DIGITAL NEW DEAL FOUNDATION

RAPPORT D'ÉTUDE **SEPTEMBRE 2015**

QUELLE POLITIQUE EUROPÉENNE EN MATIÈRE DE DONNÉES PERSONNELLES ?

www.thedigitalnewdeal.org

QUELLE POLITIQUE EUROPÉENNE EN MATIÈRE DE DONNÉES PERSONNELLES ?

Note d'analyse – Digital New Deal Foundation - septembre 2015

Judith Rochfeld

Judith Rochfeld est titulaire d'une maîtrise en droit français à l'Université Panthéon-Sorbonne, Paris 1. A la suite d'un DEA de droit privé, elle a soutenu sa thèse à l'Université Panthéon-Sorbonne en 1997 et a passé l'agrégation de droit privé et de sciences criminelles en 1999. Elle a été professeur à l'Université du Maine puis à l'Université Paris-Sud, 11, Faculté Jean Monnet, à Sceaux. Elle est professeur à l'Université Panthéon-Sorbonne (Paris 1) depuis 2007.

Judith Rochfeld a dirigé le groupe de recherche en droit européen des obligations au sein de l'Unité Mixte de Recherche n° 8103, CNRS-Paris 1. Elle a dirigé et co-dirigé plusieurs ouvrages de droit européen.

Judith Rochfeld a été membre du groupe de recherches sur le droit communautaire existant, dit groupe « Acquis communautaire », de 2000 à 2009. En son sein, elle a participé à la rédaction d'ouvrages reconnus. Ce groupe a également participé au Projet de cadre commun de référence.

Judith Rochfeld a régulièrement tenu une chronique de sources législatives, à la Revue trimestrielle de droit civil, de 2000 à 2010 ; de droit des obligations, à la Semaine juridique, de 2000 à 2005 ; de sources de droit des contrats, à la Revue des contrats, depuis sa création.

Ses principaux domaines d'enseignement et de recherche sont le droit des contrats, interne et européen ; le droit de la consommation ; les grandes notions du droit privé ; le droit du commerce électronique ; le renouvellement des figures de la propriété. Elle dirige le Master 2 de droit du commerce électronique et de l'économie numérique de l'Ecole de droit de la Sorbonne, Université Panthéon-Sorbonne. Ses publications sont nombreuses, en français et en anglais. Son dernier essai, A qui profite le clic ?, paru en 2015, explore la question du partage de la valeur à l'ère numérique.

Sommaire

I - LE CONTEXTE RELATIF AUX DONNÉES PERSONNELLES : LES BASCULEMENTS DE LA CRÉATION DE VALEUR

Traditionnellement, la personne est productrice de valeur par sa force de travail ou encore par le résultat de sa création. Mais depuis peu, l'individu sécrète une **nouvelle source de valeur**, presque à son insu, dans la mesure où elle ne suppose pas de sa part des efforts conscients : la valeur émane des informations qu'il génère, soit consciemment (quand une personne remplit un formulaire d'inscription sur un site par exemple), soit inconsciemment. A ce dernier égard, en effet, lors de ses pérégrinations sur internet et par le biais de témoins ou *cookies* de connexion ou de navigation, des informations sur ses préférences et préoccupations se trouvent stockées.

Ces informations sont, par la suite, activées lors de la navigation de l'individu de site en site : ces *cookies*, gérés par des régies publicitaires spécialisées, livrent à des partenaires qui le leur demandent, et ont conclu des accords en ce sens, les détails de ces visites ; les régies les analysent et permettent d'adapter extrêmement rapidement (on parle de centièmes de seconde) la publicité qui sera tout spécialement destinée à la personne ciblée. Un commerçant ou un prestataire de service (ou plus exactement la régie qui s'occupe de son compte) devient ainsi capable de proposer, dans un laps de temps très court, des produits et des services en rapport avec les précédentes visites et centres d'intérêt de l'internaute. Qui n'a pas fait l'expérience, à l'occasion d'une navigation sur internet, de voir s'afficher (sous forme de bannières défilantes, d'un lien commercial, etc.) des offres en lien direct avec une page web antérieurement consultée ? Une offre de vol pour New York ou de chambre d'hôtel correspondant miraculeusement à une ancienne requête ?

Ces informations ne sont pas seulement collectées lors d'une utilisation d'un ordinateur ; la réalité physique est de plus en plus connectée et numériquement tracée. La géolocalisation des détenteurs de *smartphones*, qu'elle repose sur l'utilisation de puces RFID ou consiste en l'indexation de contenus échangés par le biais de bornes Wi-Fi, permet de suivre les mouvement et parcours de leurs porteurs et d'adapter, également, la publicité ou les offres de produits ou services en fonction de l'endroit où ceux-ci se trouvent : « à 5 mètres, le magasin X propose une remise de 10% ! ».

