Éthique publique

Revue internationale d’éthique sociétale et gouvernementale

vol. 14, n° 2 | 2012 :
Quelques enjeux éthiques du numérique
Les personnes et la sécurité à l'ère numérique : quelle éthique ?

L’éthique à l’épreuve des nouvelles particularités et fonctions des informations personnelles[1]

JESSICA EYNARD

Résumés

FrançaisEnglish
Au fil du temps, les données personnelles semblent avoir changé de nature. Désormais, elles saisissent des éléments intrinsèques de la personne. Or, en même temps, elles paraissent échapper à la maîtrise de l’individu, et ce, à deux égards. Premièrement, la personne ne parvient pas à les appréhender intellectuellement. Deuxièmement, elle semble être dans l’impossibilité de les protéger juridiquement. Cette situation aboutit à une utilisation étendue et moins contrôlée des informations, utilisation dont le but est d’anticiper les besoins et comportements de l’individu. Ce dernier est enfermé dans un profil qui ne peut lui correspondre parfaitement, mais sur la base duquel sont pourtant prises des décisions à son égard. Un nouveau modèle se construit, automatisé et systématisé, dans lequel la personne est objectivée et réduite à un amas d’informations. L’éthique n’est alors plus vecteur d’équilibre et se fragilise au fur et à mesure de l’appréhension des informations personnelles.

The meaning of the term “personal data” seems to have changed over time. Indeed, it now includes information related to people’s physical and psychological characteristics. At the same time, the people concerned by the data do not seem to have any intellectual or legal control over it. This leads to widespread, uncontrolled use of information for the purpose of anticipating people’s needs and behaviour. People are thus trapped in a profile that does not necessarily correspond to them but that serves as a basis for making decisions in their regard. A new automated and systematized model is being built, in which people are reduced to a set of data. Ethics is no longer helping to offset

this trend and its role is gradually decreasing with the continued collection and use of personal information.

Entrées d'index

Mots-clés : méconnaissance de l'information, droits de la personnalité, profilage, information predictive, personne objectivée

Texte intégral

1 « Il n'y a point d'assujettissement si parfait que celui qui garde l'apparence de la liberté on captive ainsi la volonté même » (Rousseau, 1824 : 210). Selon Rousseau, la personne désireuse d'avoir un contrôle efficace sur les âmes doit imposer ses idées et ses volontés en toute discrétion. L'individu sous contrôle doit avoir l'impression d'agir et de penser de façon autonome. Il doit croire que les idées viennent de lui et qu'il agit librement. Cette croyance de liberté anéantit toute méfiance ou tout jugement critique. Ses pensées, faits et gestes lui sont en réalité dictés sans qu'il s'en aperçoive, et ce, grâce à une connaissance approfondie de sa personnalité et de ses comportements. Insidieusement, il se retrouve à n'être qu'une marionnette et c'est alors à sa qualité d'être humain doué de discernement, de conscience et de libre arbitre qu'il est porté atteinte.

2 Ce pouvoir, qui était épisodique au moment où Rousseau écrivait ces lignes puisque seuls les éducateurs avaient le pouvoir de manipuler les enfants, ne l'est plus avec l'avènement des nouvelles technologies qui, en multipliant les moyens de captation des informations, a permis d'affiner la connaissance que l'on peut avoir d'une personne et accentué la possibilité de contrôler cette dernière. Le réseau Internet, les puces identifiant par radiofréquence, les systèmes de géolocalisation ou encore les techniques biométriques ont abouti à ce que l'on ne se contente plus de collecter les noms, prénoms, adresses, numéros de téléphone, etc. on s'intéresse désormais aux empreintes digitales, au patrimoine génétique, aux données de connexion ou encore aux goûts. De même, on ne se satisfait plus des informations livrées volontairement et consciemment par l'individu, on préfère celles livrées à son insu, moins propices aux mensonges. Progressivement, des bases de données gigantesques sont mises en œuvre, qui permettent de faire émerger des données sur l'individu. Rien n'est ensuite plus facile que d'utiliser ces connaissances contre lui ou d'en tirer profit.

3 À cet égard, l'inquiétude sur la réalité de certaines valeurs éthiques est légitime. L'éthique peut être définie comme « un mode de régulation des comportements qui provient de l'individu et qui met l'accent sur des valeurs co-construites et partagées pour donner un sens à ses décisions et à ses actions, faisant ainsi appel à son jugement personnel et à sa responsabilité » (Boisvert *et al.,* 2003 : 31). L'éthique vise donc à réfléchir à son comportement et à l'adapter en fonction de valeurs que l'on juge essentielles. Dès lors, « s'il y a obéissance à la règle, c'est parce que celle-ci ou les comportements qu'elle exige actualisent une ou plusieurs valeurs qui sont jugées importantes par l'agent » (Bégin, 2011 : 44). Elle s'éloigne en cela du droit, dont les règles s'imposent par peur de la sanction en cas de violation.

