INTRODUCTION

Les intelligences numériques des informations personnelles

*Vers un changement de perspective
pour garantir le droit à la vie privée ?*

BÉNÉDICTE REY

Faut-il aujourd'hui se soucier de protéger « la » vie privée ? Faut-il ouvrir ce questionnement aux effets possibles de l'exploitation et de l'exploration de masses de données toujours plus volumineuses ? Un tel questionnement revêt-il encore un sens, alors que la vie privée, c'est-à-dire aussi les informations relatives aux faits, gestes et préférences des individus sont de plus en plus diversement impliquées dans les environnements numériques inscrits dans notre quotidien ? À y regarder de manière globale, rien n'est moins sûr... Les individus semblent en effet s'exposer et s'observer sans grande réserve ; les systèmes utilisent toujours plus de données d'usages pour diverses applications, du marketing aux recommandations de consommation ; la perspective *big data* vient complexifier la circulation et les usages secondaires (et plus encore) des données. Tout cela semble

renouveler les enjeux en termes de traitement des données, en termes d'usages des informations ainsi produites (notamment leur utilisation à des fins de services qui se veulent de plus en plus individualisés), en termes de capacité à s'y soustraire, aussi. Que deviennent les informations personnelles ayant trait à la vie privée dans un tel contexte ? Quelles opportunités et quels biais peuvent être générés par les dispositifs sociotechniques actuellement utilisés et annoncés comme de plus en plus présents ?

La question de la vie privée s'entend traditionnellement comme celle de sa protection. La vie privée comme valeur essentielle à l'être humain, comme valeur à défendre, s'est élaborée progressivement (Rey, 2012). C'est initialement une volonté de préserver autour de l'individu un espace qui ne soit pas soumis au regard et à l'influence d'autrui qui s'est fait jour, pour garantir à chacun la liberté de penser par soi-même, d'entretenir des liens sociaux librement choisis, de disposer de son image... en un mot de permettre de se construire pleinement comme individu. C'est au détour d'affaires que la vie privée, dans cette essence, a peu à peu été défendue contre diverses intrusions, au premier rang desquelles les risques d'intrusion émanant des gouvernements, et des grands médias de masse. Par ce mouvement, la vie privée est devenue une forteresse à défendre, au bénéfice d'un individu plongé dans des rapports de force déséquilibrés vis-à-vis des auteurs possibles d'intrusion.

Aujourd'hui encore, c'est bien souvent lorsqu'il y a problème que cette préoccupation émerge, aussi bien dans le quotidien de chacun qu'au détour d'affaires venant occuper le terrain médiatique pour quelques heures ou quelques jours. Selon les postures, c'est d'une part la fragilité de la vie privée qui est interrogée, son insuffisante protection face à quelques géants institutionnels ou économiques qui est dénoncée. Mais d'autre part, la pertinence d'une sanctuarisation de la vie privée, au risque d'en figer les contours, est également mise en question au regard de pratiques qui ne cessent d'évoluer, tant du point de vue des usagers que du point de vue des institutions et des entreprises.

Du point de vue des usagers, c'est l'essence même de la vie privée comme valeur à préserver qu'en dernier lieu les frontières mouvantes et subjectives des zones vécues comme publiques, privées, semi-publiques etc. (Cardon, 2008) semblent venir interroger. L'individu contemporain, en quête d'autonomie (de Singly, 2003), en exploration de soi et de ses liens sociaux

au détour de l'exposition et de la mise en partage d'informations sur soi (Cardon, 2008 ; Cardon et Delaunay-Téterel, 2006 ; Allard et Vandenberghe, 2003) témoigne d'une appétence certaine pour les services numériques. Par ailleurs plus responsable de ses actes s'il l'on en croit certains chercheurs (Giddens, 2002), il participerait activement à un basculement de perspective relativement à la gestion et à la protection des données personnelles. Les réseaux sociaux mais également de manière croissante tout un ensemble de services reposent aujourd'hui sur l'exploitation de ces données (générées malgré soi mais aussi très largement « données » volontairement lors des usages) et leur restitution (partielle, le plus souvent) aux usagers sous des formes diversement travaillées et visibles. C'est ce qui confère à ces services sens et valeur pour les individus eux-mêmes (au-delà des enjeux pour les entreprises concernées) (Kessous et Rey, 2009). Les individus ne sont alors plus seulement de possibles victimes d'intrusions émanant d'institutions extérieures (Woo, 2006) face auxquelles ils ne sauraient se défendre sans un arsenal juridique et réglementaire, mais ils deviennent des acteurs de premier plan de la production, de la diffusion et de la consommation de données et d'informations.

