Identité, différence et droit au secret à l'ère numérique

Pierre-Antoine Chardel, Armen Khatchatourov

Identité, différence et droit au secret à l'ère numérique

Pierre-Antoine Chardel, Armen Khatchatourov

Dans Rue Descartes 2020/2 (N° 98), pages 103 à 117
Éditions Collège international de Philosophie

ISSN 1144-0821
DOI 10.3917/rdes.098.0103

PIERRE-ANTOINE CHARDEL &
ARMEN KHATCHATOUROV

Identité, différence et droit au secret à l'ère numérique

RÉSUMÉ. *L'enjeu de cet article est, tout d'abord, de proposer une réflexion sur l'identité telle qu'elle se voit amplement redéfinie à l'ère numérique, en l'abordant sous l'angle des questions qu'elle nous pose et qui concernent la part du secret qui vient nourrir les processus de subjectivation. Ceci dans une époque hypermoderne où les possibilités d'intervenir dans la gestion de nos données personnelles sont limitées : la multiplication des informations récoltées rend irréaliste l'exercice systématique du consentement et le contrôle par l'utilisateur, ne serait-ce qu'en raison de la surcharge cognitive que cet exercice effectif exige. D'autre part, le changement de nature des moyens techniques de collecte, illustré par l'avènement des objets connectés, conduit à la démultiplication des capteurs qui collectent les données sans même que l'utilisateur puisse s'en rendre compte, comme le montre l'exemple de la vidéo-surveillance couplée à la reconnaissance faciale. Dans ces agencements machiniques, le visible se réduit à ce qui peut être saisi en données, à ce qui relève de la mise à disposition immédiate des êtres, comme si on pouvait percer leurs secrets les plus intimes. Mais au-delà des contraintes générées par les architectures numériques, les possibilités d'entrevoir de nouveaux champs de réinvention permanente de soi demeurent pleinement ouvertes et permettent de créer les conditions d'émergence d'un rapport dynamique et plus inventif au secret.*

L'enjeu du présent article est de proposer une réflexion autour de la question de l'identité telle qu'elle se trouve amplement redéfinie à l'ère numérique. Ceci, en l'abordant sous

l'angle des questions qu'elle nous pose d'un point de vue socio-philosophique et qui concernent la part du secret qui vient nourrir les processus de subjectivation. Nous nous pencherons en particulier sur le fait que, dans le contexte des sociétés hypermodernes qui sont caractérisées par la généralisation des technologies numériques, l'identité se construit selon des plans distincts, mais à nos yeux complémentaires : un premier revient à assurer, dans son élaboration même, un certain droit au secret. Un second renvoie au besoin d'intégrer, dans le processus qui l'anime, un certain jeu de la différence. Où en est le respect de ces deux plans de subjectivation dans une époque où la transparence tend à devenir une norme sociale, voire une injonction ? Par quels moyens, et selon quels arguments, peut-on encore leur résister ? Surtout, avec l'aide de quels appareillages critiques ?

1. L'individu hypermoderne entre accoutumances numériques et protection du secret

Nos servitudes volontaires revêtent des aspects qui sont *a priori* éloignés de celle qui fut décrite par Étienne de La Boétie dans son *Discours sur la servitude volontaire* [1]. Un tel changement de perspective se justifie dans la mesure où, premièrement, la nature de la domination n'est plus seulement politique mais implique des logiques de pouvoir techno-industriel. Il existe un *capitalisme de surveillance* [2]. Et si des formes de servitude volontaire interviennent, par exemple, dans l'acceptation de technologies qui permettent une surveillance accrue des individus, celles-ci n'appartiennent pas purement et simplement au registre de la domination tel qu'il a été thématisé classiquement. Il implique même de nouvelles formes de construction de soi. Comme le souligne Peter Burgess à cet égard, l'écosystème symbolique généré par les médias sociaux dépend fortement d'un système d'auto-façonnage nouveau : « Notre affirmation de nous-mêmes passe par l'affirmation de tous les autres : affirmation d'une représentation fabriquée, forcement incomplète et inauthentique de nous-mêmes, et dont l'inauthenticité est de plus en plus le véhicule de notre personne [3] ». Ces modes d'existence en réseau, qui contribuent à créer une certaine consistance du sujet numérique, prospèrent sans nécessairement impliquer une conscience immédiate des effets néfastes, voire délétères, de ces pratiques de sociabilité en ligne. Surtout, à partir du moment où les critères de dangerosité ou de normalité viennent à changer dans

une société donnée. Le plus insignifiant des propos est alors susceptible de nous être reproché, avec les implications éthiques et politiques que nous pouvons imaginer.