4 Or, lorsqu'une personne collecte les informations personnelles d'un individu en vue de surveiller les faits et gestes de ce dernier, d'exercer un contrôle sur lui

et de le pousser à agir selon ses propres intérêts, elle ne viole pas les règles de droit édictées par des lois consacrées à la protection des données personnelles. L'éthique, en revanche, aurait dû, semble-t-il, la conduire à ne pas utiliser les informations personnelles à l'insu de l'individu et, surtout, contre son intérêt.

5 Ainsi, il apparaît que le développement des technologies a eu pour effet non seulement la multiplication du nombre d'informations personnelles captables, mais encore et surtout la modification de la nature des informations captables. Là où auparavant la personne conservait une maîtrise sur les données qui la concernaient, elle ne les comprend désormais plus et ne peut les protéger (I). Il s'ensuit une utilisation libre des données par les tiers qui se traduit par une méconnaissance de valeurs essentielles (II).

I) La perte de maîtrise de la personne sur les informations la concernant

6 Avant l'explosion des technologies, la collecte des informations personnelles concernait essentiellement l'état civil ainsi que les éléments de la vie privée et de la vie publique. Aujourd'hui sont recueillis l'information génétique, la composition des tubes de l'iris, les empreintes digitales, les moindres faits, gestes et attitudes, c'est-à-dire des données relatives à la physiologie et à la personnalité de l'individu. On est ainsi passé de la collecte de données qui sont la caractérisation de fractions de vie de la personne qui agit sur la scène sociétale, à la collecte de données qui sont la transcription d'éléments essentiels de l'être humain. À cet égard, une différence de nature paraît affecter les données anciennement et nouvellement captables. À la différence des premières, les secondes appréhendent les éléments constitutifs de la personne, ceux qui font d'elle un être humain. Ce faisant, la personne se retrouve mise à nue et les tiers collecteurs parviennent à lire en elle comme dans un livre ouvert sans qu'elle ait besoin de parler.

7 Petit à petit, les informations personnelles se dispersent. Les individus, étant « contraints [...] à nouer des rapports avec autrui [...], le font dans une position dépendante qui rejette dans un monde conceptuel désincarné la maîtrise reconnue à chacun sur les données qui lui sont propres » (Rigaux, 1990 : 603). La maîtrise suppose en effet l'exercice d'un contrôle moral et matériel sur les données (*Trésor de la langue française*). Or, lorsque l'on considère les informations captables avant le développement des technologies, on s'aperçoit que l'individu exerçait un pouvoir sur les données. Non seulement les connaissait-il et les comprenait-il, mais il les utilisait et savait les protéger. Les éléments de son identité, à savoir ses nom, prénom, sexe, nationalité, lui donnaient un statut qui lui permettait de se situer dans le temps et l'espace et de se positionner sur la scène du droit. Dès qu'on portait atteinte à sa vie privée, il était capable de s'en rendre compte et d'actionner les auteurs devant les tribunaux. De sa naissance jusqu'à sa mort, il maîtrisait l'information qui lui était personnelle. À l'inverse, le rapport entre la personne et les données nouvellement captables se distend aujourd'hui. La personne semble en effet totalement incapable d'appréhender les informations qui pourtant la concernent, telles que son patrimoine génétique, ses empreintes digitales ou le numéro de la puce Rfid contenu dans son passeport. En général, elle sait que la

donnée existe. Quelquefois, elle peut même s'en servir. Il lui suffit de positionner son index sur un lecteur pour accéder à un lieu par exemple. Pourtant, elle n'a pas connaissance de l'information. Ainsi, même si elle voyait son empreinte digitale dévoilée dans un magazine, elle ne s'en émouvrait pas, car elle ne la reconnaîtrait pas. Une différence essentielle apparaît donc avec les éléments de la vie privée et l'identité : les nouvelles informations échappent à la connaissance de celui qu'elles concernent. Est-il dès lors possible de soutenir que ce dernier est capable de les protéger ? Les tiers collecteurs n'en arrivent-ils pas à avoir une libre disposition des informations ? À cet égard se pose la question de savoir si l'absence de maîtrise intellectuelle (A) n'aboutit pas à une absence de maîtrise juridique (B).

A – l'absence de maîtrise intellectuelle

8 La maîtrise suppose la connaissance. Lorsque l'on dit de quelqu'un qu'il maîtrise une technique, on signifie qu'il a une connaissance parfaite du savoir-faire qu'il met en œuvre. Pour maîtriser une donnée, il faut donc nécessairement la connaître.

