De la surveillance à la veille

LOUISE MERZEAU

Le réseau n'est pas un support médiatique de plus, mais un environnement voué à contenir et transformer l'ensemble des médiations. La matière première de cet environnement est constituée par les traces que nous déposons, consciemment ou non, au gré de nos communications. Nouvelle monnaie d'une économie de l'attention, ces traces induisent des formes de contrôle inédites et paradoxales, en ce qu'elles relèvent à la fois de logiques de surveillance et d'autodétermination. Plus notre présence numérique se renforce et se ramifie, plus nous livrons un nombre croissant d'informations sur nous-mêmes, tout en redoutant d'être épiés ou suivis à la trace. C'est le *privacy paradox,* qui rend caduque toute régulation fondée sur le seul principe de la protection. Pour normaliser les trafics d'identifiants, il faut prendre acte du fait que les individus ne peuvent plus guère (ou ne veulent plus) renoncer à s'exposer et à étendre leurs relations. Si les asymétries n'ont pas disparu, la traçabilité réticulaire repose de moins en moins sur des appareils de surveillance en surplomb, et de plus en plus sur des systèmes de veilles horizontales.

1. ON NE PEUT PAS NE PAS LAISSER DE TRACES

Une mémoire par défaut

Le passage d'une informatique lourde et centralisée à des dispositifs répartis, interconnectés et mobiles favorise l'avènement d'un double numérique, à la fois distinct et étroitement lié au sujet. Le développement

Cités 39, Paris, PUF, 2009

des capacités de stockage et de miniaturisation pousse à attacher à chaque instruction, aussi insignifiante soit-elle, l'archive de sa propre effectuation. Ce changement d'échelle, en nombre de données et de sources, n'a pas que des effets quantitatifs. La croissance exponentielle des enregistrements tend à inverser le rapport séculaire des stocks à la mémorisation. Alors que l'oubli prévalait jusqu'à maintenant comme le fond contre lequel résistaient des mnémotechnies, c'est désormais « par défaut [que] toute information (sonore, visuelle, textuelle) est enregistrée et conservée sous une forme digitale – l'oubli, nécessitant une action positive d'effacement des données, devenant de ce fait l'exception plutôt que la règle »[1]. Les interfaces sont elles-mêmes des machines à mémoriser, car la demande croissante de fluidité exige paradoxalement (comme dans les terminaux utilisant la technologie *touch*) que chaque état conserve une trace de l'état précédent. Surtout, la collecte fonctionnant désormais sur le mode de la capture, il est moins coûteux de conserver l'information que de l'effacer. La trace n'est donc plus une inscription seconde, séparée du contexte d'émission, mais une dimension de l'acte communicationnel qu'elle consigne, une sorte de mémoire en temps réel qui brouille les frontières entre stock et flux.

Quand on sait que l'information enregistrée sur le réseau double toutes les soixante-seize heures, la question du déstockage des données n'est plus un problème technique, mais une exigence éthique. La quantité même des fichiers représente une mutation qualitative, dans la mesure où de telles masses de données ne peuvent plus être traitées que par l'entremise d'algorithmes et de robots, c'est-à-dire d'une *intelligence déléguée*. Cela suppose la mise en œuvre de nouveaux principes de modélisation, d'indexation et de combinaison des traces. Cette automatisation est l'un des aspects majeurs du renouvellement des logiques de surveillance. Elle a pour corollaire l'augmentation de la part non intentionnelle des marquages, qu'ils soient directement effectués par des machines ou qu'ils résultent des jeux de cascades et de duplication réticulaires. Excédant désormais les inscriptions que nous déposons volontairement, cette « ombre numérique »[2] ne relève plus d'une sémiologie, mais d'une *ichnologie*[3] d'un genre inédit.

1. Antoinette Rouvroy, « Réinventer l'art d'oublier et de se faire oublier dans la société de l'information ? », *in* Stéphanie Lacour (dir.), *La sécurité de l'individu numérisé. Réflexions prospectives et internationales,* Paris, L'Harmattan, 2009, p. 2.