La connexion des objets du quotidien le permettra encore davantage : qu'ignorera-t-on de nous quand tous nos frigos seront connectés et surveilleront que nous avons toujours du lait en quantité suffisante en fonction de la taille et de l'âge des occupants du foyer ? Quand les inhalateurs des vaporisateurs contre les allergies et l'asthme dessinent déjà, sur fond de données partagées, la carte des endroits que les asthmatiques doivent éviter ? Quand se généraliseront les fourchettes qui vous signalent que vous mâchez trop vite ? Ces objets seront bientôt dans toutes les maisons et donneront des indications que tous commerçants (assureurs,

employeurs, ou Big Brothers en tous genres) souhaiteront pouvoir exploiter. Nos téléphones ou nos cartes de paiement sans contact diront tout de nos achats, habitudes et envies.

Pour autant, il est faux de dire que « la » personne, seule, est créatrice de valeur. **C'est bien davantage la multitude** qui l'est : une donnée personnelle a peu de valeur isolée ; elle n'en acquiert que **mise en relation avec d'autres**, ce que d'aucuns nomment le « graphe », le « réseau » (P. Bellanger) : la valeur est difficilement mobilisable par chacun des producteurs individuels ; elle n'est intéressante et n'émerge véritablement, pour le *Big Data* ou le *Big Analysis*, qu'au moyen d'une mise en relation.
En outre, les ressources issues de ces masses (plus exactement leur accroissement exponentiel) ne sont génératrices de richesse que dans la mesure où elles sont détectées, hiérarchisées, « poussées » vers ceux qui en sont les destinataires. La valeur vient du rassemblement, du recoupement et de l'analyse de l'information qui permet de faire parler les données ainsi recyclées.

C'est donc bien l'utilisation secondaire (voire les multiples utilisations secondaires) de la donnée et ses nouveaux instruments de compréhension (majoritairement à des fins prédictives) qui en révèlent toute la valeur. **La valeur provient essentiellement de l'exploitation des données en masse, ou de masse, par les opérateurs capables de les recueillir et ou de les agréger.**
Le traitement des données personnelles n'échappe donc pas au paradoxe actuel de l'économie numérique : le double phénomène de production éclatée de la valeur et de sa restitution *via* une concentration de l'attention organisée autour de grands intermédiaires ; c'est ce phénomène qui doit conduire à reconsidérer les schémas juridiques actuels pour éprouver leur capacité à s'adapter à l'écosystème numérique.
La valeur induite s'inscrit donc comme le produit d'une rencontre entre la valeur éparpillée, d'une part, et l'attention de destinataires, d'autre part[1].

Les données représentent ainsi **une manne** si l'on veut les utiliser pour guider les comportements de consommation, voire pour les influencer. Mais parlons chiffre, même s'ils peuvent être sujets à caution : à combien s'élève leur valeur et qui en profite ? Viviane Reding, vice-présidente de la précédente Commission européenne, estimait que la valeur des données livrées par les citoyens européens en 2011 s'était élevée à environ 315 milliards d'euros. Elle prédisait que cette valeur produite par les données en Europe pourrait représenter 1000 milliards en 2020[2], soit **8% du PIB européen**. Le modèle d'affaire, « l'or noir » de l'internet, c'est le *data to value* : rassembler les informations numériques laissées dans le sillage de la navigation ; réaliser des socio-types des internautes ; les cribler de manière permanente de messages publicitaires, pour ultimement, déclencher le clic d'achat ; à terme, produire des services et des biens qui correspondent à ce que les utilisateurs voudront dans 6 mois, avant même qu'eux-mêmes le sachent… Plus d'un milliard de bannières publicitaires *par jour* sont livrées aux sites du monde entier par Critéo, la start-up française au 200 000% de croissance en cinq ans.

Or, cette immense valeur des données, si tant est que l'on parvienne à la saisir véritablement, **ne profite pas à tous ceux** qui s'en trouvent à l'origine, à savoir les individus numériques… La plupart d'entre eux n'ont pas même conscience, d'ailleurs, qu'ici réside la véritable contrepartie de la gratuité de la vie sociale dont ils sont devenus les captifs consentants. Combien de fois sont acceptées, sans les lire, des clauses précisant que l'opérateur dispose de la « propriété » des données dont il pourront à loisir faire les usages les plus étendus ? Quand bien même serions-nous vigilants, comment renoncer à certains services dont l'accès est conditionné par ces Conditions Générales d'Utilisation ? Qui aurait le courage aujourd'hui de couper un adolescent de ses réseaux sociaux, au motif que ses discussions dilapident un précieux capital informationnel familial ? Si la donnée émane de l'individu, celui-ci est loin de maîtriser son destin, forcé qu'il est, pour appartenir à la société numérique, d'en abandonner le contrôle. Ce d'autant plus que l'utilisation de ces données et traces sert également ses intérêts pour rendre les services utilisés plus efficaces. L'argument utilitaire constitue d'ailleurs le principal fondement des opérateurs pour justifier cette captation. L'exemple de l'avertissement en matière d'utilisation des cookies rendu obligatoire par la CNIL démontre que les opérateurs savent transformer une obligation en un atout « marketing ». Les cookies ne sont-ils pas utilisés, selon eux, « pour rendre plus agréable la navigation » ?

