Le droit à la protection de la vie privée comme droit à un avenir non pré-occupé, et comme condition de survenance du commun

Rouvroy, Antoinette

Published in:
Petits entretiens de la vie privée

Publication date:
2016

Document Version
le PDF de l'éditeur

Antoinette Rouvroy

« Le droit à la protection de la vie privée comme droit à un avenir non pré-occupé, et comme condition de survenance du commun. »

Où en est la notion de « vie privée » dans le monde numérique ?

Il ne s'agira pas pour moi de reprendre les sempiternelles lamentations des défenseurs des droits à la protection de la vie privée et des données à caractère personnel, dont les médias font leur miel (la « vie privée » – dans son acception la plus individualiste – est un concept vendeur, qui parle au nombril des gens) : la citadelle individuelle serait, à les entendre, assiégée de toutes parts : intimité, vie privée, données personnelles seraient englouties par le réseau des réseaux. Le réflexe politique mais aussi juridique suscité par ces messages annonciateurs de la « fin de la vie privée » est une fétichisation de la donnée à caractère personnel d'une part, et, d'autre part, une absorption quasiment sans restes de la notion (beaucoup plus large[1]) de vie privée dans celle de la protection des données personnelles[2]. Je pense que l'arsenal juridique déployé afin d'accroître le contrôle que peuvent avoir les personnes sur leurs données personnelles se trompe singulièrement de cible, pour plusieurs raisons.

Premièrement, ce ne sont plus tant nos données personnelles, en tant qu'elles sont relatives à ce qui nous identifie et nous singularise, qui « intéressent » les gouvernements et les entreprises. Peut-être même n'avons-nous jamais été, dans nos singularités respectives, moins significativement visibles et plus anonymes qu'aujourd'hui. Sans doute est-ce d'ailleurs pour cela, en partie, que nous nous acharnons à « devenir visibles » et donc à « exister » sur les réseaux sociaux, un peu à la manière du bourgeois des années 1880 qui se consolait de l'anonymat dans l'espace public en surchargeant son intérieur de ses propres traces : napperons, bibelots, coussins en velours à mémoire de

---

[1] Voir à cet égard la jurisprudence de la Cour européenne des droits de l'homme reconnaissant, au titre de droit à la protection de la vie privée, la nécessité, pour les États, de protéger les individus dans des prérogatives aussi diverses que la possibilité de connaître la qualité écologique du sol sur lequel ils établissent leur résidence, la possibilité de développer librement des relations avec autrui, le droit au libre développement de sa personnalité, incluant celui de connaître ses origines biologiques…

[2] Le nouveau Règlement européen relatif à la protection des données à caractère personnel ne mentionne même plus la notion de vie privée. À cet égard, voir : Gloria Gonzalez Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Cham, Springer, 2014.

forme…[3] Qui nous sommes singulièrement, quelle est notre histoire, quels sont nos rêves, quels sont nos projets, tout cela intéresse sans doute, dans des proportions variables, nos « amis » des réseaux dits « sociaux », mais cela n'intéresse fondamentalement ni Google, ni Facebook, ni la NSA[4], ni aucun de ceux qui nous « gouvernent ». Nous n'intéressons plus tous ceux-là, et d'autres encore, qu'en tant que points de localisation dans des tables actuarielles, ou, pour le dire autrement, qu'en tant qu'agrégats temporaires, supra-individuels (profils), de données infra-individuelles (données brutes) exploitables en masse, à l'échelle industrielle, une fois décontextualisées, purifiées de tout ce qui aurait pu les rattacher à ce qui fait la singularité d'une vie. Nous ne sommes plus identifiables comme auteurs ni émetteurs des données « qui comptent » : les « données brutes », lesquelles sont de fait soigneusement nettoyées des traces de leur contexte originaire et de toute signification singulière. Autrement dit, nous avons changé de monde : la personnalisation, sur un mode industriel, des interactions administratives, sécuritaires, commerciales, sanitaires… ne s'opère plus par la connaissance fine des personnes individuelles, mais par l'entremise d'un profilage de masse pouvant très bien fonctionner sur base de données anonymes, qui n'entrent pas dans le champ d'application des régimes juridiques de protection des données à caractère personnel.

Deuxièmement, ce qui se trouve le plus menacé, aujourd'hui, en raison notamment de la centralisation à la fois des données et des possibilités d'exploitation algorithmique de ces données entre les mains des grosses administrations publiques mais aussi – et surtout – des principales entreprises de l'internet (Google, Facebook, Twitter…), c'est beaucoup moins la sphère privée individuelle que l'espace public, et le commun. La contextualisation, la géolocalisation, tout ce que l'on appelle la « réalité augmentée », entourent l'individu, y compris lorsqu'il se promène dans les espaces publics. Nous assistons à une hypertrophie de la sphère privée et à une privatisation des espaces publics devenus hyper perméables au marketing individualisé et contextualisé. Ce qui est menacé par le projet de supprimer l'écart entre le monde et sa représentation – grâce aux dispositifs de la « réalité augmentée », adaptée en « temps réel » au profil de l'utilisateur – c'est l'expérience commune, l'espace public où nous sommes confrontés à quelque chose qui n'est pas prévu pour nous. C'est cet excès d'individualisation, ce repli sur la monade subjective, qui fait aujourd'hui problème, plutôt que la soi-disant fin de la vie privée.

[3] Voir : Walter Benjamin, « Expérience et pauvreté », *Œuvres, II*, Paris, Gallimard, coll. « Folio essais », 2000, pp. 369-371.

[4] La NSA (National Security Agency) est une agence de renseignement au sein du département de la Défense aux États-Unis.

La protection de la vie privée est-elle un droit ?