2. John Gantz, compte rendu de l'étude menée par le cabinet d'analyse IDC, *The Diverse and Exploding Digital Universe* <http://www.emc.com/digital_universe>.

3. Note explicative ?

Des messages aux empreintes

Adressage des pages, identification des ordinateurs (IP), historiques de navigation, préférences, listings, *login*... : avant d'être un arrangement signifiant, l'instruction informatique est un tatouage, « une trace, construite ou retrouvée, d'une communication en même temps qu'un élément de systèmes identitaires »[1]. Nous ne sommes ni l'émetteur, ni le destinateur de cette multitude d'empreintes qui encryptent notre présence. Consulter, consommer, évaluer, jouer, voyager... la moindre de nos activités dépose des empreintes qui signalent notre comportement, sans que nous l'ayons nous-mêmes traduit en un message.

Les enjeux de cette traçabilité ne peuvent être évalués à l'aide des grilles forgées par une pensée du signe, du message et du document. Là où ceux-ci supposent un acte d'énonciation doté de sens et (en partie au moins) d'intentionnalité, la signature électronique procède d'un calcul, d'un codage et d'une connexion souvent imperceptibles. La trace numérique n'articule pas une face sensible (signifiant) à une représentation psychique (signifié), mais une marque invisible à un acte informationnel rarement perçu comme tel. Dans ce contexte, il n'y a pas de *comportement zéro* : l'information est par défaut, et toute information contient une part potentielle de données sensibles. L'environnement numérique radicalise ainsi l'équivalence entre conduite et communication, que l'École de Palo Alto avait mise en évidence pour critiquer la conception linéaire du modèle télégraphique de la transmission. Désormais, non seulement on ne peut pas ne pas communiquer, mais plus radicalement, *on ne peut pas ne pas laisser de traces*.

Le traçage est d'autant plus pervasif que la structure technique et relationnelle du réseau démultiplie les inscriptions. Aux innombrables indices que chaque individu dépose de lui-même s'ajoutent ceux que des tiers produisent sur lui, en parlant de lui, en montrant sa photo, en le citant, en *tagant* ou en commentant ses prestations, en se liant à lui ou à ses contenus, etc. Le traitement numérique du signal permettant d'exploiter des granularités d'information très en deçà du message, les données à caractère personnel ne sont plus circonscrites aux procédures d'identification explicites. « Productions et expressions diverses d'un individu,

1. Roger T. Pédauque, *Le document à la lumière du numérique,* Caen, C&F Éditions, 2006, p. 32.

messages, contacts, relations et liens, jugements de ou à propos de la personne, commentaires, images, rumeurs, traces de passage ou d'usage [...]. Ces informations sont souvent informes, incluses de fait et sans indication particulière dans un texte ou une image. Mais elles deviennent de plus en plus aisément 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. »[1] C'est cette possibilité de traiter la personne au niveau de ses composantes les plus fines qui aggrave et modifie la portée des procédures de surveillance.

2. PROFILAGES ET FILATURES

Prescriptions sur mesure

Là où la culture de masse fabriquait des dénominateurs communs, la culture numérique tend par essence à personnaliser l'information. En substituant au modèle irradiant des émetteurs celui, commutatif, des serveurs[2], la communication en réseau ne déplace pas seulement le centre vers les périphéries. Elle fait dépendre tout acte de connaissance d'un calcul de pertinence qui court-circuite les cheminements de l'information. Plus les commutations s'affinent, plus les nœuds mis en relation deviennent eux-mêmes des variables ponctuelles et éphémères. Reconstruite à chaque session, la pertinence n'est plus déterminée par une appartenance ou un statut, mais par un état passager, propre à chaque individu, situation ou registre de communication.

