



HAL
open science

Partager ses secrets en public

Louise Merzeau

► **To cite this version:**

Louise Merzeau. Partager ses secrets en public. Médium: Transmettre pour Innover, Ed. Baby-lone, 2013, Secrets à l'ère numérique, 2013/4-2014/1 (37-38), pp.153-172. 10.3917/mediu.037.0153 . halshs-00962608

HAL Id: halshs-00962608

<https://halshs.archives-ouvertes.fr/halshs-00962608>

Submitted on 21 Mar 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Médium N° 37-38,
2013/4-2014/1
Secrets à l'ère numérique
362 Pages

<http://mediologie.org/medium/medium-37-38-sommaire.html>

Résumé

On est tenté d'interpréter l'évolution du Web et plus particulièrement des réseaux sociaux comme la victoire sans retour d'une idéologie de la visibilité, déniait le droit de se dissimuler, de se retirer et de se déconnecter. Cette dictature de la transparence, qui menace aujourd'hui jusqu'aux secrets d'État, signe-t-elle pour autant la fin des opacités, des zones grises et des frontières mouvantes entre ce qui circule et ce qui se cache ? Nous voudrions montrer que l'environnement numérique se caractérise au contraire par un régime de visibilité ambivalente, où publication ne signifie pas nécessairement renoncement au secret. Relevant d'une nouvelle forme de partage, la *privacy* en public est une activité sociale où les individus n'exposent pas tout, mais règlent leurs distances en jouant des possibilités offertes par les plateformes. De leur côté, les industries du Web opacifient les processus algorithmiques sur lesquels reposent leurs stratégies derrière l'illusion d'un espace de communication lisse et transparent, pour orchestrer la grande conversation où tout se dit. Mais, de plus en plus, les usagers semblent revendiquer des zones de non traçabilité.

Louise Merzeau

Partager ses secrets en public

En 1993, Peter Steiner publiait dans une édition du *New Yorker* un dessin qui allait bientôt illustrer tous les articles, billets de blog et autres powerpoints traitant de l'identité numérique : « *On the Internet, nobody knows you're a dog* ». Vingt ans plus tard, c'est tout le pédigrée du



"On the Internet, nobody knows you're a dog."

pauvre corniaud qui se lit à livre ouvert dans ses traces numériques, et plus personne ne croit vraiment qu'on puisse demeurer anonyme sur le Web. Que s'est-il passé dans ce laps de temps ? Le web des pionniers a laissé la place au Web « social ». L'économie de l'attention s'est emparée des sites, qui ont été absorbés dans des plateformes. Les firmes ont fait de l'ouverture un *Diktat*, et le secret a changé de camp...

Logiquement, on est tenté d'interpréter ce retournement comme la victoire sans retour d'une idéologie de la visibilité, rejetant aux oubliettes et en vrac le droit de se dissimuler, de se retirer et de se déconnecter. Cette dictature de la transparence, qui menace aujourd'hui jusqu'aux secrets d'État, signe-t-elle pour autant la fin des opacités, des

zones grises et des frontières mouvantes entre ce qui circule et ce qui se cache ? Évidemment non, et c'est même cette ambivalence qui caractérise le mieux ce qui se joue aujourd'hui dans l'environnement numérique.

Pour le percevoir, encore faut-il renoncer à opposer l'information au secret, car ils sont au contraire indissociables. La première ne s'échange et se traite qu'en s'appuyant sur des *process* qui doivent rester dissimulés ; le second se construit désormais au sein même de l'espace public, comme une modalité parmi d'autres du partage.



L'individualisme connecté : repli ou rapport social ?

La personnalisation de l'information, qui résume les mutations les plus importantes de ces vingt dernières années, a placé l'individu au cœur des espaces communicationnels. Du statut de récepteur, il est passé à celui de vecteur informationnel, chargé tout à la fois d'alimenter, d'évaluer et de retraiter les flux de données. Son propre espace personnel, jusqu'ici protégé des inquisitions médiatiques, s'est ainsi retrouvé objet d'innombrables calculs. Cette évolution est souvent interprétée comme une atteinte au principe même de vie privée. À

l'heure des réseaux sociaux, il ne serait plus ni possible, ni légitime de vouloir préserver une sphère secrète, hors d'atteinte des sollicitations, des observations et des traçages.