Par ailleurs, la valeur est concentrée aux mains des GAFTAM (Google, Amazon, FaceBook, Twitter, Appel, Microsoft), qui centralisent l'audience et partant les données ; ces opérateurs sont à même de constituer des monopoles informationnels en position d'ultra-domination, chacun dans un secteur qui leur est propre d'ailleurs, ce grâce aux effets « autorenforçants » qui caractérisent l'économie numérique, comme l'a parfaitement décrit le Conseil national du numérique dans son rapport sur « la neutralité des plateformes » de mai dernier. Dès lors, le phénomène est à même de bloquer l'entrée sur le marché de nouveaux acteurs, ainsi que l'innovation, financée à partir de ces données, en « contrepartie » de services dits gratuits.

1 V.-L. Benabou et J. Rochfeld, *A qui profite le clic ?*, O. Jacob, 2015.
2 http://europa.eu/rapid/press-release_SPEECH-13-788_en.htm

II - QUELS ENJEUX POUR UNE POLITIQUE RELATIVE AUX DONNÉES PERSONNELLES ?

Nous nous sommes pour l'heure contentés d'évoquer les questions de valorisation et de répartition des profits nés des données. Ce n'est évidemment pas les seuls enjeux que doit saisir une politique relative aux données personnelles. Il faut bien davantage considérer **les conséquences en termes :**

- de frontières à garantir du caractère privé de la vie des individus (questions de la protection de la vie privée, de l'image des individus renvoyée sur internet, de leur réputation). La protection de la vie privée des individus suppose **d'offrir à chacun des mécanismes de protection efficaces** des données à caractère personnel collectées, consciemment ou non, dans un environnement numérique. Cette protection implique également de conférer aux individus les moyens de **mettre en œuvre les mécanismes protecteurs** lorsqu'ils existent. La force du numérique, son ampleur et son intemporalité notamment, supposent d'adapter les moyens de réaction juridique afin d'assurer l'efficacité de la nécessaire protection des personnes concernées. Ces nécessités s'élèvent face à un brouillage des frontières entre les sphères privée/publique, personnelle/professionnelle : l'intrusion du numérique dans nos vies a fait disparaître ces frontières, au profit d'un « tout public » et d'un principe de liberté d'expression, lui-même dévoyé dès lors qu'érigé en principe absolu.

- d'absence de discriminations (dans l'accès à l'emploi, l'assurance, l'accès aux services, la détermination du prix des produits et services), discriminations qui peuvent être menées de façon occulte, sur le fondement de profils-types élaborés par l'analyse des traces numériques consciemment et inconsciemment livrées. Cette problématique rejoint celle :

- de lutte contre les manipulations contraires aux libres choix des individus, dès lors que ceux-ci pensent prendre des décisions sur le fondement de propositions neutres de produits ou de services, alors qu'ils les élaborent en réalité sur la base d'offres différenciées et spécialement adaptées à leur profil-type par des algorithmes (questions de la transparence et de la neutralité des algorithmes).

- des capacité d'innovation et de création de valeur par le système économique. S'il n'est pas question de brimer les initiatives innovantes qui reposent, notamment, sur l'utilisation des données à caractère personnel, il convient de prévoir l'environnement juridique à même de permettre le déploiement de ses activités dans le respect des droits de chacun. Cela ne suppose pas nécessairement, ou pas exclusivement, d'interdire, mais certainement d'accompagner l'innovation par une meilleure information et une plus grande éducation de chacun sur les conséquences de l'utilisation des services numériques, des droits dont chacun dispose et des facultés de chacun pour mettre en œuvre effectivement ces droits.

- de capacité à faire collectivement des choix de société sur les utilisations de ces données en matière de sécurité publique (question des moyens admissibles par les services de renseignement).

Nous écarterons de notre propos présent les questions d'utilisation des données à des finalités prédictives de renseignement, pour nous concentrer sur les utilisations admissibles et les politiques à mener, au regard des autres finalités listées.

III - LES LIMITES D'UN RAISONNEMENT EN TERMES DE VALORISATION

Or, pour traiter de ces différents enjeux, il semble insuffisant de s'en tenir à un débat — qui a pris une ampleur importante —, en termes de « retour de valeur » vers les internautes. L'une des questions majeures, préalable à beaucoup d'autres, tient précisément en cette admission d'une valeur des données, fondée sur la « propriété » de ces dernières, que cette propriété soit consacrée au bénéfice des internautes ou des opérateurs. Le Président Obama s'est d'ailleurs prononcé en faveur de la « propriété » des données.

Mais, les données personnelles peuvent-elles véritablement être saisies comme des objets de « propriété » ?

Leur définition juridique les rattache plutôt à la personne : on entend par « donnée à caractère personnel », dans les textes européen et français :
« toute information concernant une personne physique identifiée ou identifiable », précision étant faite qu'est réputée « identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale » (article 2 de la directive 95/46 du 24 octobre 1995 ; article 2 de la loi française « Informatique et Libertés » du 6 janvier 1978, plusieurs fois remaniée).