Les segmentations qui affectaient d'en haut une catégorie à chaque acteur (âge, revenu, état civil, profession...) cèdent alors le pas à des prescriptions sur mesure. L'individu y perd en anonymat ce qu'il gagne en indépendance : il ne s'affranchit des types où l'assignait la société de

1. « 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 <http://www.internetactu.net/2009/04/03/le-nouveau-paysage-des-donnees-personnelles-quelles-consequences-sur-les-droits-des-individus/>.

2. Voir Marc Guillaume, « La révolution commutative », *Les Cahiers de médiologie,* nº 6, 1998, « Pourquoi des médiologues ? ».

consommation qu'en acceptant d'être suivi à la trace, jusque dans ses moindres déplacements, mixités et changements, par ce qu'il faut désormais appeler la société des bases de données. Inconstance, différence, mobilité... le sujet peut revendiquer sa singularité, pourvu que son double numérique laisse une signature identifiable.

La sémiotisation des comportements ne peut saisir tous les enjeux de cette traçabilité. Pour la sémiologie et la sociologie, l'analyse des phénomènes suppose que les singularités soient écartées, au profit d'une mise en visibilité des constantes, routines, lignes de force et affluences. Comme dans les études des mouvements de foule pour la gestion des situations de crise, le social n'est lisible qu'en élaguant les particularismes pour mettre en évidence des invariants : mythologies, codes, stéréotypes, grammaires. La présence numérique, elle, dépend au contraire de la possibilité de calibrer au plus près des différentiels de consommation, d'action ou d'opinion.

Dans son travail sur la normalisation, Laurent Thévenot note qu'une première étape de l'approche informationnelle des activités a d'abord consisté dans l'élaboration de grammaires d'action, à l'époque des premières saisies informatiques faites à des fins de management : « Alors que les classifications de métiers saisissent des états professionnels, les modes de "capture" décentralisée visent des unités d'activité plus élémentaires, de l'ordre de la tâche, [...] unités élémentaires réplicables, actions types reconnues par un système comptable, aux fins d'un "micro-management". »[1] Aujourd'hui, les techniques de capture et de traitement sont en mesure de cerner des profils encore plus fins. Qu'il s'agisse de nos loisirs, de notre travail, de notre consommation, de notre participation politique ou même de notre cognition (façons de lire, écrire, chercher, trier, etc.), nos manières de faire peuvent être observées jusque dans leurs moindres incohérences ou idiotismes. Au point que la logique de rentabilisation économique ou heuristique des traces s'en trouve inversée : ce qui fait l'objet d'une veille, d'un contrôle et d'une marchandisation n'est plus le *type* reproductible, mais le *token* (l'occurrence), promu au rang de plus-value de toute collecte d'informations[2].

1. Laurent Thévenot, « Un gouvernement par les normes. Pratiques et politiques des formats d'information », *in* B. Conein, L. Thévenot (dir.), *Cognition et information en société,* Paris, Éd. de l'EHESS (Raisons pratiques, nº 8), 1997, p. 229.

2. Voir Louise Merzeau, « Du signe à la trace : l'information sur mesure », *Hermès,* nº 53, 2009, « Traçabilité et réseaux », p. 23-29.

La déliaison des traces

La personne qui sert à étalonner ces procédures n'est pas celle des CV, des appartenances et des papiers d'identité – même si, de plus en plus, elle en tient lieu. C'est une collection de traces disséminées sur les réseaux. Dans l'état actuel des outils technologiques et juridiques, l'individu n'a guère les moyens de contrôler cette collection. Seuls les opérateurs, marchands, moteurs de recherche et services de renseignement peuvent avoir une vue d'ensemble de ses agissements, car ils ont la capacité de les archiver, de les recouper et de les modéliser.