Si l'industrie de l'identité à laquelle se consacrent les grands acteurs du Web s'efforce de toute évidence de réduire les distances privatives, on aurait tort d'en conclure la fin de la vie privée. Non pas que ses contours ne soient pas en train de changer, mais les interférences avec la sphère publique n'en suspendent ni l'idée, ni la réalité.

Tout d'abord, la vie privée n'a jamais été synonyme d'une interruption des rapports sociaux au profit d'un retrait dans une bulle secrète. Au fil de l'histoire, elle s'est plutôt construite comme une zone tampon où la pression du groupe pouvait être négociée ou compensée, souvent au profit d'un autre type de relations : la cellule familiale, d'abord élargie puis restreinte au noyau central, est venue contrebalancer la communauté d'appartenance et les rapports de travail, le couple a ensuite permis aux individus de s'affranchir de la famille, avant que l'autonomisation de la personne ne complique encore le tressage des distances sociales¹. Dans les sociétés occidentalisées, chacun revendique aujourd'hui le droit de se comporter et de se définir autrement que par l'héritage ou la contrainte du clan. Mais, en même temps, cette autonomie doit s'éprouver en s'exposant aux yeux, sinon de tous, du moins de ses cercles affinitaires.

Plus que le secret ou la dissimulation, c'est la possibilité de disposer d'une pluralité de modes de partage qui constitue la conquête de la vie privée : pouvoir être *entre soi*, c'est d'abord pouvoir fixer ses propres règles d'échange, indépendamment des conventions, des règlements ou du cours officiel de la bourse. Bénéficier d'un espace privatif, ce n'est pas se soustraire à toute sociabilité, mais contribuer soi-même à la régulation de ses communications.

Sans compter que, dans le contrat social issu du libéralisme politique, c'est pour pouvoir produire du consentement en toute indépendance et participer ainsi à l'espace public que les individus doivent pouvoir se replier dans une sphère intime.

Reste la question de la clôture. Jusqu'à l'explosion récente des médias sociaux, l'existence d'une *privacy* semblait supposer un espace clos, souvent marqué par une séparation physique avec les lieux de la collectivité. Assimilée à la possibilité de se tenir *derrière ses murs*, la vie privée n'était pas loin de s'identifier avec la propriété privée. Mais, en gagnant progressivement sa liberté sur un nombre croissant de coercitions exercées par le groupe, l'individu s'est retrouvé de plus en plus exposé. Tombant une à une, les barrières sociales, psychologiques et symboliques qui lui déniaient la légitimité de se présenter comme tel dans l'espace public, sans une accréditation collective, lui ont assigné un nouvel espace paradoxal : celui d'une *privacy* en public. Non pas qu'il soit devenu cet « homme sans intérieur »² que préconisait l'utopie cybernétique, mais son intériorité doit désormais se déployer hors les murs, dans l'espace interstitiel d'un environnement médiatique de plus en plus complexe.

¹ Voir Louise Merzeau, « Entrouvert », *Médium* n°,

² Voir Philippe Breton, *L'Utopie de la communication*, La Découverte, 1992, p.

³ Georges Duby, « Situation de la société, XI^e-XIII^e siècles », in Philippe Ariès et Georges Duby (dir.), *Histoire de la vie privée*, tome 2, Seuil, 1999, p. 506.

