

Cet article est paru initialement dans la Revue Lamy Droit de l'Immatériel, n° 116, juin 2015, Analyse, pp. 41-44.

Pour citer cet article : *Fabrice Mattatia, Morgane Yaïche, "Être propriétaire de ses données personnelles (2^{ème} partie) : peut-on envisager un régime spécifique ?", Revue Lamy Droit de l'Immatériel, 2015/116 ; pp. 41-44.*

DR Fabrice Mattatia, Morgane Yaïche

ÊTRE PROPRIÉTAIRE DE SES DONNÉES PERSONNELLES (2^{EME} PARTIE) : PEUT-ON ENVISAGER UN RÉGIME SPÉCIFIQUE ?

Auteurs :

Fabrice MATTATIA, ingénieur en chef des mines, docteur en droit, chargé d'enseignement à l'université Paris I Panthéon-Sorbonne

Morgane YAÏCHE, diplômée du master 2 Droit du Numérique – Administration – Entreprise de l'université Paris I Panthéon-Sorbonne

L'instauration d'un droit de propriété des individus sur leurs données personnelles constitue un débat d'actualité¹. « Chacun doit être considéré comme propriétaire de sa vie et de ce qu'il fait », propose ainsi Jacques Attali². « Il suffirait de mettre en perspective les risques avec le droit, en reconnaissant un droit de propriété des individus sur leurs données personnelles », suggère M^e Alain Bensoussan³. « Ceux qui pensent être propriétaires de nos données se trompent », rétorque la présidente de la CNIL, Isabelle Falque-Pierrotin⁴. La CNIL, le Conseil d'Etat, le Conseil national du numérique, se sont également exprimés sur le sujet.

Rappelons que les données à caractère personnel sont définies par la loi 78-17 du 6 janvier 1978 modifiée comme toute information relative à une personne physique identifiée ou identifiable. Dans notre vie quotidienne, cela recouvre aussi bien l'identité, l'adresse, le numéro de téléphone, que des photos, la liste de nos contacts mails ou téléphoniques, notre géolocalisation, nos habitudes de consommation ou de navigation web, nos opinions, notre état de santé... La création d'un droit de propriété vise à la fois à raffermir le contrôle de l'individu sur des informations qui lui sont propres et qui ne devraient pas être utilisées sans son consentement, et à lui assurer une part équitable de la valorisation de ces données.

Mais au-delà du débat sur l'opportunité politique ou économique d'instaurer une propriété des données personnelles, la question se pose de la faisabilité pratique d'un tel droit. Que signifie être propriétaire d'une donnée personnelle ? Quels sont les droits qui en découlent ? Dans un précédent article publié dans ces colonnes, nous avons vu que les régimes traditionnels de propriété, au sens du Code civil ou au sens du Code de la propriété

¹ Pr Judith Rochfeld, « Questions actuelles sur la commercialisation des données à caractère personnel », Table ronde, *Cahiers de droit de l'entreprise*, mai-juin 2012, n° 3, p. 9-17.

² Jacques Attali, « Être propriétaire de soi », *lexpress.fr*, 18 février 2013, <http://blogs.lexpress.fr/attali/2013/02/18/etre-propretaire-de-soi>.

³ M^e Alain Bensoussan, « La propriété des données », *lefigaro.fr*, 18 mai 2010, <http://blog.lefigaro.fr/bensoussan/2010/05/la-proprieete-des-donnees.html>.

⁴ Jacques Henno, interview d'Isabelle Falque-Pierrotin, "Ceux qui pensent être propriétaires de nos données se trompent", *Les Echos*, 25 novembre 2014, www.lesechos.fr/idees-debats/sciences-prospective/0203937716964-isabelle-falque-pierrotin-ceux-qui-pensent-etre-propreitaires-de-nos-donnees-se-trompent-1067857.php.

intellectuelle, ne sont pas adaptés au cas particulier des données personnelles. Dans le présent article, nous recensons les enjeux auxquels devrait répondre un régime *ad hoc* (I), ainsi que les difficultés que poserait sa mise en œuvre (II).

I – ENJEUX INHERENTS A LA MISE EN PLACE D’UN REGIME DE PROPRIETE SPECIFIQUE

1. Des enjeux financiers importants

Si l’objectif consiste à rendre possible un commerce des données personnelles, il est tout d’abord nécessaire d’évaluer leur valeur. Or les méthodes d’évaluation de la valeur des données personnelles restent floues aujourd’hui, même si la valeur boursière des entreprises traitant ces données nous donne des indices. Ainsi, l’entreprise Facebook est valorisée 200 milliards de dollars pour un milliard d’utilisateurs, ce qui représente 200 dollars par utilisateur. Mais Facebook concentre énormément d’informations intimes sur ses membres, ce qui explique sa valeur. Plus modestement, quand l’entreprise Virgin a fait faillite en France en 2013, le fichier clients contenant un million d’adresses mail a été vendu pour 54 000€.