Au-delà de l'économie des affects qui sous-tend la mise en scène de soi, les possibilités d'intervenir dans la gestion de nos données personnelles sont limitées, en rendant de ce fait toujours plus improbable une culture du secret qui viserait à maintenir une distance irréductible entre soi et les autres. Les infrastructures numériques sont telles que si nous les utilisons de manière systématique, nous nous soumettons de fait à un certain régime de transparence : dans la vie quotidienne, on s'aperçoit que la multiplication des informations récoltées rend irréaliste l'exercice systématique du consentement par l'utilisateur. De surcroît, le changement de nature des moyens techniques de collecte, illustré par l'avènement des objets connectés, conduit à la démultiplication des capteurs qui collectent les données sans même que l'utilisateur puisse s'en rendre compte, comme le montre l'exemple de la vidéo-surveillance couplée à la reconnaissance faciale dans les espaces urbains. Plus amplement, on peut songer à la somme des connaissances que les opérateurs acquièrent sur la base de ces données. Il s'agit ici d'une couche de l'identité du sujet dont le contenu et de nombreuses exploitations possibles sont absolument inconnus de la personne qui en est la source.

Dans ce paysage, une forte tendance des acteurs, étatiques et privés, consiste à vouloir s'emparer des traces numériques d'un individu de manière exhaustive et totale, en obéissant de cette manière au phantasme de le réduire à un ensemble de plus en plus complet d'attributs. Dans ce nouveau régime de pouvoir, le visible se réduit à ce qui peut être saisi en données, à ce qui relève d'une conception où une mise à disposition immédiate du « moi profond » des individus pourrait advenir. Les nouveaux régimes de « gouvernementalité algorithmique » reposent en partie sur cette illusion. Si une vision si réductrice de l'homme à ces traces ne peut être défendue au sein des sciences humaines et sociales où l'on sait faire cette différence, elle reste néanmoins opérante lorsqu'il s'agit de politiques industrielles.

Cet état de fait ne va pas non plus sans soulever des questions majeures d'un point de vue éthique et politique. Qu'en est-il de l'exercice du libre arbitre dans des environnements où les

individus n'ont aucune visibilité de l'économie qui s'organise autour de leurs traces ? Est-ce que la volonté de garder la main sur une sphère subjective, qui resterait secrète, c'est-à-dire irréductible au regard des autres, totalement hermétique à tout regard extérieur ou à toute instance de pouvoir, est au fond encore possible ? Fait-elle encore sens ?

Répondre à ces questions nécessite au préalable de reconnaître que notre conjoncture technologique crée une grande porosité, une accessibilité sans limite des dispositifs techniques même lorsqu'ils sont destinés, comme l'écrivait déjà Jacques Derrida, « à garder le secret, à chiffrer, à assurer la clandestinité, etc. [4] ». Le numérique génère une transparence inédite malgré toutes les mesures de protection que l'on peut prendre. En plus de ces contraintes techniques et matérielles, les régimes discursifs qui s'organisent autour de la surveillance sont légion. Dans l'histoire récente de nos sociétés dites « démocratiques », on sait qu'il y a des situations de terreur qui contribuent à encourager certains détournements sémantiques [5], ainsi qu'une forme de domination que le discours vient légitimer. Aux États-Unis, par exemple, le *USA PATRIOT Act* a été conçu pour rappeler que le terrorisme peut surgir partout, qu'aucun individu n'est réellement immunisé contre ce fléau, le mot même d'« exception » pouvant alors perdre tout son sens, devenir contresens [6]. L'exception tend ici à justifier, entre autres, le développement de technologies qui se révèlent toujours plus intrusives, en mettant à mal la possibilité même du secret. Les effets de ces discours vont bien au-delà de l'état d'exception en tant que tel, et installent de manière durable l'idée même de devoir accepter les mutations du droit commun et des libertés individuelles, en faisant passer les logiques de surveillance comme des impératifs en termes de sécurité. Un ordre symbolique s'exprime dans les discours qui accompagnent les technologies de surveillance, et cet ordre symbolique influence non seulement l'acceptation sociale de telle ou telle technologie, mais aussi la manière dont nous nous rapportons à nous-mêmes.