On vise là évidemment les noms, prénoms, dates de naissance, adresses postales ou électroniques, les numéros de téléphone, les numéros d'identification ou de sécurité sociale, mais aussi, de manière moins évidente, les adresses IP des ordinateurs etc. La liste n'est nullement exhaustive car, aujourd'hui, tout est devenu donnée personnelle : il est possible, à partir d'une photographie, de remonter, grâce à un logiciel de reconnaissance faciale et/ou par croisement avec une autre donnée, à l'identité de la personne ; la navigation électronique de la personne dans un moteur de recherche (grâce aux *search logs* ou mots clés qu'elle utilise) permet de l'identifier par recoupement de ses centres d'intérêt et de ses requêtes ou de son adresse IP.

L'orientation qui sera choisie dans le futur règlement européen pourra d'ailleurs accentuer cette personnalisation de la notion.

Pour autant, ce rattachement ténu à la personne exclut-il que les données soient des biens ? Que leur régime protège une valeur économique, plutôt qu'un droit de la personnalité au respect de ses données ? Ou, inversement, les données ne devraient-elles pas être traitées comme d'autres attributs de la personne, indisponibles à elle-même et insusceptibles de faire l'objet d'une patrimonialisation ? On trouvera à cet égard, toute une palette de réponses.

Les données peuvent-elles être saisies comme des biens ordinaires, circulant tout à fait librement ?

Dans une première approche dite « réaliste », d'aucuns conçoivent les données personnelles comme des objets d'appropriation : la donnée serait un bien, un élément de valeur, à l'égard duquel le droit reconnaîtrait un droit de propriété (P. Bellanger, La souveraineté numérique, 2014, qui a néanmoins changé d'avis par la suite), ou du moins un mode d'appropriation par une personne. Cela ne voudrait pas forcément dire que toute collecte (et autres traitements) ou commerce juridique seraient admis à leur égard, puisqu'il peut exister des limites, en droit, posées à la création et à la circulation d'éléments de valeur3 . Mais, de principe et sous réserve d'un encadrement et de limitations spécifiques, la collecte, la circulation et le commerce des données seraient admis.
Certes, mais l'on n'a pratiquement rien réglé par une telle conclusion : au profit de qui reconnaître une propriété des données ? Sont-ce ceux qui s'en trouvent à l'origine qui doivent en recueillir la valeur — nous tous qui disséminons nos données — ou bien ceux qui les stockent, les traitent et leur insufflent, précisément, cette valeur ? Qui en devient propriétaire et doit bénéficier de la richesse qu'elles représentent ?
La question est épineuse car il faut bien se rendre compte que si une donnée ou un ensemble de données relatif à un internaute isolé peut avoir une valeur — pour soutenir une publicité ciblée qui lui soit spécifique, par exemple —, c'est qu'un écosystème complexe et coûteux s'est mis en place, à l'initiative des agents économiques présentés. Surtout, les données acquièrent bien davantage leur valeur lorsqu'elles sont collectivement traitées (on évalue d'ailleurs la valeur des données d'une seule personne à un très faible prix[4]) : les spécialistes évoquent le « graphe », le « réseau » ou le croisement de données, celles d'un individus renseignant grandement sur d'autres personnes et les croisements permettant de les mettre en relation et de bâtir des algorithmes performants pour en tirer toutes formes d'indications[5]. Le *Big data*, le *Big analysis*, tendances lourdes de l'économie numérique actuelle, attirent précisément l'attention sur cette mise en relation ainsi que sur le traitement et le re-traitement de gigantesques quantités de données. C'est pourquoi en réalité, dans cette veine réaliste, il faut analyser quatre positions différentes :

- La première position tient en la défense de la **propriété de chaque internaute** sur ses données : chacun serait propriétaire de ses données et pourrait, auprès

3 La qualification de choses « hors commerce » s'applique par exemple à des éléments dangereux comme la drogue ou entretenant un lien particulier avec la personne qui en est à l'origine.
4 « De l'ordre de quelques centimes ou de quelques dizaines de centimes », rappelait le Conseil d'Etat dans son Rapport préc., p. 265.
5 Cf. P. Bellanger, « Principes et pratiques des données personnelles en réseau », *Contribution au Rapport du Conseil d'Etat pour l'année 2014*, disponible en ligne : http://pierrebellanger.skyrock.com/3231110655-Principes-et-pratiques-des-donnees-personnelles-en-reseau.html, évoquant les algorithmes de corrélation, à savoir les « programmes informatiques qui permettent de déduire, par probabilité, des informations par le traitement prédictif de masse de données sans rapport direct avec l'information inférée, font que chaque donnée personnelle renseigne indirectement sur autrui », ainsi que « l'effet réseau », c'est-à-dire le fait que la valeur d'une donnée soit « proportionnelle au carré du nombre de données auxquelles elle est reliée », chaque donnée prenant sa pleine signification dans un contexte et avec des données supplémentaires.