9 Cette connaissance est manifestement absente lorsque l'on considère certaines informations nouvellement captables, telles que l'information génétique, le positionnement des tubes composant son iris ou encore la forme tridimensionnelle de sa main. Pour d'autres informations, cette connaissance semble exister. Ainsi, quand il navigue sur Internet, l'individu sait quel site il visite, sur quel lien il clique et la durée approximative de sa connexion. Il paraît donc capable d'appréhender ces informations. Ce qui, en revanche, lui échappe, c'est que chacun de ses clics ou le simple fait d'allumer son ordinateur ou d'ouvrir une page Web se transforme en information. À cet égard, l'absence de maîtrise intellectuelle de la personne sur les données captables grâce au développement des technologies peut avoir deux sources : soit l'ignorance pure et simple de l'information, soit l'ignorance de la création de l'information.

10 Dans le premier cas, la personne peut avoir conscience que la donnée existe, mais elle n'en maîtrise pas le contenu. Aujourd'hui en effet, « quasiment tout, dans l'anatomie ou le comportement d'un individu, peut être transformé en un code informatique permettant de l'identifier » (Cabal, 2003 : 14). Cette évolution doit être notée, car elle aboutit à ce que la personne ne soit plus capable de comprendre l'information qui la concerne. Le circuit de la donnée est en outre transformé. Auparavant, l'information émanait de la personne et parvenait au tiers collecteur sans qu'il soit nécessaire de procéder à aucune opération. Aujourd'hui, l'information provient toujours de la personne, et ce, bien qu'elle ne la connaisse pas, et parvient toujours entre les mains du tiers collecteur mais, entre-temps, la forme de l'information a été modifiée par un « tiers technologique » (Dubouis, 2004 : 98). Ainsi, par exemple, l'empreinte digitale reste issue de la personne et est utilisée par des tiers tels que l'État ou les entreprises privées pour sécuriser les titres d'identité ou encore réguler l'accès à des lieux spécifiques. Entre ces deux acteurs pourtant, l'empreinte est transformée en gabarit, c'est-à-dire en suite numérique, grâce aux techniques informatiques. Ce faisant, elle devient incompréhensible pour la personne qu'elle concerne et seul celui qui maîtrise l'outil technique peut donner un sens à la donnée.

11 Dans le second cas, la personne peut connaître l'objet de l'information, mais ne pas avoir conscience que celui-ci est devenu une information captable par

les tiers. Il peut par exemple savoir qu'il est gourmand, mais ne pas imaginer que le magasin dans lequel il fait ses courses connaît ce trait de personnalité grâce à l'analyse des produits de son chariot. Ce qui lui échappe ici, c'est la formalisation de son trait en information (Catala, 1984 : 97). Les traces numériques, définies comme « [l']enregistrement de toutes les actions d'un individu sous forme de données informatisées » (Perriault, 2009 : 13), sont particulièrement représentatives de cette situation. Elles traduisent chaque fait et geste en information sans que la personne qui agit en ait conscience. Dès qu'elle allume son ordinateur ou se connecte sur Internet, la personne livre par exemple automatiquement et systématiquement de multiples données sur elle sans en être informée et sans pouvoir avoir le moindre contrôle sérieux sur les informations qui y sont traitées (Dinant, 1999 : 227). Hors de la Toile, le même phénomène est visible grâce aux systèmes de géolocalisation ou aux puces identifiant par radiofréquence par exemple. La personne devient ainsi un acteur que de multiples tiers épient à son insu, inconscient des informations qui sont captées et étudiées. Les valeurs éthiques s'estompent alors quand la personne n'est plus considérée comme un être humain doté de droits et de conscience, mais comme un objet de surveillance et d'étude. Seule la possibilité laissée à la personne de protéger juridiquement les données qui la concernent pourrait contrer cette déshumanisation. Il faut dès lors s'interroger pour savoir si l'absence de maîtrise intellectuelle sur les données n'entraîne pas une absence de maîtrise juridique.

B – l'absence de maîtrise juridique

12 En vertu des divers textes visant à protéger les informations personnelles, la personne est titulaire d'un droit d'accès aux informations qui la concernent, d'un droit de communication, d'un droit de rectification, d'un droit à l'oubli ainsi que d'un droit d'opposition. Ce pouvoir de l'individu sur les informations qui lui sont relatives ne peut juridiquement se traduire en droit français qu'en un droit subjectif, c'est-à-dire en un pouvoir reconnu par le droit objectif en vertu duquel la personne peut, pour protéger un droit privatif, exiger la cessation d'un agissement ou la réalisation d'une prestation.

13 Parmi les droits subjectifs se trouvent notamment le droit de propriété et les droits de la personnalité. Admettre la qualification de droit de la propriété pour qualifier le lien entre la personne et les données qui la concernent pose incontestablement problème, car cela aboutit à admettre la possibilité d'une disposition totale des informations. Or, si l'individu peut bien négocier l'utilisation des données qui le concernent, il ne peut en revanche s'en défaire complètement et irrévocablement. Elles lui restent toujours attachées. La démarche qui consiste à admettre l'appropriation des données « instaure une faculté pour l'homme de "disposer" de l'information le concernant quand seule la "jouissance" de cette information est véritablement en jeu » (Mallet-Poujol, 1997 : 334). Aussi, il faut abandonner la qualification de droit de propriété pour se tourner vers celle de droit de la personnalité.

