoluent beaucoup plus vite que les usages.

DE LA PERSONNALISATION A LA PRESCRIPTION

De l'individu à la collection de traces

L'émergence d'un domaine de recherche dédié à l'identité numérique témoigne du recentrage de l'attention sur la « personne », telle qu'elle est questionnée et probablement modifiée par l'interconnexion généralisée. Initialement confinée dans des problématiques d'ingénierie, déterminées par les exigences de sécurisation des transactions, cette réflexion gagne aujourd'hui un champ plus large, avec des implications sociologiques, politiques et philosophiques.

Les études de communication sont concernées au premier chef par ce changement de perspective, car l'individu qu'elles ont construit ne correspond plus tout à fait à celui que visent aujourd'hui les stratégies et les innovations. Ce dernier n'est réductible ni au statut d'émetteur-récepteur, ni à celui de part d'audience, ni même à celui d'acteur – fût-il « réseau ». C'est une entité informationnelle, qui ne se laisse saisir qu'à travers les traces qu'elle dépose au gré de ses connexions.

Objet de toutes les attentions et de toutes les convoitises, cette entité est en passe de devenir la principale monnaie d'une économie numérique où chaque échange se paie en données personnelles. C'est que la personnalisation, mise en œuvre depuis les premières expérimentations visant à prendre en compte le besoin des utilisateurs dans les systèmes d'information, a radicalement transformé les logiques de communication. De l'industrie informatique et des bases de données, la problématique du profilage s'est déplacée vers le marketing, les bibliothèques électroniques et le *e-learning*, avant de gagner l'information journalistique, les plates-formes de partage et la communication mobile. D'abord centrée sur l'optimisation des langages de requête et des interactions homme-machine, la construction des profils est devenue le principal vecteur de rentabilité de l'ensemble des services en ligne.

Depuis le simple filtrage des données entrantes jusqu'à la recommandation, en passant par l'arrangement des interfaces et l'aide à la navigation, le ciblage s'échelonne sur différents degrés (Bouzeghoub, Kostadinov, 2007). Au-delà des spécificités propres à chaque domaine, la personnalisation a cependant connu partout une même évolution vers une « intelligence » de plus en plus intrusive. Dans le domaine des études de marché, les segmentations qui affectaient à chaque acteur une catégorie a priori (tranche d'âge, état civil, activité, revenu…) se sont avérées trop rigides pour traiter des flux de données de plus en plus complexes et volumineux. Mobile, actif, protéiforme, le consommateur devait pouvoir être suivi de plus près, jusque dans ses moindres singularités. Parallèlement, dans la recherche d'information, le principe de pertinence s'est détaché du processus d'ajustement progressif d'une réponse à une question pour devancer la formulation de tout besoin. Désormais indexée sur la personne, telle que sa présence numérique la définit en temps réel, la pertinence réorganise les contenus pour les prescrire en amont de toute requête.

Du type au token

L'adéquation entre l'offre et la demande est par conséquent devenue plus fine, mais aussi plus indiscrète. L'individu peut obtenir à tout instant une information *sur mesure*, à condition d'être constamment suivi à la trace. La raison communicationnelle change donc de paradigme : au lieu d'écarter les singularités pour dégager des traits communs – codes, routines, stéréotypes ou lignes de force –, elle valorise maintenant la captation de données personnalisées. Cherchant à calibrer au plus près des différentiels de consommation, d'action ou d'opinion, elle ne vise plus le *type*, stable et reproductible, mais le *token*, idiosyncrasique et contextuel, devenu plus-value de toute collecte d'informations (Merzeau, 2009).

Pour les entreprises qui les collectent, les données personnelles sont d'autant plus précieuses qu'elles ne représentent plus des probabilités, mais des attestations de présence. La logique de bases de données relationnelles qui s'est substituée aux stocks d'informations clientèle permet

d'établir des relations dynamiques entre la personne et ses comportements. Les techniques de *tracking* permettant d'obtenir des données beaucoup plus fiables que les larges panels, on peut ajuster les publicités au comportement individuel des prospects, et « vendre des consommateurs aux annonceurs » (Douplitzky, 2009). L'identité numérique acquiert donc elle-même une valeur marchande : elle s'achète et se vend sous forme de publicités comportementales et de commerce de fichiers.