d'un opérateur, en décider du traitement, en revendiquer et en administrer les usages, ainsi que la disposition et la valeur.
Les avantages de cette position paraissent indéniables : elle aurait le mérite de permettre une protection des personnes et de fonder une juste redistribution de la valeur[6].
Elle n'en a pas moins des inconvénients tout aussi indéniables : d'une part, elle occulte la valorisation des données par leur mise en relation collective ; d'autre part, pour la protection de la personne, elle ne serait que très partiellement efficace. Le Conseil national du numérique, dans son avis de mai 2014, a très bien résumé les principales failles de cette direction[7] : *« elle renvoie à l'individu la responsabilité de gérer et protéger ses données » ; elle « renforce l'individualisme et nie le rapport de force entre consommateurs et entreprises » ; « 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 »*. En définitive, *« elle déboucherait sur un renforcement des inégalités entre citoyens en capacité de gérer, protéger et monétiser leurs données et ceux qui, par manque de littéraire, de temps, d'argent ou autre, abandonneraient ces fonctions au marché »*. Le Conseil d'Etat, dans son rapport pour l'année 2014, a rappelé ces critiques : *« Même si le prix des données de chaque individu est appelé à croître de manière considérable au cours des années à venir (jusqu'à quelques euros), la valeur de l'actif que la reconnaissance du droit de propriété confèrerait à chaque individu restera dérisoire »* ; par ailleurs, *« les acteurs du numérique rédigeraient leurs contrats comme la fourniture d'un service en échange de la cession de droits d'utilisation des données, ce dont nombre de conditions générales d'utilisation se rapprochent déjà beaucoup ; le rapport de forces entre l'individu, consommateur isolé et l'entreprise, resterait marqué par un déséquilibre structurel. »*[8].

- Prenant en considération l'apport des opérateurs, une deuxième réponse a également été avancée : les données seraient des *res nullius* ; sans maître, elles n'appartiendraient à personne tant qu'elles ne seraient pas captées ; ce seraient en conséquence **les acteurs de l'économie numérique, en tant que premiers occupants, qui se les approprieraient** et pourraient les utiliser et les valoriser à leur guise[9]. Dans cette même veine, on pourrait également convoquer l'article 571 du Code civil : si l'apport de l'industrie dépasse celui de la matière première, la propriété revient à celui qui apporte son travail, sous réserve pour ce dernier de dédommager l'apporteur de ressource de la valeur de cette dernière[10]. A notre sens, néanmoins, la thèse revient à faire la part (trop) belle aux opérateurs et à ignorer dangereusement le lien des données avec la personne qui les

6 P. Bellanger, *op. cit*., avant, rappelons-le, que l'auteur revienne sur cette position.
7 CNN, Avis 2014-2 sur la neutralité des plateformes : réunir les conditions d'un environnement numérique ouvert et soutenable, p. 37. V. également V. Peugeot, « Données personnelles : sortir des injonctions contradictoires », site de Vecam, juillet 2014.
8 CE, Rapport préc., pp. 265-266.
9 P. Bellanger, *op. cit*.
10 Art. 571, c. civ. : *« Si, cependant, la main-d'œuvre était tellement importante qu'elle surpassât de beaucoup la valeur de la matière employée, l'industrie serait alors réputée la partie principale, et l'ouvrier aurait le droit de retenir la chose travaillée, en remboursant au propriétaire le prix de la matière, estimée à la date du remboursement. »*

engendre ; elle implique d'abandonner toute protection de cette dernière contre les risques de dévoilement de sa vie privée, de discrimination et d'orientation des comportements et à se concentrer uniquement sur des problématiques de valorisation des données qui, à une échelle individuelle et ainsi que nous l'avons vu, resteront minimes.

- Pour tenter alors une conciliation de ces visions — de celle de la propriété des internautes et de celle de la propriété des opérateurs — une troisième position propose de réintégrer le rôle de la personne « source », tout en conservant l'idée de propriété : la donnée serait un bien mais d'une texture tout à fait particulière en raison du lien qu'elle entretient avec la personne qui s'en trouve à l'origine ; dans un parallèle avec la **propriété intellectuelle**, elle serait une création de l'internaute[11].
En conséquence, et au titre des avantages, ce dernier en serait propriétaire et, à l'instar de tout auteur, devrait être consulté sur les utilisations de ses « œuvres » et rémunéré pour ces dernières. D'aucuns avancent même l'idée que cette rémunération puisse, toujours selon ce même parallèle, être collectée par des sociétés de perception et de répartition des valeurs engrangées[12].
Au titre des obstacles à cette conception, cependant, on peut douter que la donnée soit une « création » originale de l'internaute, d'une part, à laquelle ne participeraient pas les opérateurs, d'autre part (tant ce sont eux qui lui donne sa valeur).

- Enfin, au sein de ces visions qui appréhendent les données comme des « biens », il ne faut pas ignorer une quatrième position consistant à les saisir comme des **biens communs**[13]. Cette qualification présente un certain nombre d'avantages : elle entend signifier que les données peuvent/devraient revêtir une destination collective et que leur usage devrait être le plus ouvert possible, ce afin que toute personne puisse les utiliser (que ce soit pour s'informer, pour innover ou pour créer) ; elle entend également attirer le régime des données vers la nécessité d'une gouvernance collective, dans des intérêts généraux définis consensuellement ; elle veut, par là, les soustraire à la seule mainmise des grands opérateurs privés et aux enfermements monopolistiques, ainsi qu'à des gestions qui s'effectuent uniquement dans des intérêts commerciaux et non en faveur des impératifs collectifs évoqués (information, innovation, création ; mais aussi, possiblement, en fonction des informations, pour servir la santé ou assurer la sécurité).
Au rebours de la situation actuelle, on attirerait donc leur régime vers une gestion collective, dans l'intérêt de tous.