La norme, le secret, le suspect

Sans prétendre refaire ici l'histoire de tous les mouvements qui ont fait bouger le curseur entre les sphères publiques et privées, il n'est peut-être pas inutile de rappeler que notre société connectée n'est pas la première à disqualifier les manifestations d'un retranchement individuel dans une forme de secret. Georges Duby rappelle ainsi que « la société féodale était de structure si granuleuse, formée de grumeaux si compacts que tout individu tentant de se dégager de l'étroite et très abondante convivialité qui constituait alors la *privacy*, de s'isoler, d'ériger autour de lui sa propre clôture, de s'enfermer dans son jardin clos, était aussitôt l'objet soit de soupçon, soit d'admiration, tenu ou bien pour un contestataire ou bien pour un héros, en tout cas repoussé dans le domaine de l' "étrange" [...]. Seuls s'exposent de la sorte les déployés, les possédés, les fous : c'était selon l'opinion commune, l'un des symptômes de la folie que d'errer seul »³.

Malgré l'anachronisme, il est intéressant de rapprocher cette description de celle qu'on pourrait faire des normes sociales par lesquelles les plateformes numériques formatent aujourd'hui les comportements. Ne pas être joignable, ne pas posséder de compte dans l'un des principaux réseaux sociaux, ne pas orchestrer une certaine visibilité de son univers personnel sont devenus des marqueurs d'a-socialité et des motifs d'exclusion, d'autant plus stigmatisants que l'individu est socialement fragile. On sait que les adolescents notamment sont particulièrement dépendants des conventions fixées par leur groupe. Il est inconcevable pour eux de s'épanouir en dehors de ces espaces d'échange et d'exposition, qui sont à la fois des lieux d'épreuve et de protection : des *territoires*, au sens éthologique du terme.

Plus inquiétants sont les propos rapportés par la presse, indiquant que certains psychologues ou employeurs interprèteraient désormais comme une anormalité, signe d'une potentielle dangerosité, le fait de ne pas être inscrit sur Facebook. « Selon eux, les personnes n'ayant pas de compte Facebook sont suspectes car cela signifie qu'elles ont quelque chose à cacher ou que leur compte a été supprimé pour avoir eu un comportement inapproprié en violation avec les conditions d'utilisation du site »⁴. Il suffit ensuite de rappeler que Breivick ou Merah étaient absents ou peu actifs sur les réseaux sociaux pour suspecter toute forme d'abstinence numérique de traduire un inquiétant déficit relationnel. Bien sûr, ce genre de déductions est absurde et totalement infondé (sans parler du fait qu'elles sont occidentalo-centrées). Elles témoignent toutefois de l'instauration progressive d'une norme qui fait des plateformes de réseautage, sinon une injonction sociale, du moins le principal instrument de mesure du degré de secret de nos existences.

Ce détour par la norme nous permet de rectifier plusieurs lieux communs qui continuent d'alimenter nombre de représentations des pratiques en ligne. Tout d'abord, on voit combien

³ Georges Duby, « Situation de la solitude, XI^e-XIII^e siècle », in Philippe Ariès et Georges Duby (dir.), *Histoire de la vie privée*, tome 2, Seuil, 1999, p. 506.

⁴ « Pas de compte Facebook ? Vous êtes suspect », *Numerama*, 7/08/2012, [En ligne] <http://www.numerama.com/magazine/23363-pas-de-compte-facebook-vous-etes-suspect.html>.

l'assimilation entre addiction à la connectivité et désocialisation est un véritable contresens qui, voulant stigmatiser les comportements de certains internautes, manque les enjeux les plus importants de la présence numérique. Comme l'a montré Antonio Casilli dans *Les Liaisons numériques*⁵, ce mythe d'une rupture pathologique entre monde virtuel et réalité témoigne surtout de l'incompréhension par certains observateurs des nouvelles règles qui modélisent les usages d'Internet. Du côté des stratégies orchestrées par les acteurs économiques du Web comme du côté des tactiques mises en œuvre par les utilisateurs, la valorisation de l'individu passe toujours et de plus en plus par celle du lien social. Celui-ci, on le sait, n'implique que rarement des formes d'engagement conséquentes et se limite souvent à la « force des liens faibles »⁶. Mais, quoi qu'il en soit, c'est l'image d'un individu-monade, défini par sa propre clôture, qui se voit disqualifiée au profit de celle d'un sujet-flux, structuré par ses incessants échanges avec son environnement.