Ne se soucieraient-ils donc plus de protéger leur vie privée, alors même qu'ils expriment le contraire dans nombre d'enquêtes (Rallet et Rochelandet, 2011 ; Cardon, 2009 ; Lancelot Miltgen, 2008) ? Ce paradoxe de la vie privée déjà maintes fois pointé est à nuancer. En premier lieu, il s'explique par la confrontation de deux ordres de grandeur distincts. Dans cette expression paradoxale se rencontrent en effet d'une part la réalité de pratiques quotidiennes totalement intégrées dans les manières de communiquer sur soi-même dans le cadre de relations sociales vécues tant en rencontres réelles qu'en ligne (et si ces pratiques sont certes émaillées de tensions ordinaires, celles-ci passent souvent inaperçues¹). Mais d'autre part, l'idée que les traces sont exploitées et exploitables est bien présente, même si elle est souvent peu documentée, et même si la conscience du degré de complexité des dispositifs et de leurs effets suite à l'exploitation de

1. Les enquêtes voulant mettre à jour les micro-tensions quotidiennes et les ajustements y afférant doivent souvent passer par l'observation des pratiques et les entretiens approfondis, tant les accrochages ordinaires en termes de vie privée n'émergent pas spontanément.

ces données semble limitée, comme le suggèrent plusieurs articles de ce numéro.

Un deuxième niveau d'interprétation de ce paradoxe apparent est à souligner. Pour les plus jeunes générations, les usages des technologies numériques de l'information et de la communication (TNIC) à des fins de sociabilité ou à d'autres fins ludiques ou utiles nécessitant le recours aux données de consommation, de préférences, de localisation, etc., font partie du quotidien, avec les opportunités et les risques y afférent. Des pratiques devenues si courantes qu'il semble que l'on doive réfléchir autrement à la problématique de la vie privée, car pour nombre d'utilisateurs il n'est pas envisageable de raisonner son accès, de se prémunir contre les intrusions et autres effets et biais issus des systèmes en limitant ses pratiques *a priori*. Entre confiance décidée et ses stratégies d'arbitrage des risques pris, et confiance assurée vis-à-vis d'un système sociotechnique qu'ils ne maîtrisent généralement pas et dont ils ne peuvent et ne veulent pas se passer (Rey, 2007 ; Kessous, 2007), les utilisateurs semblent davantage concernés par la capacité à intervenir sur ce qui fait tension *a posteriori*. Mais si les individus développent une palette de stratégies diverses pour faire face aux problèmes de vie privée qu'ils rencontrent, et parviennent ainsi à déployer des formes d'intelligences numériques pour apaiser un certain nombre de tensions, il n'en reste pas moins qu'il semble bien déséquilibré de leur laisser l'entière charge de se prémunir contre les effets d'intrusion ou de limitation des possibles que peuvent induire les dispositifs numériques et la manière dont on s'en sert.

Concernant la sphère marchande, cette asymétrie informationnelle entre utilisateurs et acteurs économiques semble renforcée par l'ignorance significative des utilisateurs quant aux codes de fonctionnement des systèmes à l'œuvre derrière leurs usages. En ne mettant pas à jour – y compris pour elle-même ? – les orientations sous-jacentes des systèmes algorithmiques qui explorent et mettent en musique les masses de données disponibles, la sphère marchande entretient en effet l'utilisateur dans un univers spécifique, comme une forme d'enfermement qui ne serait pas tangible. Pour l'instant, du point de vue des services, la question de la vie privée est régulièrement vécue comme une épine dans le pied, empêchant de développer certaines collectes ou certains stockages de données par exemple. Mais au-delà de ce classique espace de tension, travaillé par la CNIL, d'autres enjeux se posent autour de l'utilisation des données d'usage

relatives à la vie personnelle des usagers, à leurs préférences, centres d'intérêts, lieux de prédilection et autres habitudes de consommation. Les intelligences numériques se développant autour de ces données pour fournir de l'information « adaptée », un service personnalisé ou autres recommandations jugées pertinentes pour un individu, sont-elles de nature à élargir, ou plutôt à réduire le champ des possibles pour celui-ci ? Quelle liberté de choisir et de s'orienter reste-t-il si les possibles sont encadrés, tracés par des dispositifs dont on ne mesure pas l'impact prescripteur ?

