Valeur des données personnelles et protection des droits fondamentaux

Alors que les données personnelles sont considérées comme des biens marchands aux États-Unis, l'Europe reste attachée à une conception extrapatrimoniale de celles-ci. En découle une législation méfiante et suspicieuse au nom de la protection des libertés et du droit à la vie privée. Mais ce choix est-il le plus efficace ?

Auteur
Ariane Noiville
Professeur agrégé, lycée Gaston-Berger, académie de Lille

La capitalisation boursière de la plateforme Facebook dépasse désormais 300 milliards de dollars. Elle a doublé en l'espace d'un an et demi (150 milliards en avril 2014) et triplé depuis son introduction en Bourse en mai 2012. Facebook occupe désormais la cinquième place des plus grosses valorisations du Nasdaq derrière Apple, Google, Microsoft et Amazon. Cette valeur trouve son origine dans le milliard d'utilisateurs qui, chaque jour, se connectent à la plateforme pour l'alimenter en données que celle-ci collecte, stocke et traite pour permettre la mise en relation des internautes du monde entier (un Terrien sur sept possède un compte Facebook).

Parallèlement, le 9 février dernier, la Commission nationale de l'informatique et des libertés (Cnil) a mis publiquement en demeure Facebook de se conformer, dans un délai de trois mois, à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dite « loi Informatique et Libertés », à la suite d'investigations menées par l'Autorité de protection ayant permis de relever de nombreux manquements à la législation française. Et il a été décidé de rendre publique cette mise en demeure, notamment en raison de la gravité des manquements constatés et du nombre de personnes concernées par le service Facebook (plus de 30 millions d'utilisateurs en France).

Ce nouvel avertissement est représentatif de la difficulté à concilier aujourd'hui la création de valeur résultant de l'exploitation de données dans le cadre de modèles dont l'utilité sociale et économique n'est pas contestée, et la protection des libertés fondamentales potentiellement menacées par l'ascendant économique des sociétés technologiques et par leur potentiel intrusif croissant. Car les données qui fondent la valeur de ces entreprises – et qui, à ce titre, peuvent être considérées comme

de véritables matières premières de l'économie numérique – sont des « données personnelles » ou « données à caractère personnel ». Il s'agit donc de chercher l'équilibre dans l'utilisation de ces données entre, d'une part, la création de valeur, l'innovation et le potentiel de croissance qu'elles recèlent et, d'autre part, la protection des droits fondamentaux des personnes.

Naissance de la protection des données personnelles

Depuis les années 1970, les États occidentaux ont pris conscience de la nécessité de protéger les données personnelles, compte tenu des risques que le développement des nouvelles technologies de l'information et de la communication faisait peser sur la vie privée. En France, l'encadrement des pratiques, faisant suite au rapport Tricot de juin 1975, s'est opéré par l'adoption de la loi Informatique et Libertés. Initialement, la loi visait le contrôle des fichiers publics, car seuls les États et quelques grandes entreprises disposaient des moyens suffisants pour réaliser ces traitements de masse. Ensuite, des acteurs privés ont également acquis cette possibilité. La loi a donc été plusieurs fois modifiée.

> Les données sont collectées pour des finalités déterminées, explicites et légitimes

Son article 2 définit la donnée personnelle : « Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. »

La Cnil a été amenée à préciser les contours de cette définition et notamment ce qu'il faut entendre par « personne physique identifiée, directement ou indirectement ». Selon la Cnil, une personne est identifiée lorsque, par exemple, son nom apparaît dans un fichier : « Une personne est identifiable, lorsqu'un fichier comporte des informations permettant indirectement son identification (ex. : adresse IP, nom, n° d'immatriculation, n° de téléphone, photographie, éléments biométriques tels que l'empreinte digitale, ADN, n° d'identification nationale étudiant), ensemble d'informations permettant de discriminer une personne au sein d'une population (certains fichiers statistiques) tels que, par exemple, le lieu de résidence, la profession, le sexe et l'âge. » La Cnil ajoute que « des données que vous pourriez considérer comme anonymes peuvent constituer des données à caractère personnel si elles permettent d'identifier indirectement ou par recoupement d'informations une personne précise. Il peut en effet s'agir d'informations qui ne sont pas associées au nom d'une personne mais qui permettent aisément de l'identifier et de connaître ses habitudes ou ses goûts (une empreinte digitale, l'ADN, une date de naissance associée à une commune de résidence…). »