La deuxième idée fautive à réviser concerne les jugements moraux portés à l'encontre de l'exhibitionnisme supposé des internautes. Cette appréciation oublie tout simplement que l'écosystème du Web et les pratiques en ligne ont considérablement évolué depuis les années 1990. Rapporter la mise en visibilité des sujets connectés à des pulsions individuelles revient à plaquer sur l'environnement numérique le modèle inapproprié de la télé réalité, lui-même régi par l'idéologie de la société du spectacle. Sans doute encore transposable au moment où les premières webcams livrèrent ici et là quelques existences au fantasme d'une exposition intégrale, ce modèle a perdu toute pertinence dans le Web social. D'une part parce que les comportements décriés ne sont plus le fait de quelques pionniers imprudents, mais de toute une génération. D'autre part parce que l'exposition de soi résulte moins d'un choix que d'une soumission à l'ordre d'une nouvelle médiasphère. À la fois pression du groupe – en ligne et hors ligne – (OM) et affordance des dispositifs techniques – qui contraignent de plus en plus fortement les pratiques – (MO⁷), la propension à se laisser observer résulte bien d'une *astreinte sociale*. Elle n'est ni un effet mécanique des technologies, ni une perversion comportementale synonyme d'inculture ou d'immaturation. Enfin et surtout, la communication d'une grande quantité d'informations personnelles jadis tenues secrètes ne relève pas d'une forme spectaculaire, mais d'une indexabilité de soi. Dans l'univers des réseaux, les regards ne convergent plus vers une scène centrale et l'idée même d'une coupure scénique n'a plus guère de sens. Avant de se projeter dans un rôle, l'utilisateur numérique est d'abord une grappe de données livrées au calcul des machines.

Une transparence à sens unique

La pression exercée sur les internautes pour qu'ils livrent au réseau une part toujours croissante de leurs secrets relève d'une stratégie délibérée des firmes qui se sont fait une

⁵ Antonio Casilli, *Les Liaisons numériques, Vers une nouvelle sociabilité ?*, Seuil, 2010.

⁶ Marc Granovetter, « *Strength of weak ties* », 1973

⁷ OM : organisation matérialisée : MO : matière organisée. Les deux faces de tout médium.

spécialité d'indexer les individus. Menée sur un mode *soft*, cette coercition passe par tout un jeu de contraintes sociotechniques, présentées comme des moyens de faciliter l'accès aux services. Jamais formulé sous forme d'obligation ou d'interdit, mais toujours d'opportunité ou de gain, l'assujettissement aux *process* qui n'ont d'autre but que d'agrèger secrètement toujours plus de données personnelles s'obtient le plus souvent par consentement implicite. La docilité, voire l'indifférence des internautes peut s'expliquer par différentes raisons. Tout d'abord, si la possibilité de paramétrer certaines limitations ou protections est en général laissée aux utilisateurs, ce paramétrage est toujours facultatif et relativement complexe à effectuer. Il demande en tout cas du temps, de l'attention et un minimum de compréhension du système – lequel propose toujours l'alternative de laisser tels quels les paramètres par défaut. Souvent présenté comme l'univers des choix illimités, l'Internet est en fait régi par ces solutions par défaut, qui permettent aux propriétaires des plateformes d'imposer leur loi aux locataires que sont les utilisateurs. Le consentement lui-même relève de cette modalité, puisqu'un nombre toujours croissant de dispositifs fonctionnent selon le principe de *l'opt-out* : le prélèvement des données, l'agrégation des sources ou l'inscription à des services annexes sont automatiquement enclenchés sans autorisation préalable. Dans le mode actif, l'internaute doit cocher une case pour ne plus bénéficier du service proposé ; dans le mode passif, ce n'est qu'a posteriori qu'il pourra engager une procédure de désinscription.