Je dirais que le droit à la protection de la vie privée (irréductible à la seule protection des données à caractère personnel) est essentiel dans la mesure où on le conçoit non pas comme la défense d'un individualisme possessif et propriétaire (« mes » données à caractère personnel), mais comme un principe antitotalitaire garantissant la possibilité, pour les individus, d'adopter des modes de vie qui, sans être illégaux, pourraient néanmoins les exposer à des risques de stigmatisation s'ils étaient rendus publics. De même, la protection d'une sphère privée (conçue, cette fois, non comme hyperpersonnalisation de l'environnement, mais comme absence de « publicité ») doit aussi permettre aux individus de se forger des opinions – et d'en changer – sans éprouver le besoin de s'autocensurer par crainte de l'opinion d'autrui. Bref, nous avons besoin, dans la société, d'un certain « niveau » de vie privée afin de garantir la possibilité d'expérimenter des formes de vie nouvelles et une diversité d'opinions essentielles à la vitalité du débat public. Les fondements de la vie privée ne sont pas individualistes mais structurels : à travers les déclinaisons de ses mises en œuvre, la protection de la vie privée permet la vie en commun.

Les fondements de la vie privée sont donc collectifs, alors que le droit à la vie privée et à sa protection est un droit individuel. Comment expliquez-vous cela ?

On pourrait dire que le droit à la protection de la vie privée – dans le sens où j'ai tenté de le décrire plus haut – protège certaines capacités de l'individu (ses aptitudes à réfléchir à l'abri du conformisme, ses aptitudes inventives et d'expérimentation), qui sont nécessaires à l'existence même d'un espace public digne de ce nom : celui où l'on débat de la chose publique non rabattue sur la seule concurrence des intérêts individuels. Le développement de ces aptitudes (on en parle parfois en termes d'autodétermination, ou de droit au libre développement de la personnalité), lorsqu'il est possible (nous ne sommes pas tous égaux à cet égard), justifie que soit déployé un arsenal de mesures permettant de gérer à la fois les besoins de « solitude » (le droit d'être laissé seul), de concentration (protection contre les courriers et appels non sollicités), d'intimité (le droit à la vie privée et familiale, le droit à une vie privée relationnelle), et les besoins d'inclusion et de participation (la protection des données personnelles peut contribuer à éviter la discrimination dans l'emploi, l'assurance, l'enseignement…).

Le cercle familial est-il nécessairement privé ?

Il est privé dans notre culture, à cet instant. Mais la notion de vie privée est à géométrie variable, elle suit l'évolution de la société, l'endroit où l'on se trouve sur la planète ; la vie privée est une membrane vibratile qui sépare l'individu ou sa famille (on parle d'ailleurs de « vie privée et familiale » dans la Convention européenne des droits de l'homme) du reste du monde. La

sphère privée est un lieu dont il n'est pas fait publicité, en principe (la notion de vie privée est d'ailleurs cousine germaine des notions de bienséance et de ce qu'autrefois on appelait la « modestie » : il s'agit tout aussi bien de préserver l'espace public de comportements que la bienséance commande de ne pas exposer au public que d'empêcher les curieux de s'immiscer dans l'espace intime ou familial). Les cartes se brouillent aujourd'hui avec Facebook et d'autres réseaux sociaux, sur lesquels on expose au public des événements relevant de la vie privée (« mon fils ne fait pas ses nuits ! »). Par ailleurs – mais on est là dans la prospective – certains géants de l'internet projettent de déverser de la publicité personnalisée partout dans nos espaces privés à la faveur de l'internet des objets (notre frigo affichera les dernières offres de la grande surface du coin...) : bref, aujourd'hui, la prédation des espaces de vie et d'attention à des fins privées (marketing, publicité) érode la vie privée « de l'intérieur » pourrait-on dire.

Comment définiriez-vous la vie privée à l'heure actuelle ?

Je suis surtout sensible à deux aspects dans l'ensemble des définitions qui existent : le premier, c'est l'argument « démocratique » consistant à voir dans la protection de la vie privée un instrument de protection de la diversité des modes de vie et des opinions, bref, un bouclier contre le *conformisme anticipatif*[5].Le second, c'est le caractère collectif du droit à la vie privée, parce que, même si ce droit est présenté comme un droit de l'individu et de lui seul, la renonciation à la protection de parcelles de sa vie privée et de certaines de ses données à caractère personnel n'est pas une affaire qui ne concerne que l'individu. Je vous donne un exemple : s'il existait un moyen pour chacun d'avoir accès à sa carte génétique entière, permettant de prédire les risques génétiques auxquels nous sommes chacun individuellement exposés, et que moi, je n'avais aucun risque génétique, je pourrais révéler ce « certificat de bons gènes » à mon assureur sur la vie afin de payer mon assurance-vie moins chère qu'un souscripteur qui refuserait de communiquer ces données hautement sensibles (et se verrait dès lors « profilé » comme « mauvais risque »). Ma décision de mettre sur le marché (de l'assurance, de l'emploi...) mes données personnelles oblige tous les autres à faire de même (à renoncer, donc à la protection de leurs données personnelles) sous peine de se voir sanctionnés par le marché. Laisser les individus décider d'échanger leurs données personnelles contre des avantages (quels qu'ils soient), c'est ouvrir la porte aux comportements opportunistes et détricoter la solidarité.

[5] Le conformisme anticipatif renvoie à l'idée que, lorsque nous sommes observés/surveillés, nous nous comportons différemment : nous autocensurons nos gestes et notre pensée, nous rétrécissons nos potentialités d'innovation, d'invention, de spontanéité, nous essayons d'être « le plus normal », d'agir de la façon la plus « conforme » à la norme. Et si tout le monde s'autocensure, nous finissons par être tous les mêmes : le débat démocratique n'existe donc plus puisque tout le monde partage les mêmes opinions.