14 Quant à la catégorie des droits de la personnalité, elle est née de la nécessité de donner à l'individu le pouvoir de « protéger les intérêts moraux [...] attachés à la sauvegarde de ce qui fait ou exprime sa personnalité » (Loiseau, 1997 : 328). L'information personnelle, en ce qu'elle traduit des éléments de la vie ou des aspects biologiques ou psychologiques du sujet, semble de prime abord devoir être appréhendée comme l'objet d'un tel droit. En ce sens, le pouvoir

permettant à la personne de protéger les informations qui la concernent devrait s'analyser en droit français en un droit de la personnalité. Cette thèse n'est néanmoins valable que si ce pouvoir respecte les caractéristiques propres à ce type de droit. Or, il ne peut y avoir droit de la personnalité que lorsque l'individu peut se réserver l'information ou rétablir la vérité sur sa situation s'agissant du droit de réponse. Ainsi, le droit s'appliquant à la vie privée peut s'analyser comme un droit de la personnalité, car il permet par principe à l'individu de retenir la donnée. Cependant, ce droit ne semble pas toujours pouvoir s'appliquer s'agissant des informations personnelles. Aucune atteinte au droit à la vie privée ne paraît par exemple être commise lorsque sont utilisées les empreintes digitales, la trace Internet ou l'adresse IP. Pour ces données rendues captables au fur et à mesure des avancées technologiques, seul le droit d'opposition contenu dans les différents textes de protection des données peut permettre de retenir l'information. Ce droit permet effectivement à son titulaire de s'opposer à ce que des informations le concernant fassent l'objet d'un traitement. L'exercice de ce droit est cependant soumis à l'existence de motifs légitimes. La donnée se révèle donc par principe disponible et par exception réservée. Cette disponibilité de l'information personnelle empêche de considérer que l'individu détient un droit de la personnalité sur la donnée qu'il porte. Son pouvoir ne peut dès lors s'analyser qu'en un droit subjectif *sui generis,* dont la dimension protectrice est moindre que celle des droits de la personnalité. Cet affaiblissement du pouvoir juridique associé à la perte de maîtrise intellectuelle de l'individu sur les données aboutit à une utilisation étendue et moins contrôlée des informations. Cette situation conduit à la mise en œuvre de traitements de données sans commune mesure, dont l'objectif est d'anticiper les faits, gestes et besoins de l'individu. Or, le fait de prévoir le comportement d'une personne et d'utiliser cette connaissance à son propre profit n'est-il pas le signe d'une atteinte à des valeurs éthiques ?

II) L'éthique face à la libre utilisation des informations

15 La possibilité d'anticiper les comportements individuels grâce aux procédés techniques repose sur une logique simple : l'être humain étant un être rationnel, il est probable qu'il agisse de la même façon dès lors qu'il se trouve dans deux situations strictement identiques. Il suffit donc de l'observer pour pouvoir prévoir ses réactions. Or, plus on l'observe, plus on collecte d'informations sur lui et plus il devient facile de le rendre prévisible et d'anticiper, voire de susciter, ses réactions. Dans ce cadre, les informations personnelles deviennent la clé permettant d'orienter ses choix en fonction d'un profil établi informatiquement.

16 Le profilage est

> une méthode informatisée ayant recours à des procédés de *datamining* sur des entrepôts de données permettant ou devant permettre de classer avec une certaine probabilité et donc avec un certain taux d'erreur induit un individu dans une catégorie particulière afin de prendre des décisions individuelles à son égard (Dinant *et al.,* 2008 : 5).

17 Il se décompose en deux étapes. La première consiste à amasser une grande quantité d'informations et à créer un « entrepôt de données » ou *data*

warehouse la seconde, à établir le profil individuel. Selon Lee Andrew Bygrave, ce profil s'établit en deux temps.

18 Premièrement, il faut analyser les « données personnelles à la recherche de modèles et de liens afin de parvenir à un ensemble d'hypothèses (le profil) basées sur des calculs de probabilité » (Bygrave, 2001 : 17. Je traduis). L'auteur vise ici la méthode du *data mining* qui recouvre « l'ensemble des techniques qui, de façon automatique et exhaustive, permettent d'explorer et de remonter à la surface des relations complexes à partir d'un gros volume de données » (Moxton, cité dans Omarjee, 2002 : 11 *sqq*.). En pratique, le *data mining* met en œuvre des algorithmes pour faire émerger de nouvelles informations grâce à l'analyse d'une quantité importante de données. Relativement à la personne, le *data mining* a pour objet de catégoriser cette dernière dans des profils comportementaux obtenus grâce à l'observation de nombreux individus, lesquels profils permettent d'anticiper avec une certaine marge d'erreur ses réactions dans telle ou telle situation. Dans ce contexte, la personne étudiée se retrouve dotée d'une *data shadow* (Bygrave, 2001 : 4) qui, se rapprochant au plus près de ce qu'elle est, fait état de ses goûts, de ses envies, de ses traits de caractère, de ses comportements, de sa psychologie...