Les tendances que nous connaissons aujourd'hui relatives à l'unification de l'identité numérique, à la généralisation des technologies biométriques ainsi que l'injonction de transparence absolue vont à l'encontre des dynamiques existentielles dans lesquelles un sujet a besoin de puiser pour se construire. L'identité se définissant comme *ipse*, par le fait même de pouvoir s'ouvrir à d'autres possibles. Or les idéologies dominantes qui prônent une surveillance globale rendent de fait (pour ne pas dire *structurellement*) nos vies individuelles de

plus en plus transparentes en suivant en cela une vision naïve et simplifié de la cybernétique.

Il est possible, à ce niveau, de noter une certaine schizophrénie dans la manière dont nous affrontons les questions relatives à la protection des données personnelles ou au respect des sphères privées. En effet, parallèlement à l'expansion de technologies numériques qui nous rendent de plus en plus visibles, conformément aux valeurs qui ont nourri le paradigme informationnel dominant, il semble devenir impératif de formuler des questions relatives au besoin d'opacité, au droit au secret. Mais ces questions sont, de fait, déliées des principes qui ont historiquement contribué à structurer le monde des flux d'informations dans lequel nous vivons aujourd'hui, avec son imaginaire institué [7]. La tâche de problématiser les logiques inhérentes à la surveillance totale est pour cela d'autant plus complexe. Car si nous pouvons souhaiter, d'un côté, reprendre la main sur les systèmes de capture ou de traitement de nos données, nous sommes, d'un autre côté, accoutumés au fait de livrer des parts de nous-mêmes dans tous les moments de notre vie quotidienne. Avec la valorisation sociale qu'une telle exposition entraîne le plus souvent, le régime de transparence épouse les situations les plus ordinaires de l'existence et ne concerne pas seulement les situations les plus exceptionnelles.

Nous avons à cet égard de quoi nous inquiéter face au développement massif de technologies qui assurent à certains acteurs une ubiquité quasi absolue, en saturant les espaces public et privé, « poussant à sa limite la co-extensivité du politique et du policier [8] ». Le développement actuel des technologies restructure en effet l'espace de telle sorte que l'intériorité du chez-soi est toujours susceptible d'être contrôlée ou menacée. Ainsi, avec le développement de technologies de plus en plus sophistiquées, la police a ou peut avoir ses « détecteurs [...] dans nos téléphones intérieurs, nos e-mails et les fax les plus secrets de notre vie privée, et même de notre pur rapport intime à nous-mêmes [9] ». Ce régime de transparence est d'autant plus flagrant aujourd'hui, avec la place croissante des écrans dans nos vies. Ce processus que Derrida décrivait déjà sur le terrain du pouvoir politique, vaut aujourd'hui pour le pourvoir industriel, notamment celui des GAFAM qui exploitent massivement les données de leurs utilisateurs. Face à la multitude des jeux d'acteurs qui interviennent dans les logiques de surveillance (à des fins politiques ou économiques) quelles alternatives est-il encore possible

de proposer ? Une culture de secret, qui pouvait contribuer à enrichir l'expérience de la sociabilité elle-même [10], peut-elle encore tenir aujourd'hui ?

Si nous avons le sentiment qu'une certaine résistance doit s'organiser à l'ère hypermoderne, elle doit l'être en vue de contrer la tentation du déterminisme technologique dont nous aimerions philosophiquement pouvoir nous défaire, mais qui est bel et bien sociologiquement persistante. Cette tentation émane d'une longue histoire, et structure encore beaucoup nos modes de pensée. Une voie possible pour combattre ce déterminisme est l'épanouissement d'une culture de l'interprétation au sein de nos environnements technologiques complexes. Il convient de donner aux subjectivités les moyens d'ouvrir des questions relatives au sens de la coexistence dans des contextes technologiques qui changent désormais sans cesse avec un rythme assez inouï. Et la tâche de déployer une telle réflexion critique est d'emblée complexifiée par le fait que, dans bien des cas, les dispositifs technologiques sont censés nous apporter plus de sécurité, de confort et de fluidité. Une grande part de leur dissémination dans nos existences et de notre soumission volontaire se joue là (depuis l'usage souvent inconsidéré de nos smartphones jusqu'aux objets connectés, en passant par la biométrie ou la reconnaissance faciale).