De la cible au crible

Dans cette nouvelle gestion de la traçabilité, le modèle des moteurs de recherche prend le pas sur toute autre logique d'indexation. En tant que nœuds du réseau, ils opèrent l'interconnexion des traces que tous les prescripteurs rêvent d'effectuer sans en avoir toujours les droits ou les moyens. C'est cette capacité de recouper les données qui est aujourd'hui la plus rémunératrice, comme l'atteste la position dominante de Google, qui a constitué la plus tentaculaire des « bases d'intention » (Battelle, 2005). Sa politique consiste de fait à multiplier les services pour fusionner les gisements d'informations engrangés par chaque activité – chacune couvrant une modalité particulière de l'agir communicationnel : la recherche d'information avec Google, le chat avec Talk, l'autopublication avec Blogger, le partage d'images avec YouTube et Picasia, la gestion de communautés avec Groupes, l'orientation avec Google Earth, la correspondance avec Gmail, l'organisation avec Desktop. Cette « dérive des continents informationnels » (Ertzscheid, 2005), qui établit une interopérabilité entre contenus publics et privés, fait de l'identité numérique le seul dénominateur commun d'une masse de données hétérogènes, qu'aucune classification a priori ne peut plus ordonner.

Cette transversalité de la présence numérique est la principale ressource du Web 2.0. Pour l'utilisateur, l'attrait des blogs, des plates-formes de partage et des réseaux sociaux consiste dans la mise en commun de ses marqueurs individuels (centres d'intérêt, préférences, commentaires, statuts, etc.). Dernier stade de la prescription, l'exposition des données personnelles fait du profil un contenu, soumis à l'appréciation d'autrui. La personnalisation ne s'arrête plus à l'accès, elle affecte maintenant l'information. Du modèle de la *cible* (un même contenu pointé vers des usages différents), on est passé au modèle du *crible*, où ne sont retenues que les informations validées par un utilisateur. Dans cette logique, tout contenu publié devient lui-même prescriptif, sur le mode des préférences partagées. Goûts musicaux, articles de presse ou relations : s'informer revient de plus en plus à se voir proposer, par inférence statistique ou propagation réticulaire, ce que d'autres ont plébiscité. Inversement, de Facebook à Netvibes, en passant par Amazon et Deezer, tout ce que je déclare, indexe ou achète vaut recommandation – communautaire, scientifique ou commerciale.

DE LA DELIAISON A LA REAPPROPRIATION

Calcul de l'attention

Si les traces personnelles servent ainsi de plus-value et de lien entre les informations, c'est qu'elles font elles-mêmes l'objet d'une *redocumentarisation* (Salaün, 2007). Chaque évaluation, sélection ou adhésion est en effet susceptible d'être à son tour commentée et redistribuée, par l'effet de duplication et de portabilité des annotations.

À l'heure où la saturation informationnelle fait de l'attention le bien le plus précieux, cette mobilisation des marqueurs d'intérêt est un gage de profit. Les grandes bases (de données, de profils ou de produits) ne font rien d'autre que capitaliser cette diffraction de la présence numérique, dont chaque individu est un acteur. « Le document n'est plus simplement vecteur d'attention, c'est l'attention qui devient le vecteur d'une documentation permanente » (Ertzscheid, 2009). L'économie numérique poursuit donc le processus d'industrialisation de la culture, qui

visait à catégoriser les singularités pour *rendre calculable le désir* (Stiegler et *alii*, 2005). Les stratégies fondées sur la séduction et l'intention ayant montré leurs limites, on cherche à réduire encore le taux d'incertitude par le calcul de l'attention. Avec la capture toujours plus fine des préférences, les stratèges du traçage comptent sur nos empreintes pour prédire plus sûrement nos comportements.

Un tel objectif suppose que l'individu soit lui-même décomposé en autant de marques d'intérêt qu'il y a de sollicitations. Plus le Web se « socialise » et se délocalise par la téléphonie mobile, plus les données épousent la plasticité des situations, se dispersant et se recomposant *à la volée*. La messagerie instantanée, les SMS et plus encore les outils de micro-blogging comme Twitter renforcent en ce sens moins la visibilité de la personne que sa dissémination en unités d'information n'excédant pas 140 caractères. En attendant le Web dit « sémantique », qui devrait achever la dislocation des contenus en documents personnalisables et dynamiques, c'est la personne qui voit ses contours se désagréger. Assemblage temporaire d'indices, l'individu ne contrôle plus ni l'émission ni la destination de ses empreintes. Désormais, le volume de traces non intentionnelles qu'il laisse sur les réseaux dépasse en effet la part délibérée de son identité.