La traçabilité numérique modifie ainsi *de facto* les périmètres de l'identité. Au regard du jeu dynamique des nouvelles normes qui structurent la présence et les échanges réticulaires, les règles qui rapportaient la personne à une unité, une permanence ou une volonté peuvent difficilement s'appliquer. Pour comprendre de quoi est fait ce double numérique, rappelons que dans l'environnement virtuel, le monde physique n'est pas déréalisé, mais *augmenté* par des données qui traduisent ses habitants en termes *calculables*. Dans les médiations analogiques, « la sémantique de la relation ou du cadre précède les contenus de nos représentations en général, et pilote celles-ci. Ou pour le dire autrement, communiquer suppose toujours deux niveaux d'émission ou de réception des messages : premièrement des messages-cadres, et sur la base de ceux-ci des messages de contenu ou d'information proprement dite »[1]. Dans l'espace augmenté du numérique, cet étagement des niveaux d'information vole en éclat. Les données récoltées sont des « unités isolables, agençables et calculables »[2]. Automatiquement produites, les traces ne sont plus cadrées par une métacommunication. Elles se détachent des procédures qui enchâssaient les énoncés, ouvrant sur des énonciations « incertaines », nomades et différées. Ces déictiques d'un genre nouveau ne renvoient pas à un espace-temps stable ou assignable, mais à une identité mobile et protéiforme, qu'il s'agit de prendre en filature.

Le pouvoir de surveiller dépend maintenant de la capacité de collecter, compiler et croiser ces unités d'informations essaimées par les individus. Google, Amazon, Facebook ou NSA : l'ascendant exercé par les principaux

1. Daniel Bougnoux, *Introduction aux sciences de la communication,* Paris, La Découverte, 1998, p. 19.
2. Roger T. Pédauque, *op. cit.,* p. 186.

acteurs de la traçabilité repose sur leur maîtrise des techniques de traitement susceptibles de réagencer les indices pour *les faire parler*. Clé de toute exploitation administrative, policière ou commerciale, la déliaison des traces autorise aussi des réappropriations occasionnelles, en fonction des stratégies et des besoins de chacun. À ce titre, la traçabilité relève autant de la surveillance que de la « redocumentarisation »[1]. Si on désigne par là le processus par lequel les récepteurs – destinataires ou non – peuvent réarticuler les documents selon leur interprétation, on voit qu'il recoupe en partie les méthodes de profilage. Comme n'importe quelles données, les traces identitaires se prêtent à des recoupages et des croisements, dans des dispositifs modulaires qui séparent forme et structure (balises XML *widgets,* API). Leur exploitation ne se limite pas au rapport asymétrique entre des individus d'un côté et des appareils panoptiques de l'autre. Elle relève aussi de la socialisation de l'Internet, qui rend possibles des reconstructions de contenus individuelles « à la volée ». *Podcast,* blogs, syndication... c'est dans le Web 2.0 que la personnalisation trouve ses vecteurs les plus actifs, avant que le Web dit « sémantique » ne radicalise la fragmentation des contenus en documents virtuels personnalisables, recalculés dynamiquement.

La déliaison des traces a donc pour enjeu une externalisation du sens. Particules « si élémentaires qu'on les croit vierges de toute signification »[2], leur pertinence dépend moins de ce que l'émetteur y dépose que des opérations d'extraction, d'annotation et d'agencement auxquels elles sont soumises. Beaucoup d'informations triviales, qui ne contiennent *a priori* aucune donnée sensible, peuvent acquérir un caractère personnel par analyse, recoupement, traitement sémantique ou commentaire d'un tiers. « Objets politiques et non sémantiques »[3], les traces ne font sens que pour celui qui les prélève et les traite. Tout dépend de l'agencement des « briques » : c'est l'intermédiation technologique qui confère et oriente l'intelligibilité, en fonction des attentes spécifiques du contrôleur.

1. Voir Jean-Michel Salaün, « La redocumentarisation, un défi pour les sciences de l'information », *Études de communication,* nº 30, *Entre information et communication. Les nouveaux espaces du document,* Université de Lille 3, 2007.