19 Une fois le profil créé, il faut l'utiliser « pour aider à rechercher, et/ou à prendre une décision, concernant une personne ou une entité » (Bygrave, 2001 : 4). Il s'agit ici de tirer profit du profil obtenu pour adapter son comportement, ses choix, ses stratégies à ce profil. On ne s'intéresse pas ici à une réaction générale d'un segment de population, on cherche à influencer un comportement individuel en adoptant une attitude ou une stratégie spécifique. Par exemple, l'agence de voyages en ligne qui désire vendre un séjour à destination de l'île de la Réunion va moduler son discours en fonction des goûts des internautes décelés grâce à la méthode du *data mining*. Ainsi, pour certains en quête de détente, elle a tout intérêt à vanter les plaisirs de la plage mais, à d'autres en quête d'aventure, elle doit focaliser sa promotion sur les randonnées au cœur des cirques montagneux et les paysages inoubliables vus à ces occasions. Le *data mining* lui permet donc de faire varier son discours pour l'adapter au mieux aux désirs de ses clients et ainsi vendre le séjour à un maximum d'entre eux. Elle peut ainsi ajuster ses réactions et décisions à chaque individu pour maximiser les chances d'atteindre le but fixé en amont – dans l'exemple cité, la vente du séjour à l'île de la Réunion. La difficulté qui naît de cette pratique provient de l'enfermement de la personne dans des cases prédéfinies, lesquelles ne reflètent pas exactement sa personnalité et qui conditionnent pourtant le discours qui va lui être dicté. Ainsi, l'internaute que l'informatique aura profilé comme étant en quête de détente ne se verra proposer que des séjours en bord de mer, sans grande activité physique. Il ne sera pas informé de la possibilité de faire des randonnées, de dormir en refuge ou d'accéder au sommet du Piton de la Fournaise. Pourtant, l'être humain a pour caractéristique d'évoluer et ce n'est pas parce qu'à un moment M, il désire se détendre, qu'à un moment M+1, il ne voudra pas se dépenser. Le profilage a donc pour effet d'enfermer les personnes dans des modèles dont il leur est difficile de sortir alors même que ces modèles ne leur correspondent jamais parfaitement, car ils ne sont qu'un reflet basé sur leurs habitudes individuelles. Ils nient l'essence même de la personne en la réduisant à une catégorie obtenue grâce à l'utilisation de procédés statistiques, informatiques et mathématiques sans tenir compte de son libre arbitre et de sa possibilité de changer et d'évoluer. Ce constat aurait naturellement dû conduire les tiers collecteurs à ne pas recourir à de tels profils. L'éthique aurait en effet dû servir de mode de

régulation du comportement de ces tiers, si on part du principe que le respect de la personne humaine est nécessairement une valeur essentielle. L'éthique se révèle ainsi insuffisante pour empêcher l'objectivation de la personne permise par le profilage et le droit, qui aurait pu prendre son relais, apparaît aujourd'hui comme un outil de mise en œuvre des mécanismes de profilage.

20 En effet, de nombreux textes légaux se font l'écho de cette tendance à vouloir anticiper les comportements individuels. En matière sécuritaire notamment, les politiques pénales tendent à cibler les potentiels délinquants le plus tôt possible. Les travaux préparatifs à la loi française sur la prévention de la délinquance[2] énonçaient ainsi que « [s]i les actions de prévention veulent être efficaces, elles doivent impérativement commencer dès les prémicesde déviances, c'est-à-dire dès le plus jeune âge » (Bénisti, 2004 : 8), et préconisaient d'expérimenter une action « auprès des enfants qui présentent un comportement prédicteur de délinquance dès la crèche, la maternelle ou l'école primaire » (Syndicat des commissaires et hauts fonctionnaires de la police nationale, 2005 : 5). Un enfant en maternelle qui se bagarre, mord, donne des coups de pieds, refuse d'obéir, remue sans cesse, n'attend pas son tour (Inserm, 2005 : 381), etc., se trouve alors stigmatisé comme futur délinquant sur la base d'un profil comportemental établi statistiquement. Le risque d'exclusion est ici grand.

21 L'utilisation des *Passenger Name Record* (PNR) est également symptomatique de cette volonté d'anticiper les comportements déviants. Il s'agit purement et simplement de corréler les informations contenues dans les dossiers des passagers aériens dans le but de prévenir des comportements terroristes. Sur la base de données telles que le nom du voyageur, son contact à destination, son itinéraire ou sa volonté d'avoir un repas sans porc, des profils à risque sont constitués qui permettent de surveiller ou d'arrêter préventivement des suspects potentiels dès leur arrivée sur le sol américain ou européen. De simples voyageurs sont de cette façon enserrés dans une catégorie qui conduit à des décisions défavorables à leur égard, mais dont il leur est très difficile de sortir. Un processus systématique de catégorisation est ainsi mis en œuvre, qui nie la propension de tout être humain à agir différemment des autres dans une même situation.