Dans une société profondément individualiste telle que la nôtre, si cette carte génétique devenait accessible demain aux individus, comment pourrait-on empêcher des discriminations ou disparités de traitement ?

Il faudrait se mettre d'accord collectivement sur les biens de base auxquels tout le monde devrait avoir accès, quel que soit son état de santé actuel ou potentiel, quels que soient son profil Facebook ou son profil de consommateur. Et donc, si on décide que l'assurance-vie est un bien de nécessité, il faudrait voter une loi stipulant l'accès pour tous à un minimum d'assurance-vie, et au-delà, on peut laisser jouer le marché. En Belgique par exemple, un débat parlementaire a donné lieu à une loi interdisant la prise en compte des informations génétiques – même communiquées volontairement par l'assuré – dans le domaine de l'assurance. La solution est dans le débat collectif et dans l'identification de ce qui doit faire débat. En l'occurrence, on le voit : ce n'est pas tant la nature « personnelle » de la donnée génétique qui doit guider le choix normatif, mais plutôt les conséquences – en termes de justice distributive, d'égalité d'opportunités – de leur mise en circulation dans des contextes concurrentiels tels que l'assurance ou l'emploi. Les problèmes relatifs à la vie privée et à la protection des données s'inscrivent dans ce cadre collectif.

Cette vision collective de la vie privée est à contre-courant de ce qu'on entend régulièrement dans les médias : « attention, il faut protéger vos données ! »

Oui. On lit sans cesse que chacun doit être attentif à ce qu'il fait de ses données, apprendre à ne pas mettre n'importe quoi sur Facebook. Je ne nie pas l'aspect individuel de la vie privée ni l'importance de l'éducation, mais ce n'est pas du tout suffisant. C'est bien sûr dans l'air du temps : l'idée de rendre les individus individuellement responsables (voir propriétaires) de « leurs » données, et leur faire assumer seuls les risques d'une surexposition sur la toile (après tout, ils étaient avertis) plutôt que de sanctionner les usages abusifs de ces données par les « gros » acteurs de l'internet. C'est, en un certain sens, légitimer et naturaliser les abus (de faiblesse) pratiqués par les industries qui font leur miel de la prolifération des données en poursuivant des intérêts parfois très désalignés par rapport à ceux des internautes. Cela correspond très bien à l'*ethos*[6] néolibéral dans lequel nous macérons depuis quelques années déjà. Personnellement, je reste très attachée à la valeur de la vie privée. Je pense qu'il faut défendre la protection de la vie privée, mais à condition de sortir du fétichisme de la donnée personnelle et de repenser collectivement les raisons de notre attachement à la notion de vie privée. Car rien de tout cela ne va vraiment de soi.

[6] L'*ethos* signifie, en grec, la manière d'être, les habitudes d'une personne. (Source : Wikipédia.)

Pour vous, quelles sont les raisons de cet attachement à la protection de la vie privée ?

Tout d'abord, il y a une raison absolument pas scientifique : lorsque je constate qu'une valeur est en déclin dans la société néolibérale, j'ai tendance à prendre sa défense, par pur esprit d'opposition peut-être. Je me rends compte qu'on vit dans un régime de capitalisme informationnel où le caractère prédictif des données individuelles est survalorisé et où la valeur monétaire des données personnelles est très (trop !) grande. Par conséquent, ce régime individualise les risques et, en proportion, dévalorise les circonstances environnementales, économiques, sociales et culturelles qui font que les gens sont plus ou moins (mal)heureux dans une société. Vous êtes responsable de ce qui vous arrive : ce n'est pas à cause de la pollution que vous développerez la maladie de Parkinson, mais parce que vous avez le gène prédisposant. Dès lors, j'essaie de travailler la notion de vie privée dans son contexte environnemental, politique, dans son contexte collectif, pour contrer la tendance néolibérale qui exacerbe l'individualisme, qui exacerbe les « libertés » individuelles sans voir que la liberté n'est pas un concept purement psychique, qu'elle a des bases économiques, matérielles, écologiques, relationnelles. Dans le néolibéralisme, vous êtes totalement libre, mais aussi absolument responsable de ce qui vous arrive, y compris de ce sur quoi vous n'avez aucune prise. Si une tuile vous tombe dessus, c'est pour votre pomme !

Vous êtes seul responsable…

Exactement ! Pour caricaturer un peu : ce sont vos gènes qui ont orienté votre comportement, vous avez été poussé par une force intérieure dont la société n'est aucunement responsable et dont vous avez à porter seul les conséquences.

C'est de ce constat – de la société néolibérale et individualisante – qu'est né votre concept de gouvernementalité algorithmique ?

Ce concept de gouvernementalité algorithmique est né de mon intérêt pour les effets produits par la « numérisation du monde » (des quantités massives de données offrant de nouvelles possibilités de modélisation du social), sur les modalités de « gouvernement » (de conduite des conduites). Il s'agit d'un glissement supplémentaire par rapport au mode de gouvernement néolibéral. J'ai voulu décrire ce glissement du gouvernement néolibéral au gouvernementalgorithmique: un mode de gouvernement nourri essentiellement de données brutes (qui opèrent comme des signaux infrapersonnels et asignifiants mais quantifiables) ; qui affecte les individus sur le mode de l'alerte provoquant du réflexe plutôt que sur le mode de l'autorisation, de l'interdiction, de la persuasion, en s'appuyant sur leurs capacités d'entendement et de volonté ; qui vise essentiellement à anticiper l'avenir, à borner le possible, plutôt qu'à réglementer les conduites. Les dispositifs de

la gouvernementalité algorithmique intègrent le *data mining* (l'exploitation de gisements de données massives et brutes qui n'ont individuellement aucun sens) pour en faire surgir des profils de comportements. Le *data mining* permet de gérer les gens de façon personnalisante, industrielle, systématique, préemptive, en ne s'intéressant à eux qu'en tant qu'ils relèvent d'une multitude de profils (de consommateurs, de délinquants potentiels, etc.)