2. M. Melot, préface à Roger T. Pédauque, *Le document à la lumière du numérique, op. cit,* p. 14.

3. *Ibid.*

Information sur l'information

Si l'individu peine à maîtriser la trajectoire des traces qu'il émet, c'est parce que l'information utile s'est déplacée de la surface lisible des messages aux couches internes, moins déchiffrables. L'instabilité des documents impose en effet de dédoubler chaque inscription par une *information sur l'information*. Pour traiter des assemblages dynamiques, dont les composantes se renouvellent par bifurcations, il faut des métadonnées. Ce sont elles qui permettront aux contenus d'être découpés, classés et recyclés par des « agents intelligents ». Cette information au deuxième degré n'a pas pour fonction de cadrer le message comme du métalangage, mais de le rendre disponible pour d'autres contextes. Ainsi les contenus valent de moins en moins par eux-mêmes, et de plus en plus par les données qui leur sont attachées : descripteurs, *tags,* notes d'évaluations ou commentaires.

Grâce aux *metatags,* les traces que nous laissons sur les réseaux peuvent elles-mêmes être réinjectées comme des contenus offerts au calcul ou à la curiosité d'autrui. Les empreintes des uns sont recyclées en traces des autres, faisant des données personnelles l'espace même où nous naviguons : mes commentaires sont reversés dans l'hypertexte collectif de la blogosphère, mes achats dans la vitrine des sites de vente en ligne (Amazon), mes photos de vacances dans des cartographies interactives (Flickr) et mes goûts musicaux dans les webradios (Deezer).

L'élaboration d'index et de cartes devient donc un enjeu majeur dans la compétition que se livrent les industriels de la communication. La puissance de contrôle ne dépend plus seulement de l'achat de bandes passantes et de serveurs. Il faut aussi développer des outils de représentation des données, d'où procéderont de nouvelles offres de services.

Tout est mis en œuvre pour que les prescriptions d'achat ou d'opinion paraissent émaner directement de la pratique des autres utilisateurs. Se multiplient des outils comme Hotmap ou TouchGraph, qui permettent d'observer ce que d'autres ont cherché, visionné ou marqué. Et tout message tend à se convertir en « statut » s'affichant sur un mur comme un embrayeur de conformisme. Dans tous les cas, la pertinence n'est plus ni absolue, ni individuelle, mais indexée sur le cours changeant des humeurs, des visites et des rencontres.

Industries de l'attention

L'information étant maintenant surabondante, le bien rare est l'attention. Le traçage des singularités a pour finalité cette captation du regard, du clic ou de l'écoute dont dépendent l'achat ou l'adhésion. « Tant en ce qui concerne les entreprises que l'État, les informations personnelles constituent la matière première essentielle d'une "économie de la connaissance" qui s'appuie sur la personnalisation, la réactivité, l'agrégation de services autour de l'individu, la mobilité et la continuité. »[1] Comme l'information elle-même, cette économie consiste à réduire l'incertitude en calculant des prévisibilités. La surveillance des réseaux vise moins à contraindre ou interdire des agissements qu'à les anticiper. Avec la capture toujours plus fine des préférences et des manières de faire, les stratèges du traçage attendent de nos empreintes qu'elles prédisent nos comportements. Jusqu'ici, l'indexation servait à décrire des contenus ou à en baliser l'accès. Désormais, elle vise à constituer des « bases de données de nos intentions »[2].

La traçabilité numérique prolonge donc logiquement le modèle qui a dominé l'industrialisation de la culture. Ce modèle, rappelons-le, repose sur une « fabrication industrielle du désir, rendue possible par les technologies d'information et de communication, [et il] consiste à catégoriser les singularités, c'est-à-dire à rendre calculable ce qui, étant incomparable, est irréductiblement incalculable »[3]. La personnalisation de l'information et les modes de surveillance qui en découlent postulent aussi une calculabilité des identités. Mais celle-ci est maintenant censée s'enregistrer d'elle-même, par capitalisation de préférences. Bien sûr, les choix individuels à partir desquels les profils sont modélisés ne sont pas produits *ex nihilo*. Dépendants eux-mêmes des conditions sociales, économiques et culturelles dans lesquelles ils sont effectués, ils expriment moins une liberté qu'un consentement aux offres qu'ils sont censés orienter.