22 Cette tendance à la prédiction s'étend au-delà de la sphère sécuritaire pour contaminer de nombreux domaines. Le secteur bancaire utilise ainsi la technique du « score », « dont la finalité est l'appréciation du risque de crédit par des moyens automatisés, [et qui] a pour résultat la constitution d'un profil de l'emprunteur par chaque organisme » (CNIL, 1988). Le monde du travail cherche aujourd'hui à évaluer l'état de fatigue, de stress ou encore de déterminer quel type d'émotions est ressenti par le candidat ou l'employé. Sur le fondement de ces informations, des décisions relatives à la carrière de ce dernier sont prises.

23 Quant au secteur marchand, il se révèle profiler à outrance et pose des difficultés particulières en témoignent les documents officiels qui lui sont consacrés[3]. Sa spécificité est de ne pas se référer systématiquement à l'identité des personnes dont il utilise les informations. La question s'est donc posée de savoir si ces informations pouvaient être qualifiées de données à caractère personnel au sens de la directive 95/46/CE du 24 octobre 1995 (Parlement européen et Conseil de l'Union européenne, 1995 : 31) et donc, si les règles protectrices découlant de ce texte devaient s'appliquer. En effet, la directive définit la donnée à caractère personnel comme « toute information concernant une personne physique identifiée ou identifiable » (Art. 2 a) de la directive du

24 octobre 1995). Or, si la notion d'identification se réfère à l'identité, l'ignorance de cette identité conduit à ce que la personne ne soit pas identifiée. Si les éléments recueillis ne permettent pas d'aboutir indirectement à l'identité, la personne n'est en outre pas identifiable, de sorte que les informations collectées ne peuvent être qualifiées de données personnelles et, *a fortiori,* que le régime protecteur instauré par la directive communautaire ne peut être appliqué. La résolution de ce problème réside en définitive dans la définition des notions d'identification et d'« identifiabilité ». Il s'agit ici de déterminer si la connaissance de l'identité ou la simple possibilité de connaître l'identité de la personne dont les données sont collectées est inhérente à l'identification ou « identifiabilité ». Simplement, faut-il obligatoirement pouvoir connaître l'identité civile de la personne pour considérer qu'elle est identifiée ou identifiable ? Pour le Groupe de l'article 29,

> si l'identification par le nom constitue, dans la pratique, le moyen le plus répandu, un nom n'est pas toujours nécessaire pour identifier une personne, notamment lorsque d'autres « identifiants » sont utilisées pour distinguer quelqu'un. [...] Sur l'internet aussi, les outils de surveillance du trafic permettent de cerner facilement le comportement d'une machine et, derrière celle-ci, de son utilisateur. [...] Sans même s'enquérir de son nom et de l'adresse de la personne, on peut la caractériser en fonction de critères socio-économiques, psychologiques, philosophiques ou autres et lui attribuer certaines décisions dans la mesure où le point de contact de la personne (l'ordinateur) ne nécessite plus nécessairement la révélation de son identité au sens étroit du terme. En d'autres termes, la possibilité d'identifier une personne n'implique plus nécessairement la faculté de connaître son identité[4](G29, 2007 : 15).

24 Dès lors, il faut considérer qu'il y a identification à partir du moment où la personne est individualisée, et ce, quel que soit l'élément pris en compte pour y parvenir, identité ou autre identifiant. Or, dans le cadre du profilage utilisé par le secteur marchand, de nombreuses informations sont imputées à un profil particulier via une carte de fidélité ou une adresse IP. Ces informations méritent de revêtir la qualification de données personnelles et, de ce fait, d'être protégées, car elles s'appliquent à la personne profilée qui, sans que son identité soit connue, est individualisée comme celle détentrice de la carte de fidélité ou de l'adresse IP. Aujourd'hui, le secteur marchand va plus loin que le simple profilage puisqu'il tend à s'en remettre au neuromarketing, c'est-à-dire à

> l'étude des processus mentaux, explicites et implicites, et des comportements du consommateur, dans divers contextes marketing concernant aussi bien des activités d'évaluation, de prise de décision, de mémorisation ou deconsommation, qui se réclame des paradigmes et des connaissances des neurosciences cognitives et affectives (Droulers et Roullet, 2006 : 7).

25 Le but ici est de stimuler la partie du cerveau décisionnaire qui conduit à l'achat. Sans que l'individu le sache, sa liberté individuelle et son libre choix sont inexistants. Là encore, l'éthique se révèle insuffisante pour discipliner les comportements et le droit inutilisé pour prendre son relais.