C'est une évolution qui est antidémocratique, selon vous ?

Cela peut paraître très égalitaire, non discriminant, dans la mesure où des profils réalisés par des algorithmes automatiques de corrélation statistique ne visent personne en particulier (ça ne vise pas plus les hommes que les femmes, pas plus les Noirs que les Blancs, pas plus les homosexuels que les hétérosexuels) ; ces algorithmes mettent simplement en évidence des corrélations entre des données, des simultanéités, sans identifier les causes (l'algorithme ne dit pas que telle personne a agi de telle manière parce que c'est une femme, mais parce qu'elle a tel profil, elle a visité tel site internet, voyagé à tel endroit à tel moment). Les profils qui émergent paraissent très objectifs. Ça n'est pas très démocratique, pourtant, car cela fait échapper toute une série de choses au débat public : on sous-traite la détermination des critères de besoin, de mérite, de désirabilité… à des machines fonctionnant sur des algorithmes très peu transparents (ils le seront de moins en moins au fur et à mesure que l'on évolue dans les perspectives d'apprentissage automatique – *machine learning* en anglais).

Un tel dispositif ne va-t-il pas créer de nouvelles formes de discriminations, non plus sur base du sexe ou de la couleur de peau, mais sur base de « catégories », par exemple « ceux qui voyagent dans tel pays sont susceptibles d'être terroristes » ?

Ce type de profilage est classique, il suffit de se procurer la liste des passagers de l'avion. Ce dont il s'agit est un profilage qui croise plusieurs types de données. Les corrélations sont faites sur des bases de données tellement diverses et incommensurables qu'il devient très difficile de superposer ce profilage algorithmique sur des catégories socialement éprouvées : tous les Sikhs avec un turban ne seront pas arrêtés à l'aéroport, mais peut-être qu'un roux à lunettes qui a visité des sites sur l'Afghanistan et sur les drones le sera. Les catégories sociales sont mélangées. Je ne pense donc pas que le risque du profilage algorithmique soit la discrimination à l'ancienne. Le risque, c'est, pour les individus, d'être catégorisés d'une manière qu'ils ne peuvent pas comprendre ni contester, puisque les catégories reposent sur des inductions statistiques et non sur de la causalité. En tant qu'êtres humains rationnels, nous sommes habitués à lier des phénomènes à leurs causes, et non à faire de la statistique sur de très grands nombres. Comme mon esprit n'est pas capable de comprendre pourquoi je suis catégorisée comme terroriste potentielle, et qui sont les autres personnes appartenant à la même catégorie,

je ne peux pas entamer d'action collective. Par contre, quand un groupe de personnes est systématiquement discriminé, ses membres peuvent se regrouper (« j'ai été discriminé à cause de ma couleur de peau », « c'est du sexisme parce que je suis une femme », « c'est à cause de ma religion ») ; il y a une prise contre ce pouvoir-là, il y a du débat, il y a du conflit. Contre le profilage algorithmique, il n'y a pas d'argument puisque c'est la machine qui a décidé.

Ne pensez-vous pas qu'il soit possible, avec le temps, qu'une action collective contre le profilage se mette en place ?

C'est difficile, parce que ces algorithmes sont produits en temps réel, et évoluent en temps réel. Je suis classée dans une catégorie au temps X, et dans une autre au temps Y parce que j'ai reçu un spam sur ma boîte mail. Les profils sont fuyants, *one shot*. C'est ça qui est difficile : pour la première fois dans l'histoire, l'exercice du pouvoir n'est plus assumé par aucune figure concrète, mais par des machines – non pas des instruments auxquels nous faisons faire des choses, mais des machines qui nous font faire des choses. Ce qui compte pour ces machines, c'est des réseaux de données qui ne correspondent à personne en particulier, dans le but d'anticiper des potentialités (opportunités, risques) qui ne visent personne en particulier. Pourtant, ces machines nous gouvernent… Elles nous gouvernent en creux et ne permettent donc pas de débat sur leur propre dangerosité. Le débat, le conflit et la diversité des opinions sont remplacés par l'objectivité machinique de la détection, de la classification et de l'évaluation automatisées.

Cela rend-il les machines d'autant plus dangereuses ?

Ce ne sont pas les machines qui sont dangereuses. Elles peuvent apporter des solutions intéressantes dans de nombreux domaines, en nous dispensant par exemple de séries d'opérations mentales routinières et en nous libérant l'esprit pour d'autres tâches plus « intéressantes ». Cela devient dangereux dans la mesure où cela nous dispense, collectivement, de comparaître les uns devant les autres, de nous rencontrer pour nous mettre d'accord au départ de positions antagonistes, de discuter, de débattre, de rendre compte de nous-mêmes non pas devant des machines, mais devant autrui, bref, dans la mesure où cela nous dispense des occasions et conditions de surgissement du commun. Car c'est précisément du commun, de la communauté, que la gouvernementalité algorithmique semble nous dispenser, au profit d'une régulation systématique, automatique, « objective » et « opérationnelle » du social (dont on pourrait se demander si, traduit sous forme de 1 et de 0, il s'agit encore du « social »). Je dis « objectivité » et « opérationnalité », mais il va de soi qu'il ne s'agit que d'un certain type d'objectivité (machinique), qui n'est pas l'objectivité critique, et qu'il s'agit d'un certain type d'opérationnalité (fluidité), qui n'est pas nécessairement efficace : par exemple, à partir du moment où des algorithmes détectent des terroristes potentiels, on les arrête préventivement, mais on ne pourra jamais savoir si c'étaient des faux-positifs, puisque par définition, l'acte empêché ne s'est jamais produit.