Une étude de 2012 du Boston Consulting Group (BCG) estime que la valeur créée pour les organisations et pour les citoyens par l’exploitation des données personnelles représentera 1000 milliards d’euros par an en Europe d’ici 2020⁵. La valeur des données personnelles prend donc une ampleur de plus en plus importante dans le cadre de la croissance mondiale et la tentation d’un marché de ces données devient plus forte.

Cette même étude du BCG recherche les critères d’évaluation financière des données personnelles, et démontre que les consommateurs et les entreprises ont un point de vue différent. Pour les consommateurs, la valeur de leurs données personnelles apparaît immatérielle : le BCG la définit comme le surplus de valeur que reçoivent les consommateurs grâce au développement de nouveaux services qui leur permettent, soit de gagner du temps (services numériques dans le secteur public par exemple), soit de profiter d’un service gratuit (ex : réseaux sociaux), ou même d’économiser sur leurs impôts (ex : économies du gouvernement grâce à la numérisation des données). Pour les entreprises il s’agit plutôt d’une valeur réelle (un gain de chiffre d’affaires), mais aussi des économies réalisées⁶.

L’idée d’instaurer une taxe spécifique sur l’exploitation des données personnelles a été étudiée par le rapport Colin et Collin sur la fiscalité du numérique de 2013 : cette taxe sur les données personnelles, qui sont « *la matière première dont l’économie numérique se*

⁵ Boston Consulting Group, *The Value of our Digital Identity*, 2012, pp. 3-4 : « *All told, the value created through digital identity can be massive – at a 22% annual growth rate, applying personal data can deliver a €330 billion annual economic benefit for organizations in Europe by 2020. Individuals will benefit to an even greater degree, as the consumer value will be more than twice as large: €670 billion by 2020.* ».

⁶ Boston Consulting Group, *The Value of our Digital Identity*, 2012 - Chiffres clés et méthodologie.

nourrit », viserait à renforcer l'économie numérique Elle permettrait notamment d'« accroître la protection des libertés individuelles sur Internet, au travers d'une réappropriation, par les internautes, de leurs données personnelles »⁷. Cependant, cette idée a reçu un avis défavorable du Conseil national du numérique, qui considère que cette taxe spécifique pose des objectifs qui « sont difficilement atteignables et parfois complexes à appréhender »⁸. Mais si on rend possible le fait de commercialiser ses données pose également la question de leur taxation dans le droit commun : faudrait-il soumettre les données personnelles à la TVA ou bien à l'impôt sur le revenu ?

2. Des enjeux juridiques à prendre en compte

Vendre ses données personnelles signifie conclure un contrat. A ce titre, le consentement a une place primordiale dans la marchandisation des données personnelles. Le terme de consentement n'est pas à prendre ici dans le sens défini par l'article 7 de la loi Informatique et Libertés⁹, mais tel que prévu par le Code civil dans le droit des contrats, et plus particulièrement, pour ce qui relève du numérique, par l'article 1316-4 du Code civil qui dispose¹⁰ :

« La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.

Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat. »

Certes, lorsque le boulanger nous vend une baguette, il y a entre le vendeur et l'acheteur contrat et consentement, mais ceux-ci sont tacites. Pourquoi faudrait-il alors exiger un formalisme plus lourd pour la vente de données personnelles ? Sans doute parce que ces données touchent de bien plus près à l'intime qu'une simple baguette de pain, et que le fait de les céder n'est pas anodin : toute la présente polémique trouve son origine dans la volonté de donner à l'individu un meilleur contrôle de la divulgation et de la monétisation de ses données. Ce contrôle, s'il se veut réel, exige de manière évidente un consentement exprès à chaque transaction.