Plus que par intrusion, la pénétration des secrets individuels s'opère ainsi de plus en plus par ramification. Au cas par cas, les utilisateurs sont plutôt prudents et ne livrent consciemment que peu de leurs données sensibles. Mais la capacité d'indexer et de recouper les innombrables traces infinitésimales que nous laissons sur les réseaux donne aux firmes un pouvoir inédit de surveillance. *Graph search*, le moteur récemment mis en œuvre par Facebook, témoigne de cette nouvelle calculabilité des fragments de nos existences. Il permet de mener toutes sortes de recherches dans le graphe social du réseau (c'est-à-dire dans les innombrables indices déposés au fil des ans par les membres), en croisant autant de critères que l'on souhaite. Désormais, il est ainsi possible de retrouver les personnes célibataires de sexe féminin qui habitent telle ville, qui ont lu *Fifty shades of grey* et qui ont déclaré aimer sortir en boîte de nuit. Ou encore, des hommes qui comptent parmi leurs « amis » une personnalité politique extrémiste, qui ont été identifiés sur une photo de manifestation, et qui ont *liké* la page d'un marchand d'accessoires d'autodéfense...

L'agrégation des traces est rendue possible par deux mécanismes. Le premier réside dans la conservation à long terme de toutes les informations captées, quand bien même l'utilisateur a pour sa part l'impression de ne participer qu'à des échanges éphémères. Pour l'individu, cette mémoire intégrale est aussi absurde que celle de Funès⁸, car il n'a les moyens ni de trier, ni de synthétiser cette masse énorme d'instantanés insignifiants. Pour les machines algorithmiques en revanche, la combinaison des préférences, habitudes ou centres d'intérêt, mais aussi d'une quantité d'avis, de contacts ou de propos inconséquents sert à composer, à l'insu de l'internaute, le portrait-robot du consommateur potentiel qu'il est secrètement.

⁸ Voir Jorge Luis Borges, « Funes ou la mémoire », in *Fictions* (1944), Folio, 1974.

Le second mécanisme consiste à relier un nombre toujours plus important de services, dont le maillage permet de croiser les renseignements fournis dans chacun d'eux. Une requête dans le moteur de recherche de Google révélera davantage de secrets si elle peut être corrélée aux messages envoyés par la même personne sur Gmail, aux cercles d'amis qu'elle a sélectionnés sur Google+, aux photos qu'elle a publiées sur Picasa et aux documents qu'elle a partagés sur Google Drive. Ici, l'utilisateur n'a en général plus le choix : s'il veut bénéficier de l'un des services, il doit accepter que ses données soient redistribuées dans l'ensemble des applications contrôlées par le prestataire. Ce tissage de réseaux dans le réseau sert un double objectif : centraliser secrètement toutes les informations que l'utilisateur a plutôt l'impression de disséminer, et l'enfermer dans des silos où il est censé pouvoir mener toutes ses occupations sans jamais s'évader chez les concurrents.

Quels que soient les produits et fonctions qu'ils proposent aux internautes, l'activité des géants du Web se résume aujourd'hui à des services d'identité numérique. En collectant les données de chaque individu, d'un côté ils constituent d'immenses bases de renseignements occultes, de l'autre ils se présentent comme des tiers de confiance fournisseurs et garants de nos identités. Logiquement, cette double finalité ne peut être atteinte que si les internautes renoncent aux pseudonymes et aux identités multiples. Facebook, puis Google ont donc explicitement interdit l'usage de noms d'emprunts aux membres de leur réseau. « Les utilisateurs de Facebook donnent leur vrai nom et de vraies informations les concernant, et nous vous demandons de nous aider à ce que cela ne change pas », peut-on lire dans les conditions générales d'utilisation de la plateforme. La FAQ martèle le même principe : « Facebook est une communauté dans laquelle les gens communiquent en exposant leur identité réelle. Nous demandons à tous les utilisateurs d'utiliser leur vrai nom ». La raison officiellement avancée pour justifier cette obligation de transparence : les internautes se comporteraient mieux et les commentaires seraient plus pertinents lorsque le signataire est contraint de s'identifier. De façon encore plus perverse, les firmes jouent aussi sur le désir supposé de l'utilisateur de savoir à qui il a affaire lorsqu'il communique en ligne : « Les profils Google fonctionnent mieux lorsque l'utilisateur est identifié. Ainsi, vous êtes certain de contacter la bonne personne et les autres utilisateurs savent qu'ils ont affaire à une personne réelle lorsqu'ils consultent un profil. C'est pourquoi dans votre profil Google, vous devez indiquer le nom que vous utilisez dans la vie de tous les jours »⁹.