---

11 L. Chemla, « Nous sommes tous des ayants droit », Mediapart, 23 octobre 2013.

12 L. Chemla, préc.

13 V. Peugeot, préc. ; C. Argenton et J. Prüfer, "Search Engine Competition With Network Externalities", http://ideas.repec.org/p/dgr/kubtil/2011024.html, pour les données issues des historiques de recherche ; S. Mercier, « Biens communs et données personnelles : il faut réinventer ! », blog Bibliobsession, 12 mars 2014 : http://www.bibliobsession.net/2014/03/12/biens-communs-et-donnees-personnelles-il-nous-faut-inventer/ ; CNN, Avis 2014-2, précité, p. 39, pour les données publiques, les données conditionnant les libertés d'information, d'expression ou d'innovation ; L. Merzeau, « L'intelligence des traces », *Intellectica*, n° 59, proposant la construction d'*Identity commons*.

Pour autant, même si la défense de la thèse des biens communs porte en elle des velléités de protection individuelle et collective que nous partageons, il n'en faut pas moins relever un certain nombre d'inconvénients. D'une part, elle se fonde toujours sur une qualification de bien qui occulte par trop, à notre sens, le lien avec la personne. Elle convient mieux, en conséquence, à des données publiques, non personnelles. D'autre part, la qualification de bien commun implique que l'on puisse contraindre la volonté du « propriétaire » afin qu'il accepte de soumettre les utilités de son bien aux destinations collectives admises. Par exemple, le propriétaire d'un monument historique, monument reconnu comme tel en raison de l'intérêt historique qu'il présente, subit un certain nombre de contraintes dans l'intérêt de la préservation du patrimoine culturel et historique auquel son bien participe (en matière de restauration, de conservation et de destruction). Cette orientation ne nous paraît pas souhaitable en matière de données personnelles, où la protection des choix de l'individu concerné devrait à l'inverse se trouver renforcée. Or, pour atteindre ces mêmes buts, c'est une approche personnaliste qu'il faut à notre sens promouvoir.

En conséquence, seule une vision personnaliste des données nous semble à même de porter les impératifs de protection identifiés. Par là, il s'agit évidemment d'insister sur le **rattachement de la donnée à la personne de l'internaute et d'attraire son régime vers celui de la personne, de sa protection, et d'une vie privée entendue au sens large** : les données personnelles sont des éléments de la personnalité de chacun ; elles émanent des individus, révèlent leur identité et leurs comportements. A ceux que cet absolutisme effraierait, on peut néanmoins préciser deux nuances.

D'une part, on peut penser le régime des données dans un système mixte, selon un **parallèle avec les produits du corps humain : elles doivent relever, au stade des premières captations et utilisations, du consentement de la personne et d'un principe d'autodétermination informationnelle.**

Dans un parallèle avec ce qu'a forgé la Cour constitutionnelle allemande dès 1983[14], il faut plaider pour la reconnaissance d'un droit fondamental à l'autodétermination informationnelle : chacun devrait avoir le contrôle de tous les traitements relatifs à ses données (collecte, recueils de tous ordres) ; pouvoir garder le pouvoir sur les usages qui en sont faits, les administrer[15], ce pendant toute la durée des traitements (et donc décider d'accepter des changements de finalité, par exemple, grande question posée par le *Big data* mais très difficile à appliquer). C'est la thèse qu'a soutenue le Conseil d'Etat dans son rapport pour

14 Cour constitutionnelle fédérale de l'Allemagne, 15 déc. 1983, relatif à une loi sur le recensement : le principe est déduit des articles 1er (dignité de l'homme) et 2 (droit au libre développement de sa personnalité) de la Loi fondamentale et implique que « *la Constitution garantit en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel* ». V. Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie. », in K. Benyekhlef & P. Trudel (dir.), *État de droit et virtualité*, Montréal : Thémis, 2009.
15 Décider des copies, des modifications, des transferts, et des disparitions, cf. P. Bellanger, art. préc.

l'année 2014[16]. C'est également le fondement de certaines expériences menées, en Grande-Bretagne et en France, pour redonner aux usagers le contrôle des données que des opérateurs détiennent sur eux (projets « Mydatas »[17] et « Mes infos »[18]). L'approche a le mérite de se faire positive et offensive, au sens où, redonnant aux intéressés le pouvoir sur leurs données, elle leur ouvre de nouveaux champs d'utilisation, dans des buts individuels (les soumettre à des traitements que l'on souhaite et en tirer des corrélations, par exemple) ou collectifs (comme décider qu'elles doivent participer à une étude de santé publique) ; elle ne s'en tient donc pas à une approche défensive[19], en seuls termes de protection contre des agressions.