En pratique, cela nécessite malheureusement un arsenal assez lourd. En effet, il faut d'abord s'assurer de l'identité de la personne qui vend ses données personnelles, et de sa capacité à le faire (exclure les cas de minorité, de tutelle...). Il faut ensuite disposer d'un outil de signature permettant à la personne de manifester son consentement et garantissant l'intégrité du document signé. Sans même aller jusqu'à l'usage de dispositifs présumés

⁷ Nicolas Colin, Pierre Collin, *Mission d'expertise sur la fiscalité de l'économie numérique*, janvier 2013, disponible en ligne sur le site du Ministère de l'Économie, p. 142-143

⁸ Rapport du Conseil national du numérique, *Concertation sur la fiscalité du numérique*, septembre 2013, p. 23

⁹ « Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée [...] »

¹⁰ A compter du 1^{er} juillet 2016, ces dispositions seront remplacées par celles issues du règlement européen 910-2014, mais cela n'impacte en rien notre raisonnement.

fiables, sans doute disproportionné ici, le recours à ces outils représente un coût non négligeable, et nécessite une solennisation de l'acte de signature peu compatible avec la fluidité de la navigation web. Même si cet arsenal technique était déployé, il est toutefois peu réaliste d'espérer obtenir comme résultat un consentement exprès, éclairé et indubitable : on sait que les internautes acceptent les conditions générales d'utilisation sans les lire. Des chercheurs de l'éditeur britannique F-Secure ont ainsi inséré dans des conditions d'utilisation la mention « *en utilisant ce service, vous acceptez de céder votre premier né à l'entreprise F-Secure, lorsque celle-ci le demandera et selon les conditions fixées par elle. Si vous ne produisez aucun enfant, l'entreprise saisira en lieu et place votre animal de compagnie préféré. Les termes de cet accord sont valables pour l'éternité.* » - et de nombreux internautes ont cliqué¹¹.

Une fois des obligations mises en place pour garantir le consentement, des sanctions devront réprimer le non-respect de celles-ci. Les cas de dol ou d'escroquerie, pour extorquer un consentement, sont à envisager. Certains acteurs peu scrupuleux pourront également vouloir profiter de la méconnaissance par les individus de la valeur réelle des données cédées. Il y a aussi le cas des consentements extorqués pour pouvoir accéder à un contenu ou à un service, le prestataire abusant du rapport de force en sa faveur. Inversement, sanctionnera-t-on les personnes vendant sciemment des données fausses ?

On peut s'interroger sur le cas des données dites « sensibles », listées à l'article 8 de la loi Informatique et libertés : données concernant la santé, les opinions religieuses, politiques ou syndicales, l'origine ethnique, ou la vie sexuelle de la personne. Ces données seront-elles autorisées à la vente, ou, comme c'est le cas actuellement, leur traitement sera-t-il interdit ? Si un encadrement du commerce de ces données est décidé, comment le mettre en œuvre concrètement, sachant d'une part que la majorité du public n'est pas sensibilisée à la protection particulière à leur accorder (les internautes les affichent avec insouciance sur les réseaux sociaux), et d'autre part que la détermination de leur qualité de donnée sensible n'est pas aisée. Pensons par exemple à la prolifération des objets communicants dédiés au suivi de la pratique sportive, qui enregistrent le pouls, la pression artérielle, etc. : prises isolément ces données sont neutres, mais à partir de quel point leur accumulation constitue-t-elle une information sur la santé de l'individu ?

Par ailleurs, se pose la question de la modification à apporter aux actuels droits de rectification et de mise à jour des données reconnus aujourd'hui aux personnes concernées. Actuellement il s'agit de dispositions d'ordre public (l'individu ne peut pas renoncer à son droit de rectification et de mise à jour, tout au plus peut-il s'abstenir de l'exercer), car elles ont été pensées pour protéger la personne concernée. Mais en cas d'instauration d'un régime de propriété des données personnelles, comment ces droits s'articuleront-ils avec une cession ? L'individu aura-t-il toujours le droit de faire rectifier une donnée qu'il aura vendue (adresse, donnée de santé, etc.) ? En allant plus loin, l'individu aura-t-il l'obligation de tenir à jour les données vendues, dans le cadre d'une garantie d'exactitude ? Pourra-t-on l'attaquer pour tromperie sur la marchandise si une donnée se révèle erronée ou périmée ?

¹¹ M^e Etienne Wery, *Du Wifi gratuit contre un bébé*, www.droit-technologie.org/actuality/details.asp?id=1685, 21 décembre 2014.

En outre, il faudra trouver un équilibre entre le droit à une exploitation paisible et pérenne des données personnelles par leur acquéreur, et le droit à l'oubli consacré en 2014 par la Cour de justice de l'Union européenne¹². On sait que ce droit à l'oubli n'est pas absolu, et qu'il doit déjà être concilié notamment avec le droit à l'information, quand ce n'est pas avec l'intérêt légitime du responsable de traitement ou avec des obligations légales. Peut-être faudra-t-il que la personne concernée s'engage à ne pas faire jouer son droit à l'oubli ou son droit d'opposition sur des données vendues— engagement qui serait actuellement illégal face à des dispositions une fois de plus d'ordre public. Peut-être une solution consisterait-elle à définir un régime *ad hoc*, non pas de vente des données personnelles, mais de licence d'exploitation sur un périmètre bien délimité ?