Or la vie privée, dans sa définition historique fondamentale, s'inscrit dans des libertés fondamentales telles que la liberté de ne pas subir d'intrusions, les notions de respect, de confidentialité mais aussi le maintien d'un certain équilibre dans le partage de l'information entre deux protagonistes (Friedewald *et al.*, 2006 ; Gow, 2005). Ainsi, la vie privée existe dès lors que sont assurées (Rey, 2012) : la liberté de garder pour soi ; la liberté de consentir ou de ne pas consentir (à être dérangé, sollicité, fidélisé...) ; la liberté de ne pas être contraint dans ce que l'on fait, ni dans la manière dont on le fait ; la liberté, encore, de s'autodéterminer dans ses relations sociales et dans ses opinions (Westin, 1967) et de cultiver son individualité (DeCew, 1997).

Les intelligences de la vie privée invitent alors à revisiter notre manière d'en penser la protection. C'est vers un panel de solutions qu'il convient semble-t-il d'aller : prévenir, en amont, les dérives possibles d'où qu'elles viennent, en renforçant les obligations des acteurs à annoncer leur politique de confidentialité et leurs usages des données, mais plus encore à communiquer régulièrement auprès des usagers pour leur rappeler leurs consentements et refus et leur permettre d'actualiser leurs préférences de façon régulière ; sensibiliser et former les individus, dès l'école par exemple, aux fonctionnements et aux codes des environnements numériques et aux intérêts des acteurs en présence ; renouveler, enfin, le *privacy by design*, idée déjà ancienne mais qui peine à s'imposer, alors même que des solutions simples savent exister pour d'autres fonctionnalités (un bouton « j'efface » comme on cliquerait sur « j'aime » ; une manœuvre de type « marche/arrêt » pour tout objet porteur d'une puce RFID² ; etc.). Tout cela devrait être simple, clair, accessible, et être

2. *Radio Frequency Identification* (Identification par radiofréquence).

régulièrement apporté à l'utilisateur plutôt qu'il ne lui incombe de faire tout un travail de recherche et de compréhension, au risque de l'en décourager.

À l'ère du numérique, c'est donc moins de la protection du privé comme entité figée dont il est question que de la capacité individuelle à soustraire à la connaissance d'autrui des informations ayant trait à des faits et gestes que les individus vivent comme privés (ce qui varie selon les contextes, relationnels en particulier). Avec les changements technologiques, serviciels et d'usage, les contours de la vie privée, les enjeux et les modes de régulation évoluent. En laissant les intelligences de la vie privée se déployer sans craindre qu'elles ne deviennent la seule définition du privé, on saurait ainsi conserver à ces valeurs que sont la possibilité de garder pour soi, et de choisir pour soi, toute leur importance : elles seraient alors rappelées par un cadre réglementaire fondamental, mais aussi par des pratiques concrètes permettant d'ancrer la conscience des données disséminées. Peut-être pourrait-on ainsi – sans réveiller la polarisation trop forte opposant des positions pro ou anti-technologies qui font bien souvent juger caduques, voire paranoïaques, les appels à la vigilance en matière de vie privée –, permettre l'exercice effectif d'un droit à disposer de soi-même et des informations issues de nos faits et gestes individuels.

C'est dans ce contexte que ce numéro vise à interroger les « intelligences numériques » de la vie privée, entendues à la fois comme les formes d'organisations intelligentes de la part des individus faisant usage de TNIC, et comme les enjeux se posant au sein d'environnements communicants. Il se compose de cinq articles, qui explorent différents aspects de ces enjeux.

Le premier article interroge ce que les pratiques d'exposition de soi sur les sites de réseaux sociaux nous apprennent sur les évolutions de la pudeur. Choissant de se distinguer d'études focalisées sur l'ancrage numérique de telles pratiques, Fabien Granjon réinterroge ces pratiques dans une perspective plus longue pour permettre une réflexion sur les normes de « contenance de soi ». L'extension de l'intérêt pour les données d'autrui dans le cadre de relations interpersonnelles est aujourd'hui établie, et peut s'apparenter, rappelle-t-il, à une extension du domaine de la surveillance. Mais il ne s'agit pas seulement d'être regardé éventuellement contre son gré ; les manières qu'ont les individus de s'exposer aujourd'hui et d'y donner du sens s'inscrivent en effet dans une problématique de l'attention.

Elles sont, également, à penser comme des conséquences des possibles ouverts et parfois prescrits par les dispositifs sociotechniques mobilisés. Pour Fabien Granjon, les formes d'exposition de soi s'inscrivent aujourd'hui moins dans une fin de la pudeur, et plus largement de la vie privée, que dans une tension entre contrôle et « décontrôle », laquelle se met en acte de diverses manières selon les compétences que les individus parviennent à mobiliser. Ainsi, plutôt que de nier l'importance de la privatisation, il s'agirait plutôt pour les usagers de relativiser les normes et limites associées à la pudeur dans sa définition traditionnelle (Bologne, 1997), relativisation intervenant « en fonction des environnements et des personnes qui participent à ces situations d'exposition de soi. ».