Au niveau européen, la législation applicable résulte d'une série de directives. Le texte de référence est la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données, complétée, deux ans après son adoption, par une seconde directive s'appliquant au secteur des télécommunications (directive 97/66/CE) transposée dans l'ordre juridique interne par la loi de transposition du 6 août 2004 modifiant la loi du 6 janvier 1978. La directive 2002/58/CE du 12 juillet 2002 modifiée en 2006 concernant le traitement des données personnelles dans le secteur des communications électroniques accessibles au public a été transposée dans la loi pour la confiance dans l'économie numérique et dans l'article L 34-1 du Code des postes et des communications électroniques. Enfin, et afin d'accompagner l'ouverture du marché des télécommunications à la concurrence, l'Union européenne a adopté un cadre réglementaire relatif aux communications électroniques en phase avec les progrès technologiques et les exigences du marché et communément désigné comme le « Paquet Télécom » dont une directive transposée par ordonnance en 2011.

L'ensemble de ces textes européens et nationaux s'articulent autour de principes généraux : finalité, proportionnalité, loyauté, exactitude, sécurité, confidentialité, etc. Par application de ces principes, la loi prévoit de nombreuses obligations. Au moment de la collecte et pour la personne concernée, le droit d'obtention d'informations est prévu à l'article 32 de la loi. L'article 6 alinéa 2 dispose que les données « sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités ». La finalité du traitement est donc essentielle pour apprécier les conditions d'utilisation des données. Elle affecte aussi les conditions de conservation des données puisque le même article 6 alinéa 2 prévoit que seules des fins historiques, statistiques ou scientifiques justifient que les données puissent être conservées au-delà de la durée induite par la finalité du traitement (droit à l'oubli). Un traitement de données personnelles doit par ailleurs avoir reçu le consentement de

© Yoann Constantin

la personne concernée, sauf exceptions (article 7). Il existe également un droit d'opposition (article 38), un droit d'accès aux données (article 39), un droit de rectification (article 40), et des règles concernant les informations déjà stockées dans l'équipement terminal de l'utilisateur (« cookies »), aux termes de l'article 32 modifié par l'ordonnance de 2011.

L'explosion et la diversification des données dans le Big Data

Le droit s'est donc déjà beaucoup transformé face à l'explosion des données. Pourtant, la rapidité des innovations nécessite de repenser le régime juridique des droits fondamentaux. Les enjeux sont aujourd'hui très éloignés de ceux qui présidaient à la première vague de législation, dans les années 1970, alors que la circulation des données et leur valeur économique restaient limitées. Le contexte est marqué par l'essor transnational d'internet, la puissance de calcul des terminaux mobiles de toutes sortes et l'énorme valeur économique acquise par les données. En même temps qu'il ouvre de nouveaux espaces de libertés (d'expression, d'entreprendre…), le numérique constitue une nouvelle menace potentielle pour d'autres libertés (sécurité, sûreté, propriété intellectuelle, pratiques commerciales abusives, droit à la vie privée…). Il s'agit donc de chercher un équilibre entre la maîtrise de ces menaces et le potentiel de création de valeur du numérique, entre la sécurisation juridique des usages de données et un encadrement plus étroit des traitements les plus risqués. Ces nouveaux enjeux ont conduit la Commission européenne, en janvier 2012, à proposer une réforme globale des règles adoptées par l'Union européenne en 1995. L'objectif est double : renforcer et harmoniser les droits en matière de respect de la vie privée entre les États membres, tout en encourageant l'économie numérique européenne.

L'extrême diversité des données suppose au préalable un travail de classification.

Si l'on considère les données selon leur objet, il est possible – à l'instar de la classification proposée par Microsoft Advertising – d'identifier six types de données :

> données de démographie (âge, sexe, état civil, etc.) ;

> données liées aux activités et aux préférences (profil personnel, informations sur ce que l'on possède, historique d'achats, termes de recherche, sites visités, activité physique, préférences) ;

> données liées à l'organisation et aux déplacements (calendrier, emplacement via GPS), données liées à l'identité sociale (publications, photos, vidéos, listes d'amis/de contacts, etc.) ;

> données de communication (communications personnelles et professionnelles : e-mails, messageries

instantanées, SMS, bulletins d'informations, courrier, etc.) ;
> données issues d'informations personnelles (date de naissance, revenus, numéro de carte bancaire, adresse) ;
> données biométriques (reconnaissance faciale, empreintes digitales, valeurs physiologiques [rythme cardiaque, par exemple]).

Si l'on considère les données selon leur mode de collecte (*method of data collection*) par ceux qui les utilisent ou les commercialisent, on peut distinguer les données personnelles *stricto sensu* (nom, prénom, date de naissance, etc.), les données d'usage qui ne sont pas une catégorie prévue par la loi mais qui sont la traduction de nos comportements en ligne ou hors ligne et, enfin, les données de « profilage » qui résultent de l'analyse, par les algorithmes élaborés des sites web, du croisement entre données personnelles et données d'usage.