Ce qui s'enregistre, c'est en fait l'adhésion aux « logiques absolues de sécurité, d'efficacité, de confort et d'interaction »[4] devenues indiscutées.

1. « Le nouveau paysage des données personnelles... », art. cité.
2. Expression utilisée par John Battelle pour qualifier le moteur Google dans *The Search, How Google and its Rivals Rewrote The Rules of Business and Transformed Our Culture,* ■■, Portfolio, 2005.
3. Manifeste d'*Ars Industrialis* <http://www.arsindustrialis.org/le-manifeste>.
4. Antoinette Rouvroy, art. cité, p. 7.

Dans leurs manières de s'exposer, les individus procèdent eux-mêmes à des sortes d'analyses de risque, évaluant ce qu'ils peuvent gagner en biens, en informations ou en commodités au prix de la confidentialité. On peut aisément en déduire que tous ne sont pas égaux face à la traçabilité : le bénéficiaire de services sociaux, l'activiste, le supporter et le consommateur n'ont ni les mêmes choses à perdre, ni les mêmes choses à gagner dans ces tractations de données à caractère personnel.

Dans ces stratégies de la certitude, la prévention de l'insécurité est au premier rang des arguments indiscutables. À l'ère du terrorisme mondialisé, gestion gouvernementale et marketing travaillent ensemble à faire sauter les derniers verrous qui protègent la *privacy*. Du *Patriot Act* à la loi « Hadopi », visées sécuritaires et maximisation des profits justifient l'essor de la surveillance au nom d'un même principe de réduction des risques. Plus subtilement, l'État exerce de plus en plus son contrôle par le biais des services dont il devient, au même titre que les entreprises, le prestataire. C'est ce dont témoigne le détournement de certains dispositifs d'identification du secteur public vers des applications relevant de transactions privées, comme pour le pass Navigo ou la carte d'identité électronique. Comme l'avait annoncé Deleuze[1], c'est par la technique et la normalisation plus que par la répression que les individus font aujourd'hui l'objet d'une surveillance.

Sociabilité de veille

Ce que Deleuze en revanche n'avait guère prévu, c'est que les moyens de surveillance allaient se démocratiser au point d'alimenter de nouvelles formes de sociabilité fondées sur la logique de veille. Dans l'ensemble des rapports sociaux, nous sommes désormais précédés par le double numérique que chacun peut consulter en « googlant » sur notre nom ou en utilisant des moteurs d'identité comme 123people[2]. La multiplication de ces outils destinés à différents publics atteste le déplacement des pratiques de profilage du modèle asymétrique pouvoir/individu vers celui, horizontal, des relations interindividuelles, professionnelles ou privées. Domi-

1. Gilles Deleuze, « Post-scriptum sur les sociétés de contrôle », *L'autre journal,* nº 1, mai 1990.

2. <http://www.123people.fr/>.

nique Cardon relève que « si les usagers expriment une crainte générique et prospective à l'égard de la "surveillance institutionnelle", sur laquelle ils n'ont pas d'autre prise que d'espérer une régulation juridique efficace, ils sont en revanche impliqués pratiquement dans la gestion de leur visibilité face à la "surveillance interpersonnelle". Or de ce point de vue, avant d'être un risque, la visibilité est perçue par certains comme une opportunité »[1]. Aussi hasardeuse soit-elle, cette démarcation que font de nombreux internautes entre traçabilités volontaire et subie s'avère déterminante dans l'évolution des formes de présence numérique.