Les articles suivants viennent nourrir un autre aspect de la problématique de ce numéro, en s'interrogeant sur la part prescriptive des dispositifs : comment fonctionnent ces dispositifs ? Dans quelle mesure, en exploitant les traces d'usages dévoilant les caractéristiques, préférences et habitudes de consommation, les différents systèmes à l'œuvre dans les services couramment utilisés risquent-ils de gouverner l'individu contemporain, de l'orienter de manière trop appuyée, au risque de le priver de sa liberté de choix et de son libre-arbitre ?

Nous le rappelions en introduction, la notion de vie privée est bien souvent abordée dans une interrogation portant sur sa protection (ou absence de protection) notamment face à la collecte et au traitement des données d'usage. Dans une analyse intéressante de la perspective foucauldienne, Sami Coll propose ici de pousser plus avant cette perspective critique. Il suggère en effet de considérer la vie privée et les dispositifs notamment marketing y afférent comme un levier possible de la gouvernance des individus. De fait, d'un pouvoir disciplinaire foucauldien à un pouvoir de contrôle tel que proposé par Deleuze (reposant sur une capacité à mobiliser la subjectivité des individus à diverses fins et notamment à des fins de consommation), les TNIC sont en effet perçus par certains tenants de cette approche critique comme outillant la sphère marchande de capacités de « gestion des subjectivités » à distance, permettant de poursuivre l'hypothèse d'un assujettissement consenti (Foucault ; Deleuze ; Rey, 2012). L'enquête de Sami Coll, en étudiant les enjeux relatifs aux données collectées et traitées dans le cadre des cartes de fidélité en Suisse, permet de réinterroger certains concepts de Foucault de

manière originale et de proposer une réflexion inédite sur la vie privée utilisée comme outil de gouvernance des individus.

Marc Ménard propose une autre réflexion sur la part prescriptive des dispositifs numériques. Il s'attache à caractériser et questionner les présupposés véhiculés et mis en actes par les systèmes de recommandation de biens culturels. L'objectif affiché de ces systèmes analysant algorithmiquement, grâce aux multiples données collectées, les habitudes de consommation et centres d'intérêts des consommateurs est, rappelle Marc Ménard, de pouvoir recommander des biens, c'est-à-dire aussi de pouvoir prédire des préférences. C'est la généralisation possible de telles approches à l'ensemble des comportements individuels qui interroge en particulier l'auteur, en tant que les systèmes de recommandation lui semblent présenter le risque de restreindre les choix individuels à ce qui serait identifié comme susceptible de plaire. Plutôt que d'ouvrir la consommation à davantage de diversité, les systèmes de recommandation pourraient alors « enfermer leur utilisateur (...) dans un univers spécialisé qu'il connaît et apprécie déjà », au risque de générer une conformité individuelle. Conscient de la satisfaction que cela procure à nombre d'utilisateurs, Marc Ménard questionne ce risque en soulignant qu'il pourrait bien être accentué par la méconnaissance des procédés par lesquels ces recommandations parviennent aux consommateurs, lesquels ne pourraient pas choisir d'être maintenus ou non dans leur « zone de confort », de permettre ou non à l'inattendu de venir à eux.

Le quatrième article de ce numéro s'intéresse également, d'une toute autre manière, aux dispositifs et aux biais qu'ils peuvent engendrer, en s'attachant au rapport entre données et marchés. Dans une déconstruction-reconstruction originale, Jean-Sébastien Vayre rend ainsi plus explicite le système sociotechnique que constitue le *big data*. Ce faisant il montre, relativement aux enjeux de collecte, de stockage et de traitement des données, et relativement aux enjeux de régulation mais aussi aux problématiques d'usages et de cognition y afférent, que se mêlent d'une manière renouvelée dans le *big data* des aspects aux intérêts différents (scientifiques, techniques, épistémiques, politiques, juridiques, économiques, écologiques, culturels, sociaux, humains) : d'un point de vue sociotechnique, estime-t-il, il s'agit là d'une innovation incrémentale. Mais d'un point de vue sociocognitif, Jean-Sébastien Vayre juge l'innovation radicale, car il ne s'agit pas seulement de traiter ces données multiples, il

s'agit d'apprendre à les exploiter et à les explorer : « Les machines doivent donc apprendre à organiser ces données et à dégager des combinaisons pertinentes afin de permettre à l'homme de les explorer et de les interpréter en temps réel ». Jean-Sébastien Vayre propose ainsi de considérer avec le *big data* un processus d'apprentissage et de construction des connaissances spécifique. En tant que processus de documentation, le *big data* permettrait ainsi d'ajouter de la souplesse dans un environnement instable. Mais il souligne également un risque inhérent au *big data* du fait de son fonctionnement, celui de générer « des biais de connaissances importants sur le plan socioéconomique ».