On ne peut pas ne pas laisser de traces

Cette « ombre digitale » (Williams, 2008) en croissance exponentielle interdit d'assimiler la présence numérique à une représentation de soi. Si le réseau affecte en profondeur l'identité, c'est parce qu'il produit des doubles *en dessous du sens*. La traçabilité informationnelle ne se réduit ni à l'expression, ni à la projection du sujet. Les traces s'enregistrent automatiquement, sans qu'on les ait toujours élaborées sous la forme d'une image ou d'un message. Opérant comme un sismographe de l'activité réticulaire, l'empreinte électronique radicalise l'équation posée par l'École de Palo Alto : désormais, non seulement on ne peut pas ne pas communiquer, mais *on ne peut pas ne pas laisser de traces*.

Le fonctionnement des réseaux sociaux comme Facebook est le meilleur exemple de cette présence paradoxale, entre exhibition et expropriation de l'identité. La personne y est divisée en trois niveaux : « identités déclarative, agissante et calculée » (Georges, 2009). Seule la première est faite d'un choix conscient de traits pertinents (photo, préférences sexuelles ou politiques, etc.). La seconde est le relevé, par le système, des activités de l'utilisateur au sein du réseau (par exemple : « X vient de rejoindre tel groupe »). La troisième comptabilise ses scores, ses « amis », ses visites, sa production, etc. Les trois couches identitaires sont liées entre elles, sans qu'aucune ne surplombe vraiment les autres. La part déclarative a l'initiative, mais elle est conditionnée par la qualification algorithmique de la présence. L'utilisateur apprend en effet à interpréter en termes d'influence ou de réputation le calcul de son identité, et il ajuste ses signaux pour coller au modèle de compatibilité que valorise le Web « social ».

Aux indices que l'individu essaime de lui-même, s'ajoutent ceux des tiers qui le citent, le montrent, le commentent ou se lient à lui (*posts*, photos, *tags*, liens, etc.). Il peut en suivre l'évolution, mais pas en prendre le contrôle. Or, dans la manière dont les données circulent et « remontent » sur la Toile (en particulier dans les moteurs de recherche), ces informations de seconde main ne sont guère différentiables des siennes.

Cette superposition de traces comportementales avec des informations déclaratives et des données nominatives fait de la personne numérique un composite inédit. Rompant avec les conceptions de l'identité qui séparent nettement public et privé, la communication réticulaire combine les couches identitaires, étalonnant les attributs individuels au *ratio* des systèmes d'échange et de visibilité.

Granularité de la personne

Ce *ratio* impose une granularité qui permette une indexation des données personnelles partout où elles affleurent. La personne ainsi profilée n'est plus celle du curriculum vitae, de l'appartenance

ou des papiers d'identité. C'est celle des listes d'occurrences antéchronologiques ou des nuages de *tags* que recomposent à la demande des outils comme 123people. « Unités isolables, agençables et calculables », « si élémentaires qu'on les croit vierges de toute signification » (Roger T. Pédauque, 2006, pp. 186 et 14), les traces numériques ne sont plus cadrées par une métacommunication, mais par des métadonnées. Détachées des énoncés, elles ne sont que des déictiques qui pointent vers des trajectoires et des fragments.

Parce qu'elles sont « informes », ces informations sont « exploitables grâce aux moteurs de recherche, aux systèmes de *datamining* ou d'analyse sémantique, aux logiciels de reconnaissance des formes, aux graphes de réseaux sociaux, etc. » (Kaplan et *alii*, 2009). La *déliaison* des traces est ce qui permet de redistribuer la personne dans les interactions, même quand elle n'a pas fourni de données nominatives. Plutôt que de stigmatiser le caractère autocentré de la présence numérique, c'est cette délégation de l'intelligibilité des données personnelles à des agents extérieurs qu'il faut souligner. « Objets politiques et non sémantiques » (Melot, 2006, p. 14), les traces sont muettes si on les prend isolément ou du seul point de vue de celui qui les répand. Mais pour ceux qui les prélèvent et les traitent, elles mettent en jeu des intérêts et des pouvoirs.