Il est enfin nécessaire de s'interroger sur les sanctions qui seraient applicables en cas de mauvaise exécution de ces obligations. Se pose également la question de la détermination du juge compétent en cas de litige. Aujourd'hui, il existe en France un parallélisme entre les juridictions pénales classiques et la CNIL, un même dossier concernant les données personnelles pouvant être examiné indifféremment par l'une ou par l'autre voie, et même par les deux à la fois¹³. Cette atteinte au vieux principe du droit romain *Non bis in idem* est encadrée par la loi¹⁴ (plafonnement du cumul des sanctions) et validée par le Conseil constitutionnel¹⁵. Faut-il conserver cette dualité et laisser à la CNIL le pouvoir de sanctionner les infractions commises à l'occasion de la vente de données personnelles ? Cela semble une option à recommander, la CNIL disposant d'une plus grande expertise que le juge pénal, à la fois pour investiguer et pour comprendre les implications des traitements de données personnelles.

II – LES DIFFICULTES LIEES A LA MISE EN PLACE D'UN TEL REGIME

1. Des objections nombreuses

Rendre l'individu propriétaire de ses données dans la perspective de lui permettre d'en faire commerce bute sur une difficulté fondamentale qui réside dans la dyssymétrie d'information entre le vendeur et l'acheteur. En effet, l'acheteur sait parfaitement le revenu qu'il pourra retirer d'une information et donc la valeur que celle-ci a pour lui. En revanche, le vendeur n'a aucune idée de la valeur de ce qu'on lui demande de céder, et ce d'autant moins que la valeur d'une information diffère selon les acheteurs potentiels et les usages qu'ils en feront, et également selon qu'elle est isolée ou recoupée par d'autres : par exemple, le fait qu'on soit à un endroit donné à un moment donné vaut moins que le fait de savoir, par comparaison avec nos habitudes, si cette localisation est habituelle ou au contraire surprenante.

¹² CJUE, communiqué de presse n°70/14, Luxembourg, le 13 mai 2014, dans l'affaire C-131/12, Google Spain SL, Google Inc., / *Agencia Española de Protección de Datos*, Mario Costeja González.

¹³ Pour des développements sur ce thème, voir : Fabrice Mattatia, « CNIL et tribunaux : concurrence ou complémentarité dans la répression des infractions à la loi Informatique et Libertés ? », *Revue de science criminelle et de droit pénal comparé*, avril-juin 2009.

¹⁴ Article 47-2 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

¹⁵ Décisions 89-260 DC et 97-395 DC citées par le Conseil d'État, *Rapport public 2001, Les autorités administratives indépendantes*, p. 331.

La négociation sur le prix de cession (vente ou location) des données sera donc systématiquement déséquilibrée au profit des acheteurs. Cela est d'autant plus grave si la cession est définitive et permet au nouveau propriétaire d'exploiter à sa guise ces données et de les revendre à son tour : il y a risque de spoliation des individus.

Cette situation appellerait sans doute l'émergence de courtiers en données personnelles (par exemple Yesprofile¹⁶), mais ces nouveaux intermédiaires entre les individus et les acheteurs de données pourront eux aussi profiter de la désinformation des vendeurs pour capter une part de la valeur des données. Des sociétés de gestion collective sont envisageables, mais comme le souligne le Conseil d'Etat¹⁷, les frais de gestion de tels organismes seraient, en raison du coût de la répartition entre un nombre énorme d'ayants-droits, disproportionnés par rapport au caractère infime des sommes à recouvrer.

Une inégalité sociale risquerait également de se creuser, entre les individus motivés et capables de gérer leurs données et ceux qui ne le sont pas. En outre, « les plus pauvres pourraient être tentés de vendre leurs données, tandis que les données des plus riches seraient plus facilement préservées »¹⁸.