Dans la continuité du cheminement suivi au fil de ce numéro, depuis une analyse basée sur les études d'usages jusqu'aux travaux interrogeant de diverses manières les systèmes, une cinquième contribution théorique de qualité vient clore ce numéro. Marcela Baiocchi et Dominic Forest interrogent également les formes d'intelligence numérique côté système, et plus précisément les systèmes de recommandation et de personnalisation et la manière dont ceux-ci sont construits. Les auteurs s'attachent à décrypter les différentes méthodes à l'œuvre dans ces systèmes, et en pointent tant les limites (en termes de découverte de nouvelles sources d'information par exemple) que les opportunités non encore suffisamment exploitées à leur sens.

Bibliographie

- Allard L., Vandenberghe F. (2003). Express Yourself! Les pages perso entre légitimation techno-politique de l'individualisme expressif et authenticité réflexive peer-to-peer. *Réseaux*, n° 117, Hermès Science, Paris, p. 191-219.
- Bologne J.-C. (1997). *Histoire de la pudeur*. Paris, Hachette Littérature, Collection Pluriel.
- Cardon D. (2009). L'identité comme stratégie relationnelle. *Revue Hermès*, n° 53, p. 61-66, CNRS Éditions, Paris.
- Cardon D. (2008). Le design de la visibilité. Un essai de cartographie du Web 2.0. *Réseaux*, vol. 26, n° 152, Hermès Sciences, Paris.
- Cardon D., Delaunay-Téterel H. (2006). La production de soi comme technique relationnelle. Un essai de typologie des blogs par leur public. *Réseaux*, vol. 24, n° 138, p. 16-71, Hermès Sciences, Paris.

- DeCew J.W. (1997). *In Pursuit of Privacy : Law, Ethics and the Rise of Technology*, Cornell University Press, New York.
- Deleuze G. (1986). *Foucault*, Éditions de Minuit, coll. Critique, Paris.
- Foucault M. (1975). *Surveiller et punir*, Gallimard, coll. Tel, Paris.
- Friedewald M., Vildjiounaite E., Punie Y., Wright D. (2006). Privacy, identity and security in ambient intelligence : A scenario analysis. *Telematics and Informatics*.
- Giddens A. (2002). *La Troisième Voie. Le renouveau de la social-démocratie*. Le Seuil, coll. La couleur des idées, Paris.
- Gow G.A. (2005 6-8 April). Privacy and Ubiquitous Network Societies. *International Telecommunication Union Workshop*, www.itu.int/ubiquitous.
- Kessous E. (2012). *L'attention au monde. Sociologie des données personnelles à l'ère numérique*. Armand Colin coll. Recherches, Paris.
- Kessous E., Rey B. (2009). La vie privée à l'épreuve de l'économie numérique. *Revue Hermes*, n° 53, p. 49-54, CNRS Éditions, Paris.
- Kessous E. (2007). Quand les objets deviennent communicants. La mise en confiance des acteurs humains et la question des traces numériques. *Annales des Télécommunications*, vol. 62/11-12, p. 1192-1206.
- Lancelot Miltgen C. (2008 Septembre), « Communication de données personnelles sur internet : Incidence des attributs contextuels et individuels », *Journée e-marketing*, Nantes.
- Rallet A., Rochelandet F. (2011). La régulation des données personnelles face au web relationnel : une voie sans issue ? *Réseaux*, vol. 167, n° 3, p. 17-47.
- Rey B. (2012). *La vie privée à l'ère du numérique*. Hermès-Lavoisier, Paris.
- Rey B. (2007). L'insécurité numérique au quotidien : de la régulation quotidienne aux logiques d'alertes. *Actes du 14^e colloque international du CREIS*, Paris, p. 47-59.
- Singly F. de (2003). *Les uns avec les autres. Quand l'individualisme crée du lien*. Armand Colin, coll. Individu et société, Paris.
- Westin A. (1967). *Privacy and Freedom*. Atheneum, New York.
- Woo J. (2006). The right not to be identified: *privacy* and anonymity in the interactive media environment. *New media and society*, vol. 8, n° 6, p. 949-967.