Cet impératif d'identification représente un recul considérable par rapport aux ressources de la communication en réseau. La possibilité de cloisonner ou démultiplier ses identités, de jouer des clair-obscur et de se protéger des diverses formes d'espionnage ou de harcèlement constitue en effet pour de nombreux internautes l'un des principaux attraits de la présence en ligne. Surtout, c'est cette possibilité qui les pousse à se dévoiler, dissimulés qu'ils sont derrière la garantie de l'hétéronymat. C'est particulièrement vrai des usagers socialement vulnérables (victimes de mauvais traitements, activistes, jeunes homosexuels, etc.)¹⁰. Désormais

⁹ Aide en ligne de Google+.

¹⁰ Voir à ce sujet les travaux de danah boyd.

contraints d'être reconnus en toute circonstance, il n'est pas dit qu'ils continuent de livrer autant leurs secrets aux dispositifs qui les observent. Le mensonge reste cependant toujours possible, et il y aurait beaucoup plus de fausses informations qu'on ne pense dans ce que les firmes croient savoir de nous.

Le secret des algorithmes

Malgré le nombre toujours croissant de souscriptions aux services en ligne, l'équilibre de la confiance entre prestataires et utilisateurs est toujours précaire. Les responsables des plateformes le savent bien, et ils prennent soin de camoufler toute nouvelle contrainte derrière le principe du gagnant-gagnant. Ils se gardent bien en revanche de rendre leur propre système transparent, car leur pouvoir de recoupement des données personnelles est proprement invouable.

Secret de polichinelle ? Oui et non. Certes, la plupart des internautes savent maintenant pertinemment qu'ils sont traqués dans leurs moindres faits et gestes. Mais en règle générale, ils ne voient pas le mécanisme de ce traçage et n'en subissent qu'indirectement les effets. Ils ignorent la plupart des connexions que des services apparemment sans rapport les uns avec les autres établissent secrètement. Ils savent que le site qu'ils visitent dépose dans leur ordinateur un logiciel espion (le *cookie*) ; mais ils ne savent pas que des dizaines d'autres sites réunis dans une même régie publicitaire enregistrent simultanément leur navigation. Ils pensent enfin pour la plupart que cette transparence extorquée en vaut la peine car en personnalisant toujours plus leurs transactions, elle les facilite et les optimise.

En ce sens, l'affaire PRISM a moins révélé l'étendue de la surveillance à laquelle sont soumis les citoyens connectés, que la persistance d'une inconscience ou d'une crédulité qui peinent à mesurer les véritables enjeux de la traçabilité. La collusion entre les formes commerciale et politique de cet espionnage au quotidien n'a pas changé la nature du danger. Mais elle a révélé la perméabilité des sphères, l'imbrication générale des systèmes et la difficulté croissante de déterminer qui contrôle qui : l'État, la NSA ou Google ? En tout cas, plus les individus gagnent en autonomie dans l'organisation de leurs loisirs, de leurs relations et de leurs consommations, plus est forte la tentation de les surveiller jusque dans le moindre détail. À défaut de les commander, il reste aux puissants la possibilité de violer tous leurs petits secrets.