> Les données personnelles sont un outil marketing ultra-puissant

Quelle que soit la typologie retenue, on mesure, du fait de leur extrême diversité, la complexité à définir un régime juridique unique pour ces différentes données et à leur accorder une valeur. Il paraît certain, en revanche, qu'elles sont d'une grande utilité économique pour les organisations qui en disposent : elles leur permettent de connaître nos centres d'intérêt, nos habitudes de consommation, nos dépenses, nos trajets, la composition de notre foyer, d'établir des profils, d'optimiser leur tarification, de nous adresser de la publicité ciblée qui sera d'autant plus pertinente que la quantité d'informations détenue sur la personne sera importante, de rapprocher nos consommations effectives de notre probabilité de développer certaines maladies, de constituer et de mettre à jour des fichiers qu'elles se revendent entre elles, d'établir des statistiques, de modéliser nos désirs de consommation pour mieux les influencer dans le temps et dans le contenu, etc. À cet égard, elles sont un outil marketing ultra-puissant et ont incontestablement une importance économique majeure.

Les entreprises ne sont d'ailleurs pas les seules intéressées. Même si, aujourd'hui, les premiers acheteurs sont les acteurs de la grande distribution, les banques, les opérateurs télécoms et les transporteurs (compagnies aériennes et ferroviaires), l'État, les collectivités territoriales, les services publics, les partis politiques, les associations, les syndicats sont aussi concernés. Car l'utilisation de ces données n'a pas seulement un intérêt économique ; y sont aussi liés des enjeux de sécurité (lutte contre le terrorisme, contre la criminalité, etc.). Enfin, les données ne sont pas seulement collectées par ces entités, privées ou publiques. Elles peuvent également être diffusées par les personnes qu'elles concernent elles-mêmes (c'est le cas sur les réseaux sociaux tels Facebook, LinkedIn, Instagram, par exemple), par des tiers ou bien encore par des traitements automatisés. De nouveaux acteurs économiques ont ainsi émergé (les moteurs de recherche ou les réseaux sociaux) dont la collecte et le regroupement des données sont le principal actif stratégique.

Finalement, c'est peut-être cette infinie variété des acteurs économiques, des modes de collecte, des usages, des objectifs poursuivis (de l'Open Data au marketing individualisé), ainsi que leur multiplication permanente et exponentielle qui permettraient, au-delà de la définition légale, de définir les données à caractère personnel davantage comme un flux continu d'informations généré automatiquement par les activités numériques, que comme un concept aux contours figés et parfaitement identifiables. Si les consommateurs ont tendance à imaginer que les données se résument à celles délibérément communiquées, les organisations, elles, savent les utilisations multiples et encore insoupçonnées qu'elles peuvent en faire dans un environnement en mutation et en accélération constantes.

Valeur des données et fondement de leur protection

Ce potentiel de valeur en perpétuelle évolution en rend l'estimation difficile. Le *Financial Times* a imaginé un simulateur qui permet d'évaluer le montant que les professionnels du marketing en ligne seraient prêts à payer pour avoir accès à nos données personnelles. Les données de base (âge, sexe, code postal, niveau d'éducation) sont estimées à 0,0005 $ par personne. Mais si la personne devient un potentiel acheteur automobile, sa valeur s'élève à 0,0021 $ et s'il s'agit d'une femme au deuxième semestre de sa grossesse, sa valeur passe à 0,11 $. De façon générale, plus l'information est confidentielle et plus elle est précieuse, les données nues ayant peu de valeur. La valeur provient de la possibilité d'analyser, de retraiter, de compiler des millions de données. On peut imaginer plusieurs méthodes pour estimer la valeur des données. La première consisterait, par exemple, à diviser la capitalisation boursière d'une plateforme numérique par son nombre d'abonnés, ce qui, pour Facebook, représente environ 300 dollars par personne. Une autre consisterait à calculer le coût de ne pas divulguer ses données personnelles. Ainsi, une start-up californienne, Protect my ID, vend une protection au prix de 15,95 $ par mois. Il existe aussi aux États-Unis des *data brokers*, interdits en France, qui se spécialisent dans la vente de données destinées au ciblage publicitaire et qui sont ainsi à l'origine d'un marché et donc, d'une cotation de la donnée.