Pour l'adepte des réseaux sociaux, les traces qu'il dépose ne sont pas des indices imprudemment laissés, mais des signaux relationnels relevant de stratégies de réseautage et de valorisation. Dans un nombre croissant de groupes, une large présence réticulaire est exigée pour garantir statut et autorité. L'individu doit surtout savoir construire ses profils avec discernement, en tenant notamment compte de la spécificité de chaque plateforme (on n'affiche pas la même chose dans Facebook, Meetic ou LinkedIn). Il doit aussi savoir alterner productions, expositions et simulations, en jouant de « la dimension polyphonique de l'identité numérique »[2]. La vérité n'est pas nécessairement un critère, car la compétence relationnelle recouvre aussi la maîtrise des rôles et des avatars. En même temps, les données habituellement considérées comme sensibles (orientation sexuelle, opinions politiques, appartenance ethnique...) peuvent s'avérer les plus pertinentes pour se faire admettre dans un collectif.

Dans tous les cas, c'est la veille exercée par les autres qui fait le prix des données délivrées. Qu'elles soient publiques ou destinées à une communauté restreinte, les informations ne valent que par leur degré de visibilité : ce qui compte, c'est de montrer mon réseau en même temps que je m'adresse à lui, à travers des jeux de plus en plus subtils d'adresses et d'emboîtements qui dessinent de nouvelles mondanités (par exemple, afficher ses messages Twitter sur son mur Facebook).

Cette production d'une image protéiforme, flexible et pseudo-anonyme de soi relève à coup sûr d'une réappropriation. Il est encore trop tôt pour dire si l'individu parvient ainsi à réellement s'autodéterminer. Pour le moment, la surveillance horizontale n'est un facteur d'émancipation qu'au sein de communautés suffisamment homogènes pour s'entendre sur

1. Dominique Cardon, « L'identité comme stratégie relationnelle », *Hermès,* nº 53, p. 61.
2. Milad Doueihi, *La grande conversion numérique,* Paris, La Découverte, 2008, p. 95.

des normes de comportements. Mais ce n'est qu'en comptant avec cette sociabilité de veille qu'on trouvera des moyens de réguler la traçabilité des identités.

4. DE LA PROTECTION À LA NORMALISATION

Tactiques d'anonymisation

Interdire ou contraindre les pratiques de surveillance numérique s'avère souvent inefficace. Mieux vaut chercher les moyens de garantir un droit à l'*hétéronymat,* soit par l'usage généralisé de pseudos certifiés, soit par la construction de personnalités alternatives. Les individus réclament en tout cas de plus en plus la possibilité de régler eux-mêmes le degré de visibilité de leurs données. Un marché de la e-réputation n'a pas tardé à se développer autour de cette aspiration, pour proposer aux internautes trop exposés logiciels et services de nettoyage. Spécialistes en « capital réputationnel », « managers d'empreintes numériques » et autres coaches d'identité multiplient ainsi les appels à la prudence, tout en vivant des égarements réticulaires de leurs clients...

Pour ceux qui préfèrent prendre eux-mêmes en main leur protection, il existe une large panoplie d'outils d'anonymisation. Des simples mots de passe aux systèmes d'authentification forte, des adresses mail jetables aux technologies de filtrage collaboratif, et des identités fédérées aux « i-cartes », les solutions ne manquent pas pour renforcer la sécurité sur les réseaux. Pour certaines, la protection est essentiellement technologique (cryptographie, puce, biométrie), pour d'autres, elle passe par la médiation de tiers (certificats électroniques) ou de cercles de confiance (OpenId, Liberty Alliance).

À travers beaucoup de ces propositions, un même principe fondamental commence à émerger : celui d'une nécessaire dissociation entre l'identification (mettre un nom sur une trace) et l'authentification (certifier que cette trace correspond à un utilisateur référencé). Dans leur très grande majorité, les transactions numériques n'ont en effet pas besoin que l'individu soit identifié par son état civil. Seule les caractéristiques utiles pour traiter l'échange en question sont nécessaires : préférences, affinités, solvabilité, statut (étudiant, chômeur...), etc. La logique de personnalisation est

parfaitement compatible avec ce principe, dans la mesure où elle consiste précisément à substituer la pertinence de l'information à la catégorisation des acteurs. L'exigence de sécurité est elle aussi respectée, puisque l'authentification protège à la fois l'utilisateur et le prestataire des falsifications et usurpations d'identité.