Si elle relève aujourd'hui d'une volonté manifeste de pouvoir, l'opacité dans laquelle sont maintenus les systèmes de traitement n'est cependant pas uniquement au service d'une logique de surveillance. Quand bien même l'intention serait parfaitement altruiste, il est dans la « nature » des algorithmes d'opérer en secret, afin que leur efficacité ne soit pas pervertie par les anticipations et les détournements des utilisateurs. Dans son enquête sur Google, Dominique Cardon montre ainsi que « la condition essentielle de son fonctionnement est que les internautes n'agissent pas en fonction du PageRank, mais que leur choix de liens distribue de façon « naturelle » les honneurs et les oublis. Si les jugements qu'ils s'échangent à travers les liens ont été produits en fonction du méta-coordonateur qui les agrège, la pertinence

épistémique du résultat en sera profondément altérée »¹¹. C'est le principe d'extériorité que Google emprunte à la scientométrie dont il s'inspire : l'instrument ne doit pas interférer avec ce qu'il mesure. Le leitmotiv de la communication de Google en direction des webmasters consiste donc à leur demander de ne pas chercher à percer le secret des calculs qui produiront le classement des sites, car ce classement serait alors faussé. Mais, quand on sait qu'apparaître dans la première page de résultats du moteur de recherche est un enjeu majeur de toute stratégie marketing, on se doute que cette adjuration n'a que peu d'effets. Par toutes sorte de moyens, les responsables de sites s'efforcent de tromper le méta-calculateur pour renforcer artificiellement le référencement de leurs pages. Aux méthodes simplistes (placer le mot « sexe » dans le code source, répéter le même mot-clé en lettres blanches sur fond blanc), ont succédé des techniques beaucoup plus sophistiquées, des plus malhonnêtes (Google bombing¹², duplication de contenu...) aux plus soucieuses des nouvelles normes de la rédaction Web. Ce qui fait dire à Dominique Cardon : « Les internautes ne sont pas à la hauteur des vertus morales du PageRank : les internautes calculent, les internautes sont stratèges parce qu'ils veulent être visibles ». L'indexation des contenus ressemble alors à un jeu de cache-cache entre le moteur et ceux qui l'alimentent. Ayant oblitéré la force récursive des calculs opérés par les internautes, Google est contraint non seulement de ne jamais révéler complètement la formule de son algorithme, mais encore de le modifier sans cesse, afin qu'il ne soit pas instrumentalisé. Constamment testé, ajusté, corrigé, le PageRank devient ainsi le secret peut-être le mieux gardé du monde, au point dit-on que même chez Google, plus personne ne connaît sa formule exacte.

Vivre caché en public

On le voit, loin de produire un espace lisse où tout serait lisible, la transparence informatique est constituée d'opacités, chaque acteur cherchant à préserver sa part d'ombre tout en orchestrant la grande conversation où tout se dit. Paradoxalement, c'est l'injonction de livrer son existence au réseau qui a réintroduit le secret dans nos activités les plus anodines : tout passant désormais par la création de comptes personnels, la moindre communication nécessite des procédures d'authentification, de cryptage et d'autorisation. Celui qui voudrait être pleinement ouvert ou visible ne le pourrait tout simplement pas. Sans *login* et mot de passe, pas de présence possible sur le Web.

À égale distance de l'exhibitionnisme et de la paranoïa, l'observation des pratiques révèle une aptitude des internautes à décliner alors leur visibilité selon d'infinies variations, en fonction des plateformes, des cercles affinitaires, des registres discursifs, des profits escomptés, etc. Ce

¹¹ Dominique Cardon, « Dans l'esprit du PageRank. Une enquête sur l'algorithme de Google », *Réseaux* n° 177, 2013/1, p. 63-95.

¹² Technique de référencement visant à influencer le classement d'une page dans les résultats du moteur de recherche Google, en faisant pointer vers une cible plusieurs sites contenant le même texte. Toute requête sur ce texte conduira alors à ce site même s'il ne contient aucun des termes mentionnés

« design de la visibilité »¹³ combine exposition, simulation et dissimulation, avec un pouvoir de contrôle certes restreint, mais sans cesse réinventé.