De l'autodéfense à la gestion

Face à cette externalisation de l'identité, un nombre croissant d'initiatives manifestent le besoin d'une réappropriation. En premier lieu, des apprentissages individuels se mettent en place, en marge des opérateurs et des pouvoirs publics, pour *brouiller* l'identité : pratique de l'anonymat, usage de pseudonymes, rétention d'informations, multiplication des adresses mail, déclarations mensongères (Bell, 2008), ou essaimage de traces impertinentes pour rendre inopérants les recoupements. Pour la plupart cependant, ces « réticences » relèvent à peine de la tactique. Elles ne sont guère planifiées et coexistent souvent avec des comportements opposés de transparence ou d'exhibition. L'exercice d'une veille de la présence est une autre forme de réappropriation. Même si elle n'est motivée que par une simple curiosité narcissique, l'interrogation des moteurs de recherche sur les éléments qui composent notre identité permet d'en percevoir – et dans une certaine mesure d'en corriger – la diffraction. Par le surplomb qu'elle constitue, la page de résultats renvoie une description « objective » de la présence numérique, telle qu'elle est indexée par les algorithmes de pertinence (PageRank). Ce calcul de l'identité, l'individu peut lui-même l'infléchir, en publiant sur le réseau de nouvelles traces qui alimenteront à leur tour les moteurs d'indexation.

L'étape suivante consiste à gérer sa visibilité par une démarche active. Réservé aux familiers des réseaux, ce niveau mêle étroitement tactiques des utilisateurs et stratégies des systèmes de profilage. Les entreprises ont compris qu'elles avaient tout à gagner à laisser l'individu « devenir sa propre régie publicitaire » (Douplitzky, 2009, p. 117), du moment qu'il accepte de monnayer l'information par ses données. Ainsi, dans les réseaux sociaux, la présence revient ainsi à moduler son degré d'exposition autant qu'à nouer des contacts. Jouant des paramétrages et tableaux de bord, l'utilisateur est invité à choisir le « design de sa visibilité » (Cardon, 2008). En même temps qu'il calcule des probabilités de relations, il modèle son identité par des systèmes de filtres, d'étiquetage et de paravents.

Ce *design* est rendu possible par le fait que « chaque plateforme propose une politique de la visibilité spécifique et [que] cette diversité permet aux utilisateurs de jouer leur identité sur des registres différents » (Cardon, 2008, p. 124). Dans Facebook, LinkedIn, Peuplade ou MySpace, les profils ne découpent pas les mêmes pertinences et les mêmes affinités. Si tous les dispositifs entérinent la primauté de la relation sur le contenu, chacun formate différemment l'image par laquelle l'internaute cherche à se situer dans un réseau. Plus qu'à multiplier les masques, la dissémination des traces peut servir à *distribuer* l'identité selon différentes logiques. Certaines invitent l'utilisateur à se travestir pour établir des connexions (fabrication d'avatars dans les mondes virtuels) ; certaines l'incitent à s'exhiber pour gagner en notoriété (éparpillement de *twitts*

dans les systèmes de micro-blogging) ; d'autres enfin l'encouragent à déployer autour de lui des zones intermédiaires, mi publiques, mi confidentielles.

On débouche ainsi sur un modèle productif, où l'individu est encouragé à essaimer, entretenir et faire fructifier ses marques. Savoir *cultiver son identité numérique* relève dès lors d'une compétence, valorisée par le marché de l'attention et de la réputation. « Qualifier et quantifier ses ressources », « classer et gérer ses contacts réseau », « entretenir un capital relationnel », « construire des outils de valorisation » (Ogez, 2009) : l'utilisateur est sommé de se convertir en plan de communication, pour épouser les mécanismes du réseau tout en reprenant la main sur sa traçabilité. Il s'agit moins d'échapper à la surveillance, que d'organiser sa présence, comme en témoigne la demande de portabilité des profils. Le principe du e-Portfolio résume cette nouvelle aspiration : ne plus laisser ses indices s'éparpiller, mais documenter soi-même son dossier personnel et gérer des portefeuilles d'identités.

DE LA PROTECTION A LA MEDIATION

Des internautes laissés à eux-mêmes

La diffraction de la présence numérique déplace la maîtrise vers la fonction d'agrégation des traces. La concentration des graphes, des index et des clés d'accès se trouve propulsée au premier plan des enjeux politiques de l'identité numérique. Actuellement, l'utilisateur a encore peu de moyens d'assurer lui-même cette capitalisation de ses données. Il est contraint de s'en remettre aux principaux acteurs de l'économie numérique, qui régulent de fait les réseaux. Comme on l'a rappelé, les stratégies individuelles de réappropriation sont elles-mêmes « incluses » dans celles des systèmes de traçage, portant la même adhésion aux « logiques absolues de sécurité, d'efficacité, de confort et d'interaction » (Rouvroy, 2009, p. 7), devenues indiscutées. N'ayant d'autres ressources que de bricoler, tricher ou négocier avec les dispositifs qui se paient sur leurs données personnelles, les utilisateurs n'ont qu'une faible marge de manœuvre. De leur côté, les développeurs n'ont aucune raison de se contraindre à réduire ou corriger leurs stratégies de captation. Laissée à l'initiative privée, la standardisation des outils s'opère donc hors des préoccupations relatives aux libertés fondamentales et au bien commun.