Afin de contrer au mieux ces tendances à la création d'une identité figée et prédictible (relevant plus de l'*idem* que de l'*ipse*), il convient de défendre les conditions nécessaires à l'épanouissement de l'individu qui ne saurait être réductible à ses traces numériques. Ramener la subjectivité à l'identité numérique, c'est faire disparaître l'être-soi, irréductible à toute typologie, c'est liquider le sujet tragique de la politique, de l'amitié ou de la psychanalyse, le sujet qui se construit dans un récit avec ses fragments et ses zones d'ombre, ses parts de secret, au profit du sujet unifié d'un agent économique [11]. À ce titre, la défense de l'équilibre qui préserve la capacité d'agir individuelle, en particulier à travers la préservation de la séparation entre les contextes (étatique, professionnel, privé, intime ou médical), est une pièce maîtresse dont dépend l'autonomie de la personne.

La *privacy* est ainsi comprise non comme une simple dichotomie privé/public qui serait imposée *a priori*, mais comme le respect des normes propres à chaque contexte : les flux

d'informations doivent respecter les contextes d'usage, car chaque contexte relationnel possède ses propres normes, explicites ou non, qui correspondent aux attentes des usagers quant à la manière dont les informations vont circuler. Ces frontières ne sont pas fixées une fois pour toutes : elles peuvent être renégociées en fonction des situations, des acteurs et des technologies. Et lorsque ces normes dynamiques sont enfreintes, par exemple lorsque les données de géolocalisation d'un salarié pendant son week-end sont communiquées à son employeur, l'intégrité contextuelle est rompue : l'individu a alors le sentiment de subir une atteinte à sa vie privée. Mais cette vision ne se limite pas à la simple constatation de la nécessité de l'intégrité contextuelle. Elle procède également à une tentative de réévaluation du rôle de la *privacy*, tentative dont l'ambition est de saisir sa portée pour la vie sociale dans son ensemble : « La *privacy* en tant qu'intégrité contextuelle constitue une toile complexe et délicate de contraintes sur le flux d'informations personnelles qui lui-même donne un équilibre à de multiples sphères de vie sociale et politique [12]. » Pour autant, est-ce que le numérique qui rend de fait possible une forte porosité entre les contextes, permet encore de cultiver des zones d'opacité ? Surtout, le secret est-il réductible au contrôle des données personnelles ?

2. Le secret irréductible au contrôle

Pour donner une image globale des moyens par lesquels l'individu peut aujourd'hui être « mis au centre » des flux de données et avoir une certaine initiative dans leur circulation, nous introduisons ici la notion de paradigme de consentement et de contrôle. Ce paradigme est, selon nous, l'expression la plus générale à la fois des principes de droits relatifs aux identités numériques et des moyens techniques mis à disposition des individus.

Par « consentement », nous entendons non seulement le consentement en tant que tel, dans le sens restreint que le droit lui confère, mais aussi, en amont du traitement, la notification qui participe à l'idée d'un choix éclairé de la part de l'utilisateur. C'est le sens de l'expression *notice-and-consent*, notification-et-consentement. Nous y incluons également l'idée de la finalité du traitement telle qu'élaborée par le droit, dans la mesure où le consentement à telle ou telle finalité, supposée connue de l'utilisateur, est ici en jeu.

Par le contrôle, nous entendons la supposition théorique que les moyens effectifs de contrôle des flux des données, par exemple *via* la divulgation sélective des attributs, contribuent à redonner à l'individu l'initiative de sa propre construction. À titre d'exemple, il y a une nécessité de ce contrôle lorsque la collecte des informations personnelles est effectuée « à la source », comme c'est le cas dans les systèmes d'identité numérique régalienne dans différents États européens [13]. Mais le paradigme de consentement et de contrôle reste également en grande partie pertinent pour décrire le cas où les données qui n'ont pas été « filtrées » à la source (ou ne peuvent pas l'être en raison de leur caractère obligatoire), sont traitées et croisées dans les bases de données du côté des « responsables de traitement ». On suppose dans ce cas de figure que l'existence même des données concernant l'utilisateur lui est potentiellement connue, par exemple dans les cas de PNR (*Passenger Name Record*), l'ensemble des informations détenues par les compagnies aériennes et mises à disposition du gouvernement sur requête) ou encore de réseaux sociaux en général. Dans ce cas de figure, le contrôle peut être exercé au moyen d'accès à et de rectification des informations concernant l'utilisateur. Ce cas, de plus en plus fréquent, en appelle donc au renforcement des moyens de contrôle mis à disposition de l'utilisateur.