Pour *vivre caché en public*, les internautes usent de diverses tactiques. Cloisonner ou dispatcher son identité, on l'a vu, est de plus en plus difficile, car il faut ruser avec les efforts continus des firmes pour recouper les indices de notre présence numérique. Nombreux sont les usagers qui misent au contraire sur la cohérence contextuelle pour leur assurer une relative tranquillité. Comme dans la vie hors réseau – où nous menons toutes sortes d'activités secrètes dans l'espace public – les individus se sentent protégés par le fait de partager avec d'autres une situation. Hors de cette situation, les données qu'ils ont échangées n'ont pour eux plus de sens ou de valeur et ils les abandonnent sans remord. C'est précisément ce qui est de plus en plus reproché aux dispositifs de surveillance : non pas de récolter les traces, mais de les agréger sans tenir compte du contexte. Plus que l'indiscrétion, c'est la violation de l'intégrité contextuelle qui constitue une atteinte à la liberté.

Une autre tactique observée récemment consiste à se cacher d'un réseau trop inquisiteur dans un autre réseau, jugé plus discret. Plusieurs enquêtes ont ainsi montré que les adolescents, taxés un peu vite de « génération Facebook », quittent en masse la plateforme de Zuckerberg pour des univers comme Twitter ou Snapchat. Ce qu'ils fuient n'est pas tant la spoliation de leurs données par la firme, que la surveillance ou le harcèlement exercés au quotidien par leurs proches : parents, enseignants ou relations mécaniquement ramenées par le dispositif qui contraint d'avoir toujours plus de *friends*, sans jamais pouvoir refuser, s'évader ou se retirer. Après un temps où il était de bon ton d'être « ami » avec ses aînés ou toute sa classe, les cercles ont ainsi tendance à se refermer sur l'intimité secrète des vrais liens. Sur Twitter, la possibilité d'user d'un pseudonyme permet surtout de se construire un personnage tout à la fois opaque et célèbre. C'est ce que recherchent ces jeunes, qui ne veulent plus payer leur désir de popularité du prix de leur quiétude.

De manière générale, plusieurs observateurs ont constaté que les natifs du numérique commencent à se rebeller contre les pratiques de leurs aînés : le partage à tout prix, l'interconnexion des univers, l'identification des photos, l'indifférence à la pérennité des traces... Sarah Perez remarque ainsi qu'ils rejettent les valeurs de la génération précédente : « ils ne veulent pas de réseaux sociaux ouverts, ils veulent leur intimité. Ils ne croient pas que tout acte doive être sensé et permanent. Ils imaginent le web comme quelque chose d'effaçable »¹⁴. Contre la surveillance de tous et de chacun, le dernier refuge imaginé par les plus jeunes usagers du Web serait donc l'éphémère. Pour vivre caché, vivons sans archives. C'est ce qui expliquerait le succès de Snapchat, service de messagerie où les images sont supprimées après avoir été partagées. La difficulté de retrouver des tweets anciens constituerait aussi à leurs yeux un des avantages de Twitter, là où leurs parents voyaient une limite de la plateforme.

¹³ Dominique Cardon, « Le design de la visibilité : un essai de typologie du web 2.0 », *Réseaux*, 2008/6, n°152.

¹⁴ Sarah Perez, « *The Rise Of The Ephemeralnet* », *Techcrunch*, 30 juin 2013 (traduction partielle par Xavier de la Porte dans *Internetactu*, <http://internetactu.blog.lemonde.fr/2013/07/12/vers-un-web-ephemere/>)

Combinés à des dispositifs de cryptage, les services qui permettent d'installer des systèmes de communication sans mémoire constitueront peut-être la nouvelle base de la sociabilité en ligne. Après avoir publié sans retenue les miroitements de nos existences, écrasés par nos petits secrets, nous nous réfugierons alors dans le bref et l'oubli comme derniers garants de nos intimités.

<http://merzeau.net/>

louise@merzeau.net