Appelant au « *self-control* de sujets contractants considérés comme autonomes, conscients, informés et perçus par le seul prisme du citoyen-consommateur » (Forest, 2009), l'incitation à autogérer sa e-réputation dispense les pouvoirs publics de réfléchir à une écologie des réseaux. En France, on ne peut qu'être frappé par l'inaptitude de la classe politique à prendre en charge le dossier de l'identité numérique, autrement que par une pénalisation des pratiques individuelles non conformes. Le législateur semble avoir « renié sa mission de protecteur des individus », préférant « défendre l'ordre public avant que d'assurer la défense de nos libertés individuelles et collectives, et donc nos vies privées » (Guillaud, 2009). C'est en tout cas ce dont témoigne l'évolution récente du cadre juridique, depuis la « Loi sur la Société de l'Information » jusqu'à la « Loi Création et Internet » : d'obligations en interdictions, la puissance publique n'envisage plus l'internaute que sous deux aspects : consommateur ou délinquant.

Le double jeu sécuritaire

Dans cette dérive, l'argument de sécurité joue un double jeu déterminant. D'un côté, l'Internet est systématiquement décrit comme une extériorité dangereuse dont le citoyen doit se protéger (voir la campagne lancée par le secrétariat d'État à la Famille en novembre 2008). De l'autre, l'État cherche à tirer lui-même profit de la traçabilité et utilise les mêmes techniques de surveillance que les entreprises, sous prétexte de prévenir les risques de délinquance et de terrorisme. Cette conception sécuritaire, qui combine une hyperréglementation policière avec une dérégulation du marché,

refuse de penser la présence numérique en termes d'*environnement* et de *pouvoir de synchronisation* (Stiegler, 2009). On fait comme s'il suffisait de rationaliser la circulation des informations. La manière dont le trafic des données affecte contenus et identités n'est jamais prise en considération. La question du droit n'est donc envisagée que sous l'angle de l'adaptation des règles anciennes à de nouveaux objets. Elle n'est que très rarement formulée dans le sens d'une refondation des droits du citoyen. C'est pourtant dans cette direction qu'il faut travailler, si l'on veut concilier le développement de l'économie numérique avec l'affirmation des liberté fondamentales.

L'inertie politique ambiante sur la question de l'identité numérique commence cependant à se lézarder. En témoigne le rapport d'information remis au Sénat le 3 juin 2009 (Détraigne, Escoffier, 2009), où sont préconisées des mesures visant à « faire du citoyen un "homo numericus" libre et éclairé, protecteur de ses propres données ». Pour l'heure, le climat demeure toutefois celui d'une société de méfiance, où l'on fait régner un sentiment d'insécurité tout en laissant les intérêts marchands organiser la circulation des données. Les logiques de traçage économique et policière partagent de fait la même ambition de calculer les comportements pour les rendre plus prévisibles. Dans les deux cas, c'est le principe même d'incertitude qu'on voudrait évacuer, en déduisant des traces une modélisation des goûts, des pratiques et des opinions.

Cette primauté de la logique sécuritaire se retrouve jusque dans les dispositions légales censées protéger les utilisateurs. Centrée sur la notion de vie privée, les réglementations actuelles postulent un individu clairement séparé de ses usages réticulaires et capable de s'en passer. Du coup, elles sont de plus en plus inapplicables, ou rejetées par ceux-là mêmes qu'elles prétendent défendre, mais qui ne sont plus disposés à ne pas communiquer. Il est donc temps de repenser l'articulation de « l'informatique et des libertés », que ne saurait décrire une loi conçue avant l'Internet.

Confiance et incertitude

Pour garantir un exercice éclairé de la présence numérique, la sécurité ne suffit pas : c'est de confiance que l'environnement numérique a besoin. Qu'il s'agisse de réseaux sociaux, de commerce électronique, d'intelligence collective ou de participation « citoyenne », la démocratie ne peut exclure le risque. Elle est elle-même un pari sur l'incertitude, rendu possible par la confiance des membres dans la vitalité du collectif qui les rassemble.