Scientifiquement, ce n'est pas validé, mais c'est opérationnel (réduction des coûts de personnel dans les aéroports, plus grande fluidité des passagers puisque seules certaines cibles sont fouillées). Il y a donc une complicité entre le capitalisme (libération des flux) et ces dispositifs algorithmiques.

En se laissant gouverner par un tel système, n'accepte-t-on pas implicitement la supériorité de la machine sur l'être humain, estimant que la machine ne peut être leurrée ? Les machines sont-elles vraiment objectives et infaillibles ?

Je ne pense pas. Il faut, je pense, voir dans tout cela surtout un changement de « régime de vérité » (pour évoquer Foucault[7]) : une nouvelle manière de rendre le monde signifiant et de pouvoir, à travers cela, agir sur lui. Le témoignage, l'aveu, le discours d'autorité, l'expertise, l'enquête… comme modes d'accès privilégiés à la « vérité » sont en train de laisser la place à l'analyse automatique, en temps réel, de données numériques en quantité massive. Il s'agit, à mon avis, moins d'un désaveu de l'intelligence humaine que de l'exploitation de possibilités nouvelles, inédites, d'accéder beaucoup plus « directement », « immédiatement » (sans passer par aucune médiation langagière, symbolique, institutionnelle, conventionnelle…) à ce qui passe non plus pour une représentation réaliste du réel, mais pour le réel lui-même. La grande illusion des *big data*, c'est l'idée que les hommes auraient enfin un accès immédiat au monde, un accès qui ne passerait plus par aucune médiation, fût-elle langagière, qui nous dispenserait de toute représentation. Le peintre belge Luc Tuymans le dit très clairement : « These days the notion of the *"real" rules everything – not realistic but "real"*[8]. » Cette soif d'immanence – héritée des années 1960, Alain Badiou[9] l'appelle, dans sa critique d'un certain théâtre contemporain, « un appétit excessif pour le réel[10] ». Le refus de toute médiation dans notre rapport au réel est porteur de conséquences « dramatiques » : c'est le refus du droit (de la qualification juridique, de l'intervention du tiers…), de l'institution (en charge de multiples médiations symboliques), de la convention (il n'est plus rien dont il faille convenir puisque le « réel » s'impose de lui-même comme vérité)…

Mais cette « objectivité » n'est bien sûr que de façade : parmi les applications sécuritaires, par exemple, certains systèmes de détection sont conçus en contexte de guerre (conflit israélo-palestinien par exemple) et ensuite transposés ailleurs (États-Unis par exemple). Il va de soi que le douanier américain

---

[7] Michel Foucault (1926-1984) est un philosophe français. Ses travaux traitent des rapports entre *savoir* et *pouvoir*.

[8] « De nos jours, la notion de "réel" gouverne tout – pas le "réaliste", mais le "réel" » ; Luc Tuymans, in Paul Thek et Luc Tuymans, *Why?!*, Conversation by Julian Heynen *et al.*, Berlin, Distanz, 2013.

[9] Alain Badiou (1937-) est un philosophe, romancier et dramaturge français.

[10] Alain Badiou et Nicolas Truong, *Éloge du théâtre*, Paris, Flammarion, coll. « Café Voltaire », 2013.

ne se demande pas comment la machine a appris à reconnaître un risque (de terrorisme par exemple). Il y a évidemment des biais. Ces machines, ces « prothèses cognitives » ont juste besoin d'être opérationnelles. Comment ? En nous dispensant de nous demander pour chaque cas interrogé d'où la personne vient, où elle va, quelles sont ses intentions, qu'est-ce qu'elle a dans ses bagages, etc. Ces machines nous permettent de reporter la responsabilité des décisions sur des machines. On observe le même phénomène dans les administrations. En principe, la décision administrative d'octroi d'aides pour le chauffage en hiver pour les personnes défavorisées est prise sur base d'une enquête sociale, mais supposons qu'on remplace l'enquête par des algorithmes qui croisent les données du chômage, des taxes que vous payez, de vos dépenses, cela facilite la tâche du fonctionnaire, parce que la machine est plus objective que lui. Le problème, c'est que l'enquête sociale permet de se rendre compte qu'une famille est dans des circonstances qui n'ont pas été prévues par le questionnaire ou par l'algorithme, et qui justifient, au nom de la justice et de l'équité, que l'on fasse une exception. La gestion systémique des situations par des assistants sociaux est remplacée par une gestion systématique qui fait gagner du temps et qui permet de contrôler le temps de travail des fonctionnaires. C'est une nouvelle manière « rationnelle » de gouverner les gens, y compris les agents de services publics, en décourageant la prise de décision individuelle (il s'agit de suivre les recommandations de la machine), c'est-à-dire en neutralisant les capacités décisionnelles subjectives des agents : s'ils s'écartent de la recommandation automatique et prennent une décision « qui rate », ils auront à assumer la double responsabilité – de s'être écartés de la recommandation d'une part, et d'avoir provoqué un « échec » d'autre part –, alors que s'ils se conforment à la recommandation automatique, ils n'assument aucune responsabilité pour un éventuel échec, aussitôt imputable à un « bug » de la machine. Le problème, évidemment, c'est que, dans leur objectivité autiste, les machines ne sont pas (encore) dotées de réflexivité éthique.