Pourtant, si le droit reconnaît un droit de propriété sur les fichiers et les bases de données, il n'en est pas de même pour les données personnelles qui, elles, relèvent du droit à la vie privée. En tant que droit attaché à la personnalité, le droit à la vie privée est un attribut que la loi reconnaît à tout être humain au même titre que le droit à l'intégrité corporelle, le droit à l'honneur et à l'image, le droit au respect de la présomption d'innocence, etc. Et tous ces droits de la personnalité ont pour caractéristique d'être placés en dehors du commerce juridique et d'être dotés d'une opposabilité absolue.

Concrétisant le processus de réforme engagé en 2012, l'Union européenne a adopté le 17 décembre 2016 le General Data Protection Regulation (GDPR) qui s'appliquera en 2018 à toute entreprise qui collecte, traite et stocke des données personnelles dont l'utilisation peut directement ou indirectement identifier une personne. Ce règlement européen, dont le but principal est de simplifier et d'harmoniser la protection des données personnelles dans les pays membres, s'appliquera à tous les acteurs économiques : les entreprises bien sûr, mais aussi les associations, administrations, collectivités locales et syndicats. Il repose sur le droit de chacun à la protection de ses données personnelles. Il énumère des droits renforcés, notamment en prévoyant la nécessité d'obtenir que la personne indique clairement qu'elle consent au traitement des données à caractère personnel, en prévoyant un accès plus facile de la personne aux données qui la concernent, en prévoyant des droits à la rectification, à l'effacement des données et à l'oubli, le droit de s'opposer notamment à l'utilisation des données à des fins de profilage, ainsi que le droit à la portabilité des données d'un prestataire de services à un autre. Parallèlement, le GDPR impose aux entreprises des obligations et des sanctions en cas de non-respect.

Au niveau national, dans la même dynamique, a été adopté en première lecture à l'Assemblée nationale, le 26 janvier 2016, le projet de loi pour une République numérique. L'exposé des motifs du projet de loi rappelle que son article 26 consacre le droit à la libre disposition de ses données, c'est-à-dire le droit de l'individu de décider de contrôler l'usage qui est fait de ses données à caractère personnel. Il est censé constituer une réponse à la perte de maîtrise par les individus de leurs données personnelles, en donnant sens aux droits déjà reconnus par les textes existants (droit d'accès, droit d'opposition…).

En 2013 déjà, un rapport du Forum économique mondial de Davos publié en collaboration avec le Boston Consulting Group, développait l'idée d'*empowerment* des individus et la nécessité d'une nouvelle approche. Le rapport opposait deux conceptions : la première, traditionnelle, prévalant dans les années 1970 et fondée sur le consentement de l'individu à l'usage de ses données au moment de leur collecte, et la seconde, plus récente, rendue nécessaire par la complexité de l'écosystème des données personnelles caractérisé par sa rapidité d'évolution, par l'immense potentiel de valorisation des données et par le rôle dévolu à l'individu, à la fois producteur et consommateur de ses données. Et le rapport de recommander un changement dans notre manière de penser pour passer de la protection au moment de la collecte des données à une approche qui renforce la confiance de l'individu dans l'utilisation qui sera faite de ses données personnelles ultérieurement. Dans son rapport annuel de 2014, le Conseil d'État développait aussi cette idée, faisant remarquer que les droits reconnus aux individus se limitent, pour l'essentiel, à leur permettre de rester à l'écart du traitement de leurs données (choix qui n'est presque jamais fait), sans leur donner un réel pouvoir sur le contenu du service et la manière dont leurs données sont traitées. D'où l'exigence de mettre le numérique au service des droits individuels dans une logique d'*empowerment*, d'autonomisation des individus, visant à accroître leur capacité à agir pour la défense de leurs droits.

Les évolutions législatives récentes ont donc fait le choix de consacrer un droit à la libre disposition de ses données. L'objectif est de renforcer les pouvoirs de contrôle de l'individu sur ses informations personnelles dans une société de l'information et de la communication qui semble l'en priver du fait de la puissance de traitement permise par les technologies. L'idée est qu'il devienne le véritable maître de ses données personnelles. Il s'agit donc bien de répondre à l'objectif de protection par la création d'un nouveau droit rattaché à la personne.

Efficacité du droit à la libre disposition des données personnelles

Il est pourtant possible de s'interroger sur l'efficacité de ce principe de libre disposition dans la défense de nos libertés. Comme certains ont pu le faire remarquer, il est à craindre que l'individu soit au contraire ainsi fortement démuni face à des auteurs de fichiers et de traitements qui ne s'encombreront pas de trop de précautions pour s'assurer du plein et libre consentement des intéressés. Déjà débarrassées depuis la directive européenne de 1995 de l'obligation d'obtenir, sauf cas particulier, l'autorisation préalable de la Cnil, les entreprises ne verront-elles pas ainsi leurs formalités encore allégées ? L'individu ne devrait-il pas être considéré comme une partie faible face aux sites des géants de l'internet ? N'est-il pas trompeur de s'abriter derrière la proclamation

d'un droit fondamental et le pouvoir qu'on donne ainsi officiellement à un individu pour, en réalité, l'exposer au risque de consentir sans le discernement nécessaire à des clauses éminemment techniques insérées dans des contrats d'utilisation rédigés par des professionnels et incompréhensibles du profane ?