Cette tendance est confirmée par la mise en place du RGPD [14] et du droit au déréférencement. Il s'agit par ces mesures de mettre en place les conditions nécessaires pour l'exercice de consentement et de contrôle. Néanmoins, une difficulté réside dans l'articulation problématique entre la définition positive de la *privacy* et la mise en place des mécanismes de contrôle par l'individu. Aussi paradoxal que cela puisse paraître, la surdétermination du domaine du privé peut aussi conduire au renforcement de la surveillance et du contrôle de l'individu. Illustrons cette idée par deux exemples.

Un premier exemple s'appuie sur le fait que l'octroi de contrôle apparent sur les données personnelles à l'individu ne conduit pas nécessairement à l'autonomie pleine de celui-ci. Le contrôle n'est pas une valeur effective qui serait simplement capable de donner plus d'autonomie à l'individu, mais aussi une valeur prescriptive, qui indique ce que celui-ci doit faire. En réalité, plus le domaine du contrôlable – de manière illusoire ou non – par le sujet est circonscrit positivement, plus les actions de ce dernier sont elles-mêmes sujets de visibilité et

de contrôle. Ici, l'essentiel n'est pas simplement dans le soupçon permanent dont notre société porte l'empreinte, et dans laquelle l'individu n'est envisagé que sous deux aspects : consommateur ou délinquant [15]. Ce qui est beaucoup plus important à nos yeux, c'est la démarche même de devoir réguler ce qui doit ou ne doit pas être contrôlable par le sujet, démarche qui *de facto* définit le domaine de ce que le sujet est en mesure ou pas de considérer comme sien, comme relevant de sa vie privée. Par la régulation du champ du contrôlable par le sujet, c'est le possible et son horizon de sens, en accord avec la caractérisation foucaldienne des sociétés néolibérales, qui se trouvent définis de manière positive.

Paradoxalement, pour laisser exister non pas le contrôle par l'utilisateur, mais un espace de jeu dans lequel la subjectivité puisse advenir, pour contrer à la fois cette légifération « envahissante [16] » et cette exhaustivité mémorielle, il faut maintenir, contre la fluidité contemporaine, ce que July E. Cohen nomme « la discontinuité sémantique [17] ». La discontinuité sémantique fait ici référence, non seulement à la séparation entre les « contextes », mais plus fondamentalement à la nécessité des espaces de non-détermination, à la non-superposition des territoires existentiels. La discontinuité sémantique est l'opposé de l'absence de frontières (*seamlessness*) : « elle est une fonction de la complexité interstitielle à l'intérieur des cadres institutionnels et techniques qui définissent les droits d'information et les obligations, et établissent des protocoles pour la collecte, le stockage, le traitement et l'échange d'informations. La complexité interstitielle imprègne le tissu de notre existence quotidienne et analogue, où son importance est le plus souvent inaperçue et sous-estimée. Pourtant sa fonction est vitale. Elle crée de l'espace pour l'indétermination sémantique qui est vitale et indispensable en ce qu'elle rend possible le jeu des pratiques quotidiennes [18]. »

Nous évoquerons ici trois volets de cette « fluidité » (*seamlessness*) qui portent la trace de l'ambiguïté contemporaine : l'interaction fluide depuis longtemps thématisée dans le domaine scientifique de l'interaction homme-machine et dont *Apple* par exemple est le porte-parole industriel ; le phénomène de convergence qui se joue au niveau de l'architecture des réseaux ; et la légifération croissante sur les échanges des données. Pour ce troisième volet, on notera, entre autres exemples, l'ambiguïté intrinsèque du débat sur la portabilité des données, en France et en Europe : à l'endroit même où on se donne pour ambition d'octroyer plus de

contrôle à l'utilisateur au moyen des formats généraux, on ouvre également la porte à la faisabilité technique de l'échange de ces mêmes données par d'autres acteurs, de manière de plus en plus fluide et ce en dehors de tout contrôle. On commence alors à percevoir en quoi les technologies numériques, et les discours qui les accompagnent, ont tendance à niveler la discontinuité sémantique.