Qui décide des critères à encoder pour la définition des catégories algorithmiques ? Un humain ou la machine elle-même ?

Cela dépend : certains systèmes de profilage présupposent que les critères soient prédéfinis par les humains, mais de plus en plus, on s'oriente vers des systèmes de *machine learning* dans lesquels les machines apprennent elles-mêmes (par essais et erreurs) à reconnaître les critères pertinents pour l'élaboration des catégories. L'objectif du *data mining*, c'est précisément de ne plus avoir à présupposer les critères de classifications dans les catégories, mais de faire surgir ces critères de la masse des données directement. Il ne s'agit plus d'analyser les données en vue de vérifier ou d'infirmer des hypothèses posées au départ, mais au contraire de faire surgir les hypothèses de l'analyse des données (une analyse qui s'écarte d'ailleurs des pratiques statistiques traditionnelles de bien des manières). En tout état de cause, l'objectif du profilage, ou de la personnalisation, c'est d'anticiper les

comportements, attitudes, trajectoires « possibles » et d'agir sur ceux-ci (de manière à les faire se réaliser ou à les empêcher) avant qu'ils ne se produisent « spontanément ». La cible, c'est la dimension de potentialité qui affecte nos comportements futurs. Pour en revenir à la problématique de la vie privée, on voit bien ici que c'est une toute nouvelle facette de notre vie privée qui se trouve affectée : peut-être faudrait-il, à côté des discussions importantes relatives au « droit à l'oubli », réfléchir aussi à l'instauration d'un « droit à un avenir non pré-occupé ». La dimension de potentialité qui nous habite, cet excès de nos comportements possibles sur nos comportements probables, devrait peut-être être prise en compte au titre du droit à la protection de la vie privée.

Mais les pouvoirs politiques ne sont pas toujours conscients ou renseignés sur ces enjeux…

Non, et je pense que ça leur sert ; les politiciens réagissent de plus en plus à des stimuli, sur le mode du réflexe, sans jamais vraiment prendre de décision. Pourtant, on perd la dignité de la décision politique qui consiste à trancher en situation d'incertitude, sans le filet de sécurité des chiffres et des algorithmes. Prendre une décision, c'est prendre un risque, le risque de se tromper, de devenir impopulaire. Ce n'est pas répondre aux stimuli des réseaux sociaux, ce n'est pas seulement réagir, c'est agir, trancher, poser des gestes décisifs, des gestes qui peuvent rater et dont on assume le ratage.

Qu'est-ce que le droit à l'oubli selon vous, et à quel point doit-il être défendu dans notre société hyperconnectée ?

Je pense que le mot « oubli » est trompeur. Il y a des distinctions énormes entre la mémoire humaine et la mémoire numérique : la première est réputée faillible mais authentique, alors que la seconde est infaillible mais paraît inauthentique. L'humain classe ses souvenirs de façon hiérarchique, par ordre d'importance, il oublie certains événements, tandis que dans la mémoire numérique, rien n'est hiérarchisé, tout est toujours disponible, c'est un actuel qui dure. La réinterprétation du passé est propre à l'oubli et à la sélectivité de l'esprit humain, alors que la mémoire numérique enregistre tout de façon brute, « par défaut ». Cette distinction est importante, parce que je pense que si on ne la comprend pas, on fausse le débat sur le droit à l'oubli. Personnellement, je trouve que l'oubli est important : il faut absolument avoir le droit à une seconde chance ; comme on efface le casier judiciaire après un certain temps, on devrait pouvoir effacer nos traces. Mais le souvenir est important aussi, surtout à l'heure actuelle où une grande partie de nos interactions se produisent numériquement : c'est un devoir d'archive de notre temps. La notion de souvenir est importante : dans *1984* d'Orwell[11], quand le personnage principal trouve un objet du passé sans connaître son utilité, l'objet devient alors *transitionnel*, il permet de réaliser qu'un autre monde a

[11] *1984* est un roman d'anticipation de George Orwell, publié en 1949.

existé avant, que le monde présent est donc relativement contingent, et que le futur pourrait être encore différent. Le souvenir a une dimension transitionnelle aussi, qui permet de se souvenir que la situation actuelle est un résultat relativement contingent, et que le changement est possible.

Comment reconfigurer ce droit à l'oubli, selon vous ?

De toute façon, le droit à l'oubli sur internet est difficile à rendre effectif, parce qu'on ne maîtrise pas les trajectoires des informations qu'on poste. C'est pourquoi je préfère parler de *l'art de se faire oublier*, utile, légitime, nécessaire en certaines circonstances, mais pas de façon absolue. Finalement, sur internet, on joue le jeu si on le veut bien : il y a une économie de la réputation qui peut tout aussi bien nous servir, on peut devenir « célèbre » (par exemple, on peut devenir célèbre comme chercheur si on utilise bien les médias pour parler de nos recherches, ou trouver des collègues avec qui chercher). Je ne diabolise pas du tout les réseaux sociaux à ce niveau-là, mais je pense qu'il faut aussi posséder l'art de se faire oublier si on le désire. Comme tout art, ce n'est pas inné, c'est une pratique qui demande de l'éducation. On ne se comporte pas dans le monde numérique comme dans le monde physique, « l'acoustique » est différente. Mais certaines personnes se comportent de la même manière dans le monde numérique, ce qui donne l'impression qu'elles crient en permanence, qu'elles hurlent en public des secrets privés. Il faut transposer certaines contraintes du monde physique dans le monde numérique, mais c'est une discipline personnelle.

Le droit à l'oubli réfère aussi à l'idée que certaines données personnelles sont retenues à notre insu ou contre notre volonté...