La création d'un droit rattaché à la personne n'était pas la seule solution possible. Il y a plusieurs années déjà, l'ancien président de la Cnil, Alex Türk, faisait remarquer « qu'il y a un fossé abyssal entre la conception américaine des données personnelles qui sont pour eux des biens marchands et la conception européenne où il s'agit d'attributs de nos personnalités ». Et en effet, la thèse patrimoniale sur les données personnelles affirme que la meilleure réponse est de faire entrer les données dans le champ patrimonial des personnes. Il s'agirait d'instaurer une propriété privée sur les données qui n'existe aujourd'hui dans aucun pays au monde.

C'est pourtant une solution que le Conseil national du numérique (CNNum) excluait expressément dans son rapport du 13 juin 2014. Si « la reconnaissance d'un droit de propriété sur les données personnelles est souvent avancée comme moyen de rééquilibrer les pouvoirs avec les entités collectrices », le CNNum invite à exclure cette option pour trois principales raisons :

> « 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 sur 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. »

Finalement, que l'on s'oriente plutôt vers l'octroi réglementé d'un droit d'usage ou d'un droit de propriété intellectuelle ou vers une forme de droit de propriété plus global dont les contours ne sont toutefois pas aujourd'hui définis, le choix risque d'avoir peu d'effet pratique pour chacun. Quelle sera en effet la réalité de ce droit au moment où l'individu acceptera, par un simple clic, les clauses multiples d'un contrat d'adhésion abscons par lequel il reconnaîtra, à son tour, de multiples droits au fournisseur de services sur ses propres données ? Cette situation ne doit pourtant pas être vue comme une défaite de l'individu face à de puissants acteurs transnationaux. L'accès à un service gratuit de grande qualité, l'optimisation de l'expérience utilisateur ou une surveillance renforcée dans le cadre de la prévention et de la lutte contre le terrorisme, la délinquance et les accidents sont des avantages à ne pas sous-estimer et qui constituent déjà des motivations puissantes à l'acceptation à titre gratuit de l'usage de nos données personnelles.

L'arbitrage coûts/opportunités de cette autorisation d'usage pourra alors relever soit du marché (le moteur de recherche gratuit DuckDuckGo propose une alternative à Google en garantissant l'absence de toute collecte de données et par conséquent de tout échange de données, libre à chacun de l'adopter contre quelques restrictions de qualité), soit du droit souple (recommandations, chartes d'engagements, standards, etc.) comme la Cnil l'encourage déjà. Ce mode de régulation intelligent promeut un nouveau paradigme économique autour des données personnelles : celui d'une économie symétrique, où les consommateurs/clients bénéficieront d'une valeur d'usage de leurs données pour devenir de véritables cocréateurs de valeur autour de quelques principes forts : transparence réelle sur l'utilisation des données, utilité avérée de leur exploitation et effectivité des droits de rectification, de suppression et d'oubli. ●

> bibliographie/sitographie

Bellanger P., *La Souveraineté numérique*, Paris, Stock, 2014.

Babinet G., *L'Ère numérique, un nouvel âge de l'humanité*, Paris, Le Passeur, 2016.

Cahen M., « Utilisation des données à caractère personnel ». En ligne : www.legavox.fr/blog/murielle-cahen.

CIGREF, *Économie des données personnelles : les enjeux d'un business éthique*, rapport, octobre 2015.

Conseil national du numérique, *Rapport sur la neutralité des plateformes*, mai 2014.

Conseil d'État, *Étude annuelle 2014 : le numérique et les droits fondamentaux*, Paris, La Documentation Française, 2014.

Microsoft Advertising, *La Valeur des données personnelles*, étude, juin 2015.

Peugeot V., « Données personnelles : sortir des injonctions contradictoires », 13 avril 2014. En ligne : http://vecam.org, rubrique « Cogitations ».

World Economic Forum, *Unlocking the Value of Personal Data: From Collection to Usage*, avec la collaboration du Boston Consulting Group, février 2013.

Site de la Cnil : www.cnil.fr

Site de la Commission européenne : http://ec.europa.eu