Comme les éléments du corps humain, les données alimentent des circuits de valeur ; elles pourraient être marquées par une patrimonialisation graduelle au sens où, plus elles sont transformés et leur lien avec la personne dilué, plus leur circulation est aisée ; cette valeur ne revient pas aux personnes « sources » (comme dans le cas de l'élaboration de médicaments brevetables à partir d'échantillons biologiques prélevés sur des patients). Par exemple, le sang ne peut faire l'objet que d'un don lorsqu'il est prélevé, mais les médicaments composés de produits sanguins, issus de sa transformation, peuvent quant à eux être cédés à titre onéreux entre professionnels[20]. Quant aux éléments de personnalité, ils ont, eux, subi une patrimonialisation directe, qui a abouti à ce qu'un individu puisse désormais, par contrat, octroyer à des tiers le droit d'utiliser ces éléments. Dans l'application du principe d'autodétermination, il pourrait donc être intéressant de faire un parallèle avec ces mouvements de patrimonialisation graduelle. On considèrerait alors, d'une part, que la personne peut accepter, au titre des décisions relatives à l'usage de ses données, certaines patrimonialisations (à condition que les termes de l'échange soient libres et clairs, ce qu'ils ne sont pas toujours actuellement, c'est-à-dire que l'usager sache que, pour bénéficier d'un service, il livre en échange ses données ; les textes sont pourtant déjà en ce sens qui insistent sur la loyauté du traitement, la transparence). D'autre part, on pourrait considérer que plus les données portent de liens avec la personne et permettent de la révéler, plus elles doivent être traitées dans l'orbite de la protection de cette dernière (on vise ici la collecte initiale et les utilisations qui conservent un lien fort avec un internaute) ; inversement, plus elles seront transformées et le lien avec la personne effacé, moins elles devraient être traitées comme un élément de personnalité (on vise là les traitements avec anonymisation irréversible par exemple, sous réserve que l'irréversibilité puisse véritablement exister ; les utilisations de données sous forme de statistiques[21] ; les propositions de triple chiffrement cryptographique, propre à garantir

16 CE, Rapport préc., p. 267.
17 Projet lancé par le Gouvernement de David Cameron en 2011 et visant à ce que les entreprises acceptent de partager, avec leurs clients, toutes les informations personnelles qu'elles détiennent sur eux.
18 Projet mené par la Fondation Internet Nouvelle génération (FING), v. le site : Mesinfos.fing.org.
19 Dans le même sens, CE, Rapport préc., p. 268.
20 Art. L. 1211-1 à L. 1274-3 puis L. 1243-1, c. santé publique.
21 Dans le même sens, CE, Rapport préc.

l'absence d'identification des personnes identifiées et à maîtriser les usages qui en sont faits[22]).
Reste que des difficultés non négligeables consistent à précisément tracer ces stades de détachement. Il demeure également que ces choix ne pourront s'effectuer qu'à une échelle collective.

Enfin, il serait nécessaire de tenir compte de la **dimension collective de la création de valeur** que les données induisent : la valorisation des données prend sa pleine mesure dans un traitement collectif de ces dernières, dans celui du graphe, du réseau de données ; leur régime de protection devra refléter cette dimension. Par ailleurs, c'est aussi **collectivement que les personnes devront pouvoir se défendre**, avec des outils de négociation collective, pour intégrer le passage à une « vie privée par négociation » (A. Casilli, « Contre l'hypothèse de la «fin de la vie privée» », *Revue française des sciences de l'information et de la communication*, n° 3, 2013 ; V. Peugeot, précitée), ainsi qu'au sein **d'actions collectives** dont il faut réclamer l'extension à la matière.

22 P. Bellanger, art. préc.

IV - LES HÉSITATIONS DU CADRE JURIDIQUE ACTUEL ET LES PROPOSITIONS DE PISTES DE RÉFLEXION

Actuellement, le droit positif se compose, en France, de la Loi du 6 janvier 1978 dite « Informatique et Libertés », plusieurs fois réformée, ainsi que, en Europe, de la Directive du 24 octobre 1995. Des discussions très mouvementées sont en cours, depuis 2012, relativement à une Proposition de règlement européen visant « à la protection des personnes physiques à l'égard du traitement de données à caractère personnel », ainsi qu'à une directive relative « à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données ». Ces deux textes, proposés le 25 janvier 2012, sont sur le point d'être adoptés en cette fin 2015.

En l'état, les instances européennes s'arrangent pour avancer sur une ligne de crête, dans un équilibre instable et à la recherche de compromis. Elles passent ainsi sous silence la question cruciale de ce qu'elles entendent prioritairement protéger : la circulation des données pour assurer la pérennité des modèles économiques ou la protection des personnes ? Les titres même des textes entretiennent le flou : la directive de 1995, comme l'actuel projet, affichent les deux finalités puisqu'ils sont relatifs « à la protection des personnes physiques à l'égard du traitement de données à caractère personnel » comme « à la libre circulation de ces données »[23]. Il est toutefois difficile de déterminer avec certitude l'orientation et la philosophie qui prévaut, tant les amendements portés par les partisans d'intérêts divergents, voire antagonistes, ont modifié l'économie générale du dispositif discuté.

La direction de protection des personnes n'y est néanmoins pas dépourvue de soutiens. Si l'on se réfère à quelques marqueurs pertinents, on remarquera que les textes européens et français font une place :
- au consentement de la personne concernée par l'utilisation de ses données ;
- à l'information sur les traitements (sur les données impliquées, sur leurs finalités et leur durée) ;
- aux divers droits dont l'individu bénéficie à l'égard des traitements qui sont effectués (d'information, d'accès, d'opposition, de rectification).