Oui tout à fait. Et là, il y a des prises possibles, car on a affaire à du traitement automatisé à caractère personnel. Le cadre juridique européen permet une série de recours pour les individus. Quand il s'agit de données à caractère personnel, on n'est pas tout à fait démuni, on a le droit à revendiquer l'effacement, la correction. La difficulté est pratique : comment effectivement s'assurer que les données sont effacées ou modifiées ? Et puis, il est vrai qu'il y a une visibilité croissante de tout un chacun aujourd'hui : il suffit d'introduire un mot clé ou un nom dans Google et n'importe qui peut obtenir des tas d'information sur une personne sans se déplacer, alors qu'avant, il y avait une obscurité pratique de certains faits publics. Il y a une importante réflexion à mener sur la numérisation des documents publics.

Peut-on dire que l'identité numérique n'existe pas ? Qu'est-ce qu'internet a changé en termes d'identité ?

Ça dépend de ce qu'on appelle l'identité. Paul Ricœur[12] distingue l'*idem-identité* et l'*ipse-identité*. L'*idem-identité* est donnée par les autres (par l'état

[12] Paul Ricœur (1913-2005) est un philosophe français, qui a développé la phénoménologie et l'herméneutique.

civil qui atteste de qui je suis : nom, prénom, date de naissance, adresse...), elle me permet d'être reconnu. L'*ipse-identité*, c'est l'identité, ou plutôt la personnalité, ou le personnage, que je me fabrique au quotidien, elle n'est pas innée. C'est surtout vrai depuis que les *habitus* sociaux dont parlait Bourdieu ont fortement disparu : avant, si j'étais un garçon avec un père plombier, je devenais plombier ; notre identité se façonnait en fonction de ce qu'on était destiné à devenir, de notre groupe social d'appartenance. Aujourd'hui, c'est différent, l'identité est devenue un idéal normatif : il faut se créer une identité, elle n'est plus donnée *a priori*, « deviens qui tu désires, sois qui tu es ! ». Mais c'est une injonction paradoxale : il faut performer même si on n'a pas d'identité. Moi, personnellement, je n'ai pas encore trouvé mon identité, mais mes performances me font apparaître comme ceci ou comme cela, ce n'est pas absolument constant. J'ai des identités multiples que me donnent les autres (pour ma fille, je suis sa maman, pour mon conjoint, je suis sa compagne, pour mes élèves, je suis professeure) : ça ne me pose pas de problème. Ce qui est problématique aujourd'hui, notamment sur Facebook, c'est que les gens performent leur identité sans se rendre compte que ce qu'ils postent permet de les identifier sur le mode de l'*idem-identité*. Il y a aujourd'hui un conflit entre l'*ipse-identité* (je peux devenir qui je veux sur les réseaux sociaux) et l'*identité-idem* (la NSA, nos employeurs potentiels nous comparent avec d'autres pour étudier notre personnalité) qui nous colle à la peau et qui risque d'être plus figée que l'identité que vous pensez pouvoir changer en permanence, c'est là que se trouve la vulnérabilité et le paradoxe.

Le besoin de se montrer est-il négatif selon vous ?

Non, je pense que c'est un besoin lié à l'individualisation de la société (nous avons besoin de contacts, aussi sporadiques soient-ils), et à l'anonymisation et aussi à la raréfaction de l'espace public (comme expliqué plus haut : l'évocation par Walter Benjamin des intérieurs bourgeois de la fin du dix-neuvième siècle, dont la surcharge en traces de tous genres les consolait de l'anonymat dans l'espace public). Ce n'est pas négatif, il y a d'ailleurs de très belles performances artistiques dans le domaine. Je ne suis pas contre la technologie, mais je constate des vulnérabilités nouvelles (pas spécialement liées à la technologie). Ce que vous contrôlez de vos informations est minime, alors que les *majors* de l'internet (Google, Facebook et tous ceux avec qui ils contractent pour envoyer vos données ou vendre vos données) ont une grande maîtrise de vos informations, de leur signification et de leur valeur. Par exemple, si j'écris sur Facebook « J'en ai marre de mes profs, ce sont tous des cons », ça vous défoule sur le moment, et vos profs ne le verront pas, mais si votre potentiel employeur, dix ans plus tard, consulte une firme de *data mining* et de profilage pour vous embaucher, vous tomberez dans le profil de personnalité « personne rebelle à l'autorité qui risque d'être peu fiable dans une firme », et vous ne trouverez pas de boulot. On pense pouvoir être spontané, libre sur les réseaux sociaux, mais, si nous ne risquons la censure qu'à la marge, nous risquons par contre d'être lourdement

sanctionnés si nos comportements en ligne permettent de nous profiler de certaines manières qui soient contraires à nos intérêts.

La vie privée est donc liée à la spontanéité, la liberté d'expression ?

Oui, dans une certaine mesure, mais à dire cela, on pourrait croire que si notre vie privée semble menacée, nous serions restreints dans notre liberté d'expression. C'est totalement inexact. La situation actuelle, ou celle vers laquelle nous semblons nous diriger, ne correspond pas du tout à celle du roman d'Orwell, *1984*, dans lequel Big Brother censure l'expression libre. La gouvernementalité algorithmique est peut-être le plus parfait opposé d'un pouvoir tyrannique qui aurait aboli la liberté de pensée et d'expression : au contraire, le nouveau mode de gouvernement que je tente de décrire ne fonctionne bien que parce que les individus se sentent libres... de penser et surtout (!) de s'exprimer et donc de « semer » des données. Il suffit d'ouvrir Facebook pour se voir adresser l'injonction « Exprimez-vous » dans la fenêtre dédiée à la publication de nos « statuts ». Vous vous exprimez donc comme si vous étiez entre amis, mais vos propos sont exploités ailleurs... Mais c'est important de pouvoir s'exprimer, c'est pourquoi je pense vraiment qu'il est aujourd'hui improbable que nous nous passions des réseaux sociaux. Dans certains milieux, on n'existe même pas si on n'est pas sur Facebook : on n'est plus invité aux fêtes, aux colloques, il faut donc y être, mais cela induit des comportements par lesquels on peut nous attraper, nous nuire, et là, on est trompé.