Contrairement à la sécurité, la confiance ne se décrète pas. L'information des citoyens, non seulement sur leurs droits, mais aussi sur le potentiel de créativité qui en procède, est donc la première des exigences. La mise en place de relais aidant les individus à développer une activité numérique ne devrait plus être considérée comme une option, mais comme une nécessité. La création de labels, préconisée par la Cnil et par le rapport Détraigne-Escoffier, fait partie de ces balisages qui devraient donner au citoyen les moyens de choisir en connaissance de cause parmi les produits, les protocoles et les outils. Sans attendre l'engagement de l'État, des organismes de la société civile comme la Fevad (Fédération du e-commerce et de la vente à distance) ou la FNTC (Fédération nationale des tiers de confiance) ont pris les devants, en mettant en place des systèmes de labels dans leur propre domaine.

Plus généralement, c'est le besoin de médiation et de pédagogie qui se manifeste avec une insistance croissante, dans tous les secteurs affectés par la révolution numérique. Les *États généraux de l'identité numériques* qui se sont tenus à Paris en avril 2009, l'ont confirmé : face aux insuffisances des lois, la confiance ne peut s'établir que sur la modélisation, non des usages, mais des procédures de traçabilité (ouverture de compte, signature électronique, télépaiement, horodatage, archivage, etc.). L'élaboration de chartes des « bonnes pratiques » constitue en ce sens une avancée importante vers une appropriation collective et raisonnée des logiques de traçabilité.

Vers une régulation politique de la présence numérique

Car l'enjeu est de passer des ajustements individuels et asymétriques à une régulation politique de la présence numérique. Qu'ils émanent de l'État ou de la société civile, des dispositifs collectifs doivent prendre le relai des tactiques d'usage bricolées par les pionniers. Maintenant que le recours aux TIC n'est plus réservé à quelques uns, la maîtrise des données doit remplacer la protection. D'une part pour permettre aux individus « d'organiser à leur manière ce qu'ils veulent défendre, ce qu'ils veulent exposer et ce qu'ils sont prêts à négocier » (Kaplan et *alii*, 2009) ; d'autre part, pour exercer sur les acteurs une pression économique et citoyenne.

Techniquement efficiente, l'autorégulation du réseau ne doit pas dispenser de réaffirmer la préséance de certains droits sur les logiques industrielles. Il faut aussi combler les vides juridiques qui témoignent des impensés de la citoyenneté numérique. Enfin la normalisation des réseaux doit devenir un enjeu démocratique, au lieu d'être confisquée par les seuls impératifs de rentabilité et d'interopérabilité.

Les droits d'information, d'opposition, d'accès et de rectification des données personnelles sont inscrits dans la loi. On sait cependant qu'ils sont difficiles à appliquer. Pour faire respecter les principes édictés, il faut informer plus systématiquement les citoyens sur l'usage qui est fait de leur traces, simplifier les procédures de vérification, d'effacement, de rectification et de recours et donner plus de moyens aux commissions de contrôle. Entre 2004 et 2008, la CNIL a vu ses crédits augmenter de 65 % et ses effectifs de 50 % quand ses délibérations ont progressé de 458 %. La comparaison au plan international montre que tous les États n'ont pas établi les mêmes *ratios*, et que la priorité accordée à la protection des données relève bien d'une volonté politique.

Statut et droits du double numérique

Au delà des efforts à consentir pour appliquer les lois, le temps est surtout venu de recentrer la question de la présence numérique dans l'appareillage démocratique. Certaines des exigences formulées par le Pacte pour les Libertés Numériques peuvent en ce sens être reprises au nom d'une réhabilitation de l'exercice de la citoyenneté sur les réseaux : « préserver le principe de neutralité de l'internet dans le cadre de régulation européen en matière de télécommunications », « s'assurer du respect par les opérateurs de télécommunication du principe d'égalité devant les réseaux, selon lequel aucune donnée ne devrait être traitée de façon discriminatoire, quel que soit son contenu, son destinataire ou son expéditeur », etc. Aussi essentielles soient-elles, ces recommandations ne remplaceront cependant pas un questionnement sur le statut du double numérique et les nouveaux droits qu'il devrait conduire à formuler. En premier lieu, ce sont les contours mêmes de l'identité numérique qui demandent à être précisés. Clarifier le statut de l'adresse IP, en reconnaissant qu'elle est une donnée à caractère personnel, s'avère par exemple nécessaire. La question de la nature juridique de l'avatar est également à poser. En cas d'infraction commise depuis un monde virtuel (incitation à la haine, diffamation…), la responsabilité est actuellement indécidable. Faut-il étendre au double numérique les droits de la personne, ou lui assigner un statut spécifique ? Les cas de plus en plus nombreux d'usurpation démontrent eux aussi l'urgence à légiférer sur l'identité numérique, pour substituer aux solutions techniques, souvent liberticides, des réponses en droit.