De la loi aux normes

De toutes les études menées sur la protection des données personnelles, il ressort qu'il est vain de prétendre arrêter la double tendance à la surveillance et à l'exposition de soi. Ce qu'il est en revanche possible de réclamer, c'est que soient mis en place des protocoles garantissant une plus grande étanchéité des données. Au lieu d'être un objet de transaction et de recoupements (souvent faits à ses dépens comme entre banque et assurance, ou e-commerce et services sociaux), l'individu devrait pouvoir gérer lui-même son « portefeuille d'identités », en cloisonnant ses registres de présence.

La loi est évidemment là pour fixer un certain nombre de principes coercitifs, mais elle ne suffit pas à garantir cet « habeas corpus numérique »[1]. S'exerçant de l'extérieur et s'assimilant à « des défenses fixes »[2], elle ne peut quadriller les pratiques réticulaires qu'en allant contre leur logique, c'est-à-dire, dans l'absolu, en suspendant ce qui les fait exister. Les efforts de la CNIL pour contraindre ceux qui enregistrent nos traces à respecter des règles de finalité, de proportionnalité, de pertinence, de transparence et de non-conservation sont loin d'être inutiles[3]. Ils ne dispensent pas de chercher des moyens de régulation *en adéquation avec l'objet à réguler*. Or plus qu'un réseau à proprement parler, cet objet consiste « en un ensemble de normes, permettant à des machines de traitement numérique de l'information d' "inter-opérer" »[4]. C'est à ce niveau que doivent être repensés les protocoles de saisie, d'accès, d'échange, de mise à jour et de rectification des données. « De la "personne-fichier" à la

1. Michel Arnaud, « Un habeas corpus numérique », *Médium,* nº 13, 2007.
2. « Le nouveau paysage des données personnelles », art. cité.
3. Le rapport annuel d'activité pour 2008 est consultable sur le site de la CNIL : <http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-29erapport-2008.pdf>.
4. Éric Brousseau, Nicolas Curien, « Économie d'Internet, économie du numérique », *Revue économique,* vol. 52, numéro hors série, octobre 2001, p. 10.

"personne-graphe-hypertexte", il y a une évolution fondamentale des normes »[1] à mettre en œuvre, incluant une gestion dynamique des données et une granulosité adaptée aux nouveaux contours de l'identité.

Actuellement, les normes du Web servent plutôt à rendre possible le contournement technique des règles légales de protection. Dans les commissions de normalisation, les normes de marché prennent de fait encore souvent le pas sur les normes de droit. La place croissante de la société civile dans la gouvernance de l'Internet confirme cependant que la normativité réticulaire est non seulement concurrentielle, mais fondamentalement *ouverte*[2]. Plus que jamais, il faut rappeler que la normalisation des technologies de l'information ne concerne pas seulement des objets ou des procédés, mais des comportements. La construction concomitante des dispositifs et des dispositions ne doit donc pas être confisquée par des « experts », mais soumise à l'intelligence collective des citoyens-consommateurs. C'est à cette condition qu'on garantira une contestabilité sociale et une réappropriation citoyenne de la sous-traitance technologique. Sans cette prise de conscience que les normes ne sont pas qu'une affaire d'informaticiens, la surveillance continuera de s'exercer à nos dépens, y compris celle que nous mettons nous-mêmes en œuvre.

1. Renaud Fabre, « La personne : une régulation par les normes ? », *Hermès,* nº 53, p. 178.
2. Sur l'ébranlement de la normativité par Internet, voir Paul Mathias, *Des libertés numériques. Notre liberté est-elle menacée par l'Internet ?,* Paris, PUF, 2008.