On est tiraillé entre deux extrêmes...

Oui, c'est pourquoi il faut plancher sérieusement sur les enjeux de l'informatique, d'où mes recherches sur la gouvernementalité algorithmique : on est gouverné parce qu'on est spontané, on a l'impression d'être plus libre que dans une pièce avec nos parents juste derrière nous à nous observer, mais c'est faux. Il faut réglementer plus systématiquement les pratiques de profilage et de personnalisation exploitant les données circulant sur l'internet et les réseaux sociaux, voire même interdire le profilage dans certains cas, mais c'est un gros chantier. Pour protéger la vie privée, il faut comprendre ce qui est fait des grandes bases de données (données brutes qui ne sont pas nécessairement des données à caractère personnel, rappelons-le).

Qu'entendez-vous exactement par « données à caractère personnel » ?

Dans tous les régimes européens, une donnée à caractère personnel est considérée comme une donnée relative à un individu identifié ou identifiable. Par exemple, le fait d'avoir cliqué sur telle publicité pour tel produit sur tel ordinateur n'est pas une donnée à caractère personnel, parce que cette information peut être complètement anonymisée : ce qui est gardé, c'est le fait que vous avez visité tel site après avoir visité tel autre site dans le but de comprendre votre comportement, votre profil de consommateur potentiel, mais votre nom et votre adresse IP sont gommés. On ne peut donc

pas identifier qui a cliqué sur tel site. Grâce à ces grandes bases de données anonymisées, il est possible de créer des algorithmes prédictifs, des modèles de comportements (de consommation, par exemple).

Qu'en est-il des données que Google (et d'autres) revend à des entreprises pour leur permettre de mieux cibler notre comportement d'achat : avons-nous des possibilités de prise là-dessus ? Des leviers d'action ?

On a très peu de moyens de contrôler ces données qui font l'objet de transactions. Surtout s'il ne s'agit plus de données à caractère personnel au sens de la loi. En Europe, il est théoriquement interdit de revendre des données à caractère personnel, sauf exceptions. Dans les faits, on n'est jamais sûr que ce n'est pas revendu, c'est difficile à contrôler. En principe, en Europe, les *maîtres de fichiers* (ceux qui traitent les données à caractère personnel) sont tenus de notifier aux Autorités de protection des données (en Belgique, la Commission de la protection de la vie privée[13], en France, la CNIL[14]...) les types de traitements qu'ils font (pourquoi, pour quelle durée, etc.), et il y a normalement un contrôle, mais en Belgique la Commission de la protection de la vie privée est surchargée. C'est tout le problème de la régulation de la protection de nos données : le droit existe, mais il est difficile à faire respecter dans les faits. Je pense qu'une bonne stratégie serait de convaincre les entreprises que, sur le plan compétitif, il serait intéressant qu'elles rassurent leurs clients relativement à leurs politiques en matière de protection de la vie privée, en matière de profilage, etc. Le système de labellisation « respect de la vie privée » pourrait aussi être une voie de solution. On pourrait aussi imaginer un système d'encouragement des entreprises à l'autorégulation, menaçant de rendre les choses obligatoires sans collaboration de leur part. Mais aucune de ces solutions ne fonctionnerait vraiment, concrètement : la menace d'un éventuel procès que l'arriéré judiciaire reporterait *sine die*, le caractère dérisoire des amendes relativement aux profits de firmes comme Google... légitiment les doutes que l'on peut avoir relativement à la possibilité d'infléchir l'exploitation massive des comportements des internautes à des fins qui ne sont pas nécessairement dans leur intérêt. Peut-être qu'un levier plus efficace serait la confiance des consommateurs ; l'affaire PRISM[15] a induit une certaine méfiance (très relative) qui pourrait être une bonne

[13] La Commission de la protection de la vie privée (CPVP), née en 2004, est un organe de contrôle indépendant, qui agit sous la direction de la Chambre des représentants en Belgique.

[14] La CNIL, Commission nationale de l'informatique et des libertés, est l'autorité française de protection des données. Elle veille à ce que l'informatique ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques [www.cnil.fr].

[15] PRISM est un programme de surveillance électronique de la National Security Agency (NSA) aux États-Unis, qui cible les citoyens ne vivant pas aux États-Unis. Edward Snowden, ex-consultant de la NSA, a révélé publiquement l'existence de ce programme en juin 2013, et fut contraint à l'exil. Ces révélations ont entraîné de vives réactions dans le monde, notamment des différents chefs d'État mis sur écoute.

base pour faire pression, mais ce n'est pas évident. Il faudrait que l'affaire de la NSA fasse réellement événement, c'est-à-dire qu'il faudrait que nous décidions de la considérer comme un événement : comme une occasion d'affirmer de nouvelles possibilités d'action, que nous décidions de bâtir quelque chose de neuf à partir de cet événement que nous reconnaîtrions comme point de bifurcation, comme point de rupture ou d'interruption. C'est une décision à prendre : une décision d'organiser les conséquences de cet événement[16]. Cette décision ne semble pas avoir été prise.

[16] À ce sujet, voir Alain Badiou, « Event and Truth », Symposium *Event in Artistic and Political Practices*, Amsterdam, 26-28 mars 2013. Enregistrement disponible en ligne [https://www.youtube.com/watch?v=IE97dwA8wrU].