26 En définitive, il faut constater que l'évolution des techniques a conduit à remettre en cause l'équilibre existant entre la protection et l'utilisation des informations personnelles et, corrélativement, à porter atteinte à certains droits et libertés fondamentaux. La protection qui devrait être assurée par la

personne concernée par les données est paralysée, soit que la personne ne comprend pas la donnée, soit qu'elle n'est pas détentrice d'un droit capable d'assurer une protection effective de la donnée. Cette absence de maîtrise sur les informations par la personne censée les protéger a conduit à une utilisation accrue de ces dernières, jusqu'à aboutir à la création de « personne virtuelle » (Bourcier, 2001 : 847), copie quasi conforme de la personne réelle. Cette dernière est par là même totalement objectivée et réduite à un amas d'informations, amas sur la base duquel sont prises des décisions affectant la personne et faisant fi de sa complexité, sa spontanéité, sa faculté de se remettre en cause et d'évoluer, sa capacité à réfléchir et à adapter son comportement, son libre arbitre. Dans ce cadre, l'éthique, en tant qu'elle constitue un mode de régulation des comportements basé sur le respect de valeurs que l'on juge essentielles, aurait dû empêcher cette objectivation de l'être humain et apporter un cadre à l'utilisation des données. Chaque collecteur aurait dû, de lui-même, restreindre son recueil de données pour ne pas porter atteinte aux valeurs que sont la liberté, l'autodétermination et le respect de l'être humain. Pourtant, l'éthique a peu à peu fondu comme une peau de chagrin, en même temps que les nouvelles technologies et les préoccupations sécuritaires, économiques, etc., permettaient et justifiaient une appréhension plus grande des informations personnelles. Seul le droit semble aujourd'hui capable de venir prendre le relais de l'éthique et d'imposer des règles permettant d'encadrer l'utilisation démesurée des données et les conséquences qui en découlent. Pourtant, au regard des textes récemment adoptés, il est légitime de s'interroger sur la réelle volonté d'un législateur, désireux d'anticiper les comportements déviants et pour ce faire, d'amasser et de corréler des masses d'informations, d'édicter de pareilles règles.

Bibliographie

BÉGIN, Luc (2011), « Légiférer en matière d'éthique : le difficile équilibre entre éthique et déontologie », *Éthique publique,* vol. 13, nº 1, p. 34-61. [En ligne], [http://ethiquepublique.revues.org/361] (25 octobre 2012).
DOI : 10.4000/ethiquepublique.361

BÉNISTI, Jacques Alain (2004), « Rapport préliminaire de la Commission prévention du groupe d'études parlementaire sur la sécurité intérieure », *Centre d'initiative et de réflexion pour la défense des libertés Lyon,* [En ligne], [http://cirdel.lyon.free.fr/IMG/pdf/rapport_BENISTI_prevention.pdf] (28 octobre 2012).

BOISVERT, Yves,*et al.* (2003), *Raisonnement éthique dans un contexte de marge de manœuvre accrue : clarification conceptuelle et aide à la décision. Rapport de recherche*,Québec, Secrétariat du Conseil du trésor, Gouvernement du Québec, Centre d'expertise en gestion des ressources humaines.

BOURCIER, Danièle (2001), « De l'intelligence artificielle à la personne virtuelle : émergence d'une entité juridique ? », *Droit & Société,* nº 49, p. 847-871.

BYGRAVE, Andrew (2001), « Minding the machine : article 15 of the EC data protection directive and automated profiling », *Computer Law & Security Report,* vol. 17, p. 17-24.

CABAL, Christian (2003), Rapport nº 938 sur « Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre », déposé à la Présidence de l'Assemblée nationale le 16 juin 2003, annexé à la séance du Sénat du 12 juin 2003 sous le numéro 355.

CATALA, Pierre (1984), « Ébauche d'une théorie juridique de l'information », *Dalloz,* chron., p. 97 *sqq*.

CNIL [COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS] (1988), « Délibération nº 88-083 du 5 juillet 1988 portant adoption d'une recommandation

relative à la gestion des crédits ou des prêts consentis à des personnes physiques par les établissements de crédit », *CNIL,* [En ligne], [http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/28/] (28 octobre 2012).

CNIL [COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS] (2009), *La publicité ciblée en ligne*, 5 février, [En ligne], [http:// www.cnil.fr/fileadmin/documents/La_CNIL/actualite/Publicite_Ciblee_rapport_VD.pdf]

DINANT, Jean-Marc (1999), « Les traitements invisibles sur Internet », *Cahiers du CRID,* nº 16, Bruylant, p. 227 *sqq*.

DINANT, Jean-Marc,*et al.,* L'application de la Convention 108 au mécanisme du profilage. Éléments de réflexion destinés au travail futur du Comité consultatif (T-PD), T-PD-BUR (2008) 01, 11 janvier 2008, [En ligne], [http://www.coe. int/t/dghl/standardsetting/dataprotection/Reports/ CRID_Profilage_2008_fr.pdf].