Plus radicalement, reconnaître, comme le préconise la Fing, un droit à l'« hétéronymat » pourrait constituer une base pour réguler les pratiques des utilisateurs comme des détenteurs de données. Il permettrait à chaque personne de s'adjoindre des identités alternatives, qu'elle pourrait déposer auprès d'un organisme chargé de les valider et d'en protéger l'accès (celui-ci étant réservé au propriétaire et, dans certains cas particuliers, aux autorités). Donnant une forme de reconnaissance légale à des tactiques déjà partiellement mises en œuvre, ce droit garantirait à la fois l'anonymat et la présence, en établissant que personnalisation et identification doivent être dissociées (Arnaud, 2007). Pour quantité d'usages où l'individu est en droit d'attendre un traitement personnalisé, il n'y

a en effet aucune raison d'exiger qu'il délivre en retour des informations nominatives : attester le statut ou l'attribut qui le destine à tel ou tel service devrait suffire.

Le droit à l'hétéronymat contribuerait surtout à restaurer la confiance indispensable à l'exercice démocratique, en réhabilitant la place d'une médiation publique, étatique ou civile. La fonction du tiers de confiance a d'ores et déjà commencé à faire l'objet de débats et de négociations. Le label est naturellement prisé par les grandes entreprises, qui ont intérêt à renforcer leur mainmise objective sur les données par une reconnaissance officielle. Il est donc urgent de mener cette réflexion, non pas pour dénier *a priori* toute légitimité aux acteurs privés, mais pour rappeler qu'il s'agit bien d'enjeux politiques. Les arbitrages à rééquilibrer entre lois, standards, logiques d'usage et règles professionnelles sont des arbitrages entre pouvoirs : ils ne peuvent se résumer à des ajustements techniques. Pour la même raison, il convient d'impliquer davantage la société civile dans les procédures de normalisation. Le réseau lui-même pouvant être décrit comme « un ensemble de normes » (Brousseau, Curien, 2001, p. 10), c'est par la normalisation plus que par la législation que la traçabilité pourra véritablement être régulée. C'est au niveau des standards, des protocoles et des formats qu'on pourra corriger le déséquilibre entre normes de marché et normes de droit. Et c'est en faisant évoluer les normes de la « personne-fichier à la personne-graphe-hypertexte » (Fabre, 2009, p. 178) qu'on pourra prendre en compte les nouvelles granularités de l'identité.

Conclusion

La personnalisation progressive de l'environnement numérique fait de l'identité le nouvel étalon de mesure de la culture et du lien social. Après avoir été diluée dans l'idéologie communicationnelle des mass media, puis réduite à une attente extérieure au processus d'information, la personne fait désormais partie intégrante des flux de données. Plus qu'une facette qui s'ajouterait aux attributs antérieurs du sujet, la présence numérique tend donc à redéfinir la valeur, la pertinence et le droit.

S'il s'est d'abord appuyé sur l'affaissement des médiations, ce mouvement de personnalisation ne s'arrête pas à une tendance à l'individualisme. Tout porte à croire au contraire que la présence numérique appelle aujourd'hui une refondation des principes de l'être-ensemble, autour de nouvelles logiques d'échange, de partage et d'exposition. Cette prise de conscience des enjeux sociétaux de l'identité numérique pourrait même nourrir un retour vers le politique. En effet, si elle fonctionne sur le modèle marchand d'une transaction, la présence numérique ne s'épuise pas dans le calcul d'une satisfaction : elle pose la question de l'espace commun et des moyens de le réguler.

Reste à régler le problème du droit à l'oubli. Là encore, l'identité opère comme un révélateur : tant que les individus n'avaient pas compris qu'il est indispensable de pouvoir retirer du réseau des informations les concernant, ils n'avaient pas réalisé que l'environnement numérique est une mémoire « par défaut ». Aujourd'hui, ils commencent à mesurer ce que pourraient perdre une culture et une société incapables d'oublier.

Références bibliographiques

Arnaud, Michel (2007), « Un Habeas corpus numérique », *Médium* n°13, automne 2007, p.127-137.