Le deuxième exemple concerne la manière dont le discours sur les technologies de contrôle influence la perception de celles-ci, et comment un certain discours sur la protection des libertés individuelles comporte le risque de se rendre, de manière paradoxale, complice du contrôle du sujet. Dans ce domaine, l'exemple le plus parlant est sans doute celui de la biométrie et de ses évolutions récentes. Il a longtemps été d'usage de distinguer, comme l'a fait la CNIL par exemple jusqu'en 2016, entre la famille des techniques biométriques à traces d'un côté, et la famille des techniques biométriques sans traces et intermédiaires de l'autre. Selon cette distinction, les empreintes digitales relèvent de la biométrie à traces dans la mesure où le doigt laisse des traces dans l'environnement physique, et ce sont ces traces qui peuvent être prélevées et traitées à des fins d'identification. Cette technique laisse en particulier la porte ouverte à des détournements et « demeure risquée en termes d'usurpation d'identité », ce qui a conduit la CNIL à l'encadrer de manière assez rigoureuse. Les techniques de la deuxième famille, c'est-à-dire sans traces (typiquement le réseau veineux des doigts) et intermédiaires (l'iris, la forme du visage) sont alors considérées comme moins sujettes à caution, car le risque évoqué ci-dessus est considéré comme moins élevé. À ce titre, cette seconde famille pourrait être vue comme plus neutre à l'égard de la *privacy*, plus « protectrice » de l'individu.

Selon nous, une telle interprétation comportait déjà, avant 2016, une ambiguïté fondamentale. Dans le passage de la première famille (biométrie à traces) à la seconde famille, deux choses semblaient se jouer. Tout d'abord, on rentre de plus en plus à l'intérieur du corps, tout en donnant, par l'absence de contact, l'impression d'invasion moindre. C'est le motif de la fluidité et de l'interaction ergonomique qui l'emporte. Mais c'est l'intériorité même du corps qui se trouve ainsi scrutée de plus en plus à des fins d'identification qui se fait désormais non pas à la frontière entre le monde et mon corps, mais à l'intérieur de celui-ci. Ensuite, sous

couvert de l'argument de la protection, l'identification est en réalité de plus en plus sûre et techniquement infaillible. En effet, si l'on peut encore échapper à l'identification par empreintes digitales en se brûlant les doigts, pratique attestée parmi les demandeurs d'asile [19], il devient plus difficile d'imaginer une stratégie similaire dans le cas de l'identification par l'iris, à moins de procéder à une surenchère des mutilations. Ainsi, le discours protecteur s'accommode paradoxalement de cette progression simultanée vers l'intérieur du corps et vers l'infaillibilité de l'identification.

Cette distinction entre biométrie sans traces et à traces a été abandonnée par la CNIL en 2016. Les deux nouvelles familles remplacent désormais l'ancienne distinction. Dans la première famille (1), le gabarit biométrique, quel qu'il soit, est stocké sur un serveur centralisé (dit « en base »), elle bénéficie donc de vigilance accrue de la part de la CNIL. Dans la seconde famille, soit (2a), l'accès au gabarit « en base » est protégé par un « secret » (typiquement un code secret associé à une architecture PKI) que seul l'utilisateur connaît, soit (2b), le gabarit est stocké et vérifié localement sur la carte d'identité que seul l'utilisateur détient par exemple (dit *match-on-card*). Cette famille (2) est moins sujette à caution pour la CNIL. Il est certain que cette deuxième famille est préférable du point de vue de non-divulgation et de non-centralisation des données biométriques. Mais le paradoxe nous semble sensiblement le même qu'avec la distinction en vigueur avant 2016 : sous couvert de l'argument de la protection, les conséquences des nouvelles procédures sont en réalité de plus en plus problématiques. En effet, dans le cas où l'utilisateur perd ou divulgue le code de la carte (2a), qui va être tenu pour responsable de l'accès potentiel au gabarit stocké sur le serveur ? La révocation de cet accès et les enjeux adjacents sont-ils de même nature que la perte du code d'une simple carte bancaire ? Y aura-t-il une assurance spécifique comme pour les moyens de paiement, en individualisant encore plus le risque ? Dans le cas (2b), le problème n'est-il pas amplifié d'une certaine manière ? Car c'est à l'utilisateur qu'incombe désormais la responsabilité d'avoir toujours sur soi, de porter en permanence une annexe numérique qui valide le statut de son corps comme identifié – et de finir par considérer cette carte (2b) comme réellement « privée » au même titre que son corps. À défaut, il pourrait être considéré sans identité, ne plus avoir accès à tel ou tel service, ou encore être sommé de prouver qu'il n'a pas commis de faute afin que son identité soit « rétablie ».