Dans sa contribution à l'étude 2014 du Conseil d'Etat sur les droits fondamentaux, Pierre Bellanger a par ailleurs souligné que loin de permettre une meilleure protection des droits des individus, l'instauration d'un droit de propriété des données personnelles la fragiliserait : isolé face à des prestataires web mondiaux, l'internaute vendra peu à peu ses droits au fil de ses navigations, pour le plus grand profit des multinationales numériques : « l'individualisation juridique des données conduit à atomiser un droit collectif potentiel en une somme de droits privés plus facilement solubles : clic d'acceptation par clic d'acceptation. Il n'est d'ailleurs pas étonnant que les entreprises du réseau les plus dataphages défendent séparément ou conjointement ces deux thèses [privatisation ou non-règlementation des données] : elles leur ouvrent grand les portes de la domination absolue ».¹⁹

2. La multiplication des prises de positions défavorables

La présidente de la CNIL, Isabelle Falque-Pierrotin, a confirmé cette tendance allant à l'encontre de la propriété des données, en la qualifiant de « fausse bonne idée » dans le rapport d'activité de la CNIL pour 2013 et en écrivant que bien qu'« *a priori* séduisante, cette démarche impose en réalité une grande prudence car la privatisation de ses données, et donc leur possible cession ou vente, revêt un caractère d'irréversibilité préoccupant pour l'individu. Les droits une fois vendus, comment reprendre la main sur ses données ? À l'inverse, le droit actuel de la protection des données personnelles ouvre des droits à l'individu même lorsque ses données sont produites et traitées par d'autres »²⁰.

¹⁶ www.yesprofile.com.

¹⁷ Conseil d'Etat, *Etude annuelle 2014 : Le numérique et les droits fondamentaux*, 2014, p. 266.

¹⁸ CNIL, *Cahiers Innovation et Prospective*, « Vie privée à l'horizon de 2020 », n°01, 2012, pp. 55-56.

¹⁹ Pierre Bellanger, *Principes et pratiques des données personnelles en réseau*, Contribution à l'étude 2014 du Conseil d'Etat : Technologies numériques et libertés et droits fondamentaux, 2014. La position de l'auteur a évolué par rapport à son ouvrage *La souveraineté numérique*, Stock, 2014.

²⁰ Commission Nationale de l'Informatique et des Libertés, *Rapport d'activité 2013*, 2014, p. 8.

La CNIL n'a pas été la seule à émettre des objections à l'éventuelle adoption de ce régime. Le Conseil national du numérique s'est également prononcé contre l'existence d'un droit de propriété sur les données personnelles. Dans son rapport sur la neutralité des plateformes, publié en mai 2014, le Conseil donne trois raisons pour exclure l'hypothèse de la propriété des données personnelles :

« La reconnaissance d'un droit de propriété sur les données personnelles aux individus est souvent avancée comme moyen de rééquilibrer les pouvoirs avec les entités collectrices.

Le Conseil invite à exclure cette option :

- Parce qu'elle renvoie à l'individu la responsabilité de gérer et protéger ses données, renforce l'individualisme et nie le rapport de force entre consommateurs et entreprises ;
- Parce qu'elle ne pourrait que générer des revenus anecdotiques pour les usagers et susciter à l'inverse un marché de la gestion protectrice des données numériques ;
- Parce qu'elle déboucherait à un renforcement des inégalités entre citoyens en capacité de gérer, protéger et monétiser leurs données et ceux qui, par manque de littératie, de temps, d'argent ou autre, abandonneraient ces fonctions au marché. »²¹

Enfin, dans son *Etude annuelle 2014* consacrée au numérique et aux droits fondamentaux, le Conseil d'Etat a lui aussi rejeté la piste d'un droit de propriété des données personnelles. Le Conseil estime notamment que cette solution est inapte à atteindre les objectifs recherchés et que le rééquilibrage de la relation entre internautes et éditeurs de service serait « largement illusoire ». En effet, d'un point de vue financier, chaque individu ne peut espérer gagner que quelques euros au maximum, et les éditeurs adapteront simplement leurs conditions d'utilisation pour les transformer en contrats de fourniture de service en échange de la cession des droits de propriété sur les données : « le rapport de force entre l'individu, consommateur isolé et l'entreprise, resterait marqué par un déséquilibre structurel »²². Le « droit de propriété » deviendrait ainsi un « droit d'être dépossédé »²³. Finalement, c'est le régime « personnaliste » actuel, reposant sur une logique de droits inaliénables rattachés à la personne, qui permet la meilleure protection des individus²⁴.

²¹ Conseil national du numérique, *Neutralité des Plateformes : réunir les conditions d'un environnement numérique ouvert et soutenable*, p. 37

²² Conseil d'Etat, *Etude annuelle 2014 : Le numérique et les droits fondamentaux*, 2014, p. 264-266.

²³ Nathalie Mallet-Poujol, citée dans CNIL, *Cahiers Innovation et Prospective*, « Vie privée à l'horizon de 2020 », n°01, 2012, pp. 55-56.

²⁴ Pr Judith Rochfeld, « Les données sont-elles des biens ? », Actes du colloque CEPRISCA, PUF, 2015.