Battelle John (2005), T*he Search : How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture*, New York : Portfolio Hardcover, traduit de l'américain sous le titre *La révolution Google*, Paris : Eyrolles, 2006.

Bell, Genevieve (2008), « Secrets, lies & the possible *perils of truthful technology* », conférence prononcée dans le cadre du programme Lift de la Fing, [en ligne] http://www.liftconference.com/secrets-lies-possible-perils-truthful-technology , page consultée le 19 juin 2009.

Bouzeghoub, Mokrane ; Kostadinov, Dimitre (2007), « *Data Personalization : a Taxonomy of User Profiles Knowledge and a Profile Management Tool* », Rapports de recherche du laboratoire PRiSM, [en ligne] http://www.prism.uvsq.fr/rapports/bin/bibliography.php?id=25&lang=, page consultée le 12 juin 2009.

Brousseau, Éric ; Curien, Nicolas (2001), « Économie d'Internet, économie du numérique », *Revue économique*, vol. 52, numéro hors série.

Cardon, Dominique (2008), « Le design de la visibilité : un essai de cartographie du web 2.0 », *Réseaux*, n° 152, Paris, Lavoisier, p. 93-137.

Détraigne, Yves ; Escoffier, Anne-Marie (2009), « La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information », Rapport d'information au Sénat n° 441 déposé le 27 mai 2009, [en ligne] http://www.senat.fr/rap/r08-441/r08-441.html , page consultée le 20 juin 2009.

Douplitzky, Karine (2009), « Le commerce du moi, modèle économique du profilage », *Hermès*, n°59, Traçabilité et réseaux, p. 113-118.

Ertzscheid, Olivier (2005), « De la dérive des continents à la confusion des pratiques », *affordance.info*, [en ligne] http://affordance.typepad.com/mon_weblog/2005/10/jai_vcu_sans_go.html, page consultée le 12 juin 2009.

Fabre, Renaud (2009), « La personne : une régulation par les normes ? », *Hermès*, n°53, p.175-181.

Forest, David (2009), *Abécédaire de la société de surveillance*, Paris : éditions Syllepse.

Georges, Fanny (2009), « Représentation de soi et identité numérique. Une approche sémiotique et quantitative de l'emprise culturelle du web 2.0 », *Réseaux*, 2009/2, N°154, p. 165-193.

Guillaud, Hubert (2009), « Vie privée : Où sont les régulateurs ? Où sont les régulations ? », *InternetActu*, [en ligne] http://www.internetactu.net/2009/04/06/vie-privee-ou-sont-les-regulateurs-ou-sont-les-regulations/ , page consulutée le 20 juin 2009.

Kaplan, Daniel et *alii*, (2009), « Le nouveau paysage des données personnelles : quelles conséquences sur les droits des individus ? ». Document de travail produit par le groupe « Informatique & Libertés 2.0 ? » dans le cadre du programme *Identités actives* de la Fing, [en ligne] http://www.internetactu.net/2009/04/03/le-nouveau-paysage-des-donnees-personnelles-quelles-consequences-sur-les-droits-des-individus, page consultée le 17 juin 2009.

Merzeau, Louise (2009), « Du signe à la trace : l'information sur mesure », *Hermès*, n°59, Traçabilité et réseaux, p. 23-29.

Ogez, Émilie (2009) (dir.), *Cultivez votre identité numérique*, [en ligne] http://issuu.com/geemik/docs/cultivez_votre_identite_numerique , page consultée le 19 juin 2009.

Roger T. Pédauque (2006), *Le Document à la lumière du numérique*, Caen : C&F éditions.

Rouvroy, Antoinette (2009), « Réinventer l'art d'oublier et de se faire oublier dans la société de l'information ? », in Lacour, Stéphanie (dir.), *La Sécurité de l'individu numérisé. Réflexions prospectives et internationales*, Paris : L'Harmattan.

Stiegler, Bernard et *alii* (2005), Manifeste d'Ars Industrialis, [en ligne] http://www.arsindustrialis.org/le-manifeste, page consultée le 17 juin 2009.

Stiegler, Bernard, « Sur la culture informationnelle », entretien mené par Ivana Ballarini-Santonocito et Alexandre Serres, *Médiadoc*, n°2, avril 2009, Éducation aux médias et culture de l'information, [en ligne] http://www.fadben.asso.fr/spip.php?article78

Williams, Ian « *Digital universe continues to expand* », vnunet.com, [en ligne] http://www.vnunet.com/vnunet/news/2211903/digital-universe-continues-explode, page consultée le 17 juin 2009.