La famille (2) est qualifiée par la CNIL de « dispositifs biométriques permettant aux personnes de garder la maîtrise de leur gabarit biométrique ». Certes, la maîtrise va toujours de pair avec une responsabilité plus grande. Mais la « maîtrise » imposée, y compris imposée pour des raisons de protection, va toujours de pair avec la surdétermination du domaine du privé et avec un coût potentiel plus grand – et ce coût est ici clairement supporté par l'utilisateur. La *privacy* devient dès lors une simple injonction à « bien utiliser » la biométrie par exemple – et donc à l'utiliser quand même. Ainsi, voit-on bien l'ambiguïté fondamentale de ces technologies : plus on avance dans la définition du domaine du privé et de ce qui doit être protégé, y compris au moyen des discours protecteurs, plus ce domaine devient délimitable de manière positive, et plus il offre de prises à des stratégies de pouvoir (qu'elles soient d'ordre politique ou industriel). Comme l'écrivent à cet égard Gilles Deleuze et Félix Guattari : « Il y aura toujours une perception plus fine que la vôtre, une perception de votre imperceptible, de ce qu'il y a dans votre boîte [20] ». Il y aura toujours quelqu'un pour percevoir secrètement le secret.

Conclusion

Si les sociétés hypermodernes produisent des sujets qui se préoccupent de leur vie privée, en les incitant à intégrer une certaine culture du secret, ces sujets ne le font bien souvent finalement que de manière assez conformiste. Or, comme l'explique Sam Coll, envisager la surveillance uniquement en tant que menace pour la vie privée est potentiellement nocif. Cela peut aussi la renforcer. La vie privée et la surveillance ne sont paradoxalement pas antagonistes : « Au contraire, elles semblent travailler conjointement dans le déploiement de la société de surveillance. Plus on parle de la vie privée, plus les consommateurs se concentrent sur leur individualité, [...] ce qui les forme en tant que sujets de contrôle [21]. » Un tel état de fait conduit assez naturellement à un certain affaiblissement du sens du secret, le limitant à une expérience qui serait uniquement protectrice ou limitative. Pour ces raisons, et afin de dépasser une telle conception de l'expérience du secret, d'autres ressorts conceptuels sont à trouver. Le concept de « territoire existentiel », introduit par le psychanalyste Félix Guattari [22] nous paraît à même de répondre à cet effort de penser l'humain, en assumant pleinement la complexité ainsi que les ambiguïtés qui le définissent. La multiplicité des

territoires existentiels dans lesquels le sujet se meut correspond à une multiplicité des sens ou des cadres de référence. Le concept du « territoire existentiel » enrichit à bien des égards l'interprétation des phénomènes contemporains. Cela essentiellement parce que la notion de territoire implique celle d'un espace, d'un terrain de jeu, d'un parcours, d'une démarche dont le sujet peut être à l'origine. On souligne ainsi l'idée qu'un sujet n'est pas simplement soumis à la multiplication des horizons de sens, mais qu'il s'affirme avant tout dans un rapport actif à leur constitution. Enfin, les territoires peuvent se superposer, en faisant participer le sujet à des territoires différents, de manière simultanée ou successive. Toute la question est alors de savoir si le sujet est à l'origine de cette superposition ou bien s'il en subit les conséquences. Or si notre époque s'organise autour de mots d'ordre qui accompagnent de nouvelles formes d'asservissement, la manière dont nous nous saisissons du numérique devrait pouvoir créer les conditions de possibilité d'une réinvention permanente de soi, dans un rapport au secret qui puisse demeurer lui-même irréductible, et se réinventer sans cesse.

NOTES

1. De la Boétie, Étienne, *Discours de la servitude volontaire*, Translation en français moderne par Myriam Marrache-Gouraud, Notes réalisées par Myriam Marrache-Gouraud et Anne Dalsuet, Paris, Éditions Gallimard, 2008.

2. Voir à ce sujet : Zuboff, Shoshana, *L'Âge du capitalisme de surveillance*, Traduit de l'anglais par Bee Formentelli et Anne-Sylvie Homassel, Éditions Zulma, 2020.

3. Burgess, Peter, « Je ne suis pas la somme de mes données personnelle », *The Conversation*, 18 avril 2018 : https://theconversation.com/je-ne-suis-pas-la-somme-de-mes-donnees-personnelles-95082

4. Derrida, Jacques, *De l'hospitalité. Anne Dufourmantelle invite Jacques Derrida à répondre*, Paris, Éditions Calmann-Lévy, 1997, p. 61.