DROULERS, Olivier, et Bernard ROULLET (2006), « Neuromarketing : cadre théorique et perspectives », *Neuromarketing.be,* Actes du XXIIe Congrès AFM, Nantes, 11 et 12 mai, [En ligne], [http://www.akoustic-arts.fr/wp-content/uploads/Neuromarketing.pdf] (28 octobre 2012).

DUBOUIS, Louis (2004), « Rapport de synthèse du colloque de l'Association française du droit de la santé portant sur "Le droit des données de santé" », *Revue générale de droit médical,* numéro spécial, p. 98 *sqq*.

EYNARD, Jessica (2011), « Essai sur la donnée à caractère personnel ». Thèse de doctorat, Toulouse, Université de Toulouse 1 Capitole.

G29 [GROUPE DE TRAVAIL « ARTICLE 29 »] (2007), « Avis 4/2007, sur le concept de données à caractère personnel », 20 juin, WP 136, [En ligne], [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fr.pdf] (28 octobre 2012).

G29 [GROUPE DE TRAVAIL « ARTICLE 29 »] (2010), « Avis 2/2010 sur la publicité comportementale en ligne », *Commission européenne,* 22 juin, WP171, [En ligne], [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/ wp171_fr.pdf] (28 octobre 2012).

INSERM (2005), *Expertise collective,* Éditions Inserm.

LOISEAU, Grégoire (1997), « Des droits patrimoniaux de la personnalité en droit français », *McGill Law Journal,* vol. XLII, p. 328.

MALLET-POUJOL, Nathalie (1997), « Appropriation de l'information : l'éternelle chimère », *Dalloz,* Chron., p. 330 *sqq*.

OMARJEE, Sulliman (2002), « Le data mining : aspects juridiques de l'intelligence artificielle au regard de la protection des données personnelles ». Mémoire de maîtrise, Montpellier, Université Montpellier I.

PARLEMENT EUROPÉEN et CONSEIL DE L'UNION EUROPÉENNE (1995), « Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la circulation de ces données », Journal officiel des Communautés européennes, 23 novembre, [En ligne], [http:eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX: 31995L0046:FR:NOT] (28 octobre 2012).

PERRIAULT, Jacques (2009), « Traces numériques personnelles, incertitude et lien social », *Hermès,* « Traçabilité et réseaux », nº 53, p. 13 *sqq*.
DOI : 10.4267/2042/31537

POULLET, Yves, et Jean-Marc DINANT (2004), « Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications. L'autodétermination informationnelle à l'ère de l'Internet. Éléments de réflexion sur la Convention nº 108 destinés au travail futur du Comité consultatif (T-PD) », *Conseil de l'Europe,* 18 novembre, [En ligne], [http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Poullet_report_2004_fr.pdf] (28 octobre 2012).

RIGAUX, François (1990), *La protection de la vie privée et des autres biens de la personnalité,* Bruxelles, Établissements Émile Bruylant. (Coll. « Bibliothèque de la faculté de droit de l'Université catholique de Louvain ».)

ROUSSEAU, Jean-Jacques (1824), *Émile,* livre second.

SYNDICAT DES COMMISSAIRES ET HAUTS FONCTIONNAIRES DE LA POLICE NATIONALE (2005), *La sécurité au quotidien,* octobre.

Notes

1 Sur ce point, voir Eynard (2011).

2 Loi n° 2007-297 relative à la prévention de la délinquance, 5 mars 2007, JO n° 56 du 7 mars 2007, p. 4297 *sqq*.

3 Voir par exemple, CNIL (2009) et G29 (2010).

4 Cet avis reprend le « Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications » de Poullet et Dinant (2004).

Pour citer cet article

Référence électronique
Jessica Eynard, « L'éthique à l'épreuve des nouvelles particularités et fonctions des informations personnelles », *Éthique publique* [En ligne], vol. 14, n° 2 | 2012, mis en ligne le 23 août 2013, consulté le 20 août 2019. URL : http://journals.openedition.org/ethiquepublique/1017 ; DOI : 10.4000/ethiquepublique.1017

Auteur

Jessica Eynard

Jessica Eynard est docteure en droit privé. Elle a réalisé sa thèse, intitulée « Essai sur la donnée à caractère personnel », sous la direction de la professeure Claire Neirinck, et l'a soutenue en septembre 2011 à l'Université de Toulouse 1 Capitole. Pour ce travail, elle a obtenu le prix de thèse « Informatique et Libertés » décerné par la Commission nationale de l'informatique et des libertés (CNIL) en 2012. Elle a également réalisé un mémoire, se proposant de déterminer quelles étaient les limites de la CNIL. Outre la problématique « informatique et libertés », elle s'intéresse notamment au droit des personnes et de la famille. Elle est ainsi membre du Comité de rédaction des Cahiers de jurisprudence d'Aquitaine et Midi-Pyrénées. Dans ce cadre, elle rédige la rubrique « Rapports familiaux – Obligations alimentaires » et coécrit la rubrique « Mariage – Divorce ».

Droits d'auteur