5. L'utilisation de certains termes, en particulier aux États-Unis, tel que *Homeland Security*, n'est pas sans signifier que les pires périodes de l'histoire contemporaine peuvent, au moins sémantiquement, resurgir. Cf. Harvey, Robert, « Un monde sous contrôle. Retour sur l'USA Patriot Act », *in* Chardel, Pierre-

Antoine & Rockhill, Gabriel (dir.) *Technologies de contrôle dans la mondialisation : enjeux politiques, éthiques et esthétiques*, Paris, Éditions Kimé, 2009, p. 50-51.

6. Harvey, Robert, et Volat, Hélène, *USA Patriot Act. De l'exception à la règle*, Paris, Éditions Lignes & Manifestes, 2006, p. 119. Voir également, Pierre-Antoine Chardel, Robert Harvey & Hélène Volat, « Un USA PATRIOT Act à la française ? ou les inquiétantes résonances d'une loi », *in* Revue *Lignes*, n° 48, octobre 2015, p. 105 -124 ; Rada Ivekovic, « Terror/isme comme politique ou comme hétérogénéité. Du sens des mots et de leur traduction », *in* Revue *Rue Descartes*, n° 62, 2008, p. 68-77.

7. Nous renvoyons sur cette question à Breton, Philippe, *Le Culte de l'Internet. Une menace pour le lien social ?*, Paris, Éditions de La Découverte, 2000 ; ainsi qu'à Chardel, Pierre-Antoine, *L'Empire du signal. De l'écrit aux écrans*, Paris, CNRS Éditions, 2020.

8. Derrida, Jacques, *Force de loi. Le fondement mystique de l'autorité*, Paris, Éditions Galilée, 1994, p. 107.

9. Derrida, Jacques, *De l'hospitalité. Anne Dufourmantelle invite Jacques Derrida à répondre*, *op.cit.*, p. 65.

10. Voir à cet égard : Simmel, Georg, *Secret et sociétés secrètes*, traduit de l'allemand par Sybille Muller. Postface de Patrick Watier, Éditions Circé, 1996.

11. Nous nous appuyons, ici et dans les pages qui suivent, sur des éléments développés dans l'ouvrage : Khatchatourov, Armen, *Les Identités numériques en tension : entre autonomie et contrôle*, avec la collaboration de Pierre-Antoine Chardel, Andrew Fenneberg et Gabriel Périès, ISTE Éditions, 2019.

12. Nissenbaum, Helen, *Privacy in Context: Technology, Policy and the Integrity of Social Life*, Stanford University Press, Palo Alto, 2010.

13. Le cas d'Alicem en France est, à cet égard, aussi emblématique qu'ambigu sur le plan éthico-politique : https://www.interieur.gouv.fr/fr/Actualites/L-actu-du-Ministere/Alicem-la-premiere-solution-d-identite-numerique-regalienne-securisee

14. RGPD : https://www.economie.gouv.fr/entreprises/reglement-general-sur-protection-des-donnees-rgpd

15. Merzeau, Louise, « Présence numérique : les médiations de l'identité », *in Les Enjeux de l'information et de la communication*, vol. 1, 2009 : https://www.cairn.info/revue-les-enjeux-de-l-information-et-de-la-communication-2009-1-page-79.htm#

16. Mengue, Philippe, « Comment la multitude peut-elle échapper au contrôle ? », *in* Pierre-Antoine Chardel & Gabriel Rockhill (dir.), *Technologies de contrôle dans la mondialisation : enjeux politiques, éthiques et esthétiques,* Paris, Éditions Kimé, 2009, p. 133-148.

17. Cohen, July E., *Configuring the Networked Self : Law, Code, and the Play of Everyday Practice,* New Haven, Yale University Press, 2012.

18. *Ibid.*

19. Manach, Jean-Marc, « Les "doigts brûlés" de Calais, *Le Monde Diplomatique,* 2009 : https://www.monde-diplomatique.fr/carnet/2009-09-25-Calais

20. Deleuze, Gilles et Guattari, Félix, *Capitalisme et Schizophrénie 2. Milles Plateaux,* Paris, Les Éditions de Minuit, 1980, p. 351.

21. Coll, Sam, « Power, knowledge, and the subjects of privacy : understanding privacy as the ally of surveillance », *in Information, Communication & Society,* Volume 17, 2014 - Issue10,2014 : https://www.tandfonline.com/doi/abs/10.1080/1369118X.2014.918636?journalCode=rics20

22. Guattari, Félix, *Chaosmose,* Paris, Éditions Galilée, 1992.