La proposition de règlement du 25 janvier 2012, amendée par le Parlement européen, repose d'ailleurs les grands principes de la matière (en son article 5) :
- les données doivent être traitées de manière licite, loyale, et transparente ;
- pour des **finalités déterminées, explicites et légitimes** ; en respectant des

23 Moins ambigu est, il est vrai, le titre de la directive « intermédiaire » 2002/58/CE du 12 juillet 2002 « concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques », dite « vie privée et communications électroniques ».

principes d'adéquation et de minimisation (on en traite le minimum, seules les données nécessaires pour servir la finalité considérée, ce pendant la durée appropriée), ainsi que **d'exactitude et d'intégrité** de ces dernières.
- Elle renouvelle, au titre des conditions de licéité du traitement, la légitimation par le consentement de la personne concernée.
-Par ailleurs, la proposition de règlement renforce l'effectivité des droits reconnus au bénéfice des personnes concernées (droits d'information, d'accès, de rectification, de suppression), par exemple en posant une obligation de proposer des procédures et mécanismes pour leur exercice (articles 11 à 14).
- Elle promeut également, quoique la portée en ait été amoindrie dans la version amendée du texte, un **droit à la portabilité des données**, c'est-à-dire une possibilité de les reprendre et d'en disposer librement en cas de changement de prestataires ou d'outils. La mesure est particulièrement appropriée aujourd'hui que se généralise le stockage des données à l'extérieur des ordinateurs et tablettes et est à même de participer à une reprise de contrôle par les personnes.
- La proposition avance aussi un « **droit à l'oubli numérique » (article 17), devenu un droit « à l'effacement »** dans la seconde version du texte, censé permettre à l'internaute de demander l'effacement ou l'invisibilité de données qu'il voudrait voir disparaître, parce que gênantes dans la construction de ses identités numérique et réelle (mais seulement si le traitement est illicite dans la seconde version amendée)[24].
- Notons enfin le renforcement important, si le texte était voté en l'état, des amendes que les autorités de contrôle pourraient prononcer : à l'heure actuelle, la CNIL française peut aller jusqu'à 150 000 euros pour un premier manquement (300 000 sinon) ; on passerait possiblement à 1 million d'euros d'amende ou 2 % du chiffre d'affaires annuel consolidé[25]. Ce renforcement des sanctions et des pouvoirs est absolument nécessaires afin d'assurer une certaine effectivité aux droits reconnus aux personnes concernées.

Les textes ne vont cependant pas assez loin dans l'adoption de l'approche personnaliste et donnent des gages à l'approche réaliste, de circulation des données. Pour ne s'en tenir qu'à quelques traits saillants, de nouveau, il faut relever que :
- le consentement demeure (même dans le règlement) **une cause de légitimation alternative du traitement, une condition parmi d'autres** (six dans la proposition[26]) **et non une condition singulière, quoique non exclusive, à l'instar de ce qui prévaut dans le dispositif français**, dont la très problématique

24 En réalité, le texte se contente de rappeler qu'une personne peut faire sanctionner des traitements illicites (quand les données traitées sont inadéquates ; s'il y a eu retrait du consentement ou exercice du droit d'opposition ; plus généralement en cas d'illicéité du traitement). C'est donc bien davantage la jurisprudence de la Cour de justice de l'Union européenne qui consacre ce droit.
25 Après le Conseil de juin 2015 ; antérieurement, on a parlé de 5 millions, cf. art. 79, 4 et 5, prop. de règlement préc. et proposition amendée.
26 L'existence d'une obligation légale à la charge du responsable du traitement ; la nécessité pour la sauvegarde de la vie de la personne concernée ; l'exécution d'un contrat auquel la personne concernée est partie ou encore l'exécution d'une mission d'intérêt général.

poursuite des « intérêts légitimes (du) responsable du traitement »[27] ;
- que les transferts de données hors Union européenne, s'ils restent soumis à un principe d'interdiction, s'entourent de procédures d'habilitation plus souples (le nouveau texte promeut un système de *Binding Corporate Rules* notamment, ouvrant la possibilité de lier des groupes distincts de sociétés et permettant de ne plus demander, pour chaque transfert, une autorisation de l'autorité de contrôle nationale) ;
- que le choix procédural d'un « guichet unique », c'est-à-dire l'octroi de la compétence du contrôle à une seule autorité nationale (« chef de file ») qui concentrera toutes les demandes contre un opérateur dès lors que ce dernier aurait son établissement principal sur le territoire d'un Etat membre, peut apparaître très favorable aux responsables de traitement et à leur activité[28] ;
- que l'action collective, tout juste évoquée, n'y retient pas une attention suffisante[29].

L'équilibre est en voie de reconstruction et les discussions sont acharnées… nous vivons un **moment de choix cruciaux** à l'égard desquels il est nécessaire et urgent de se positionner. L'opinion publique allemande en est consciente, qui s'anime de grands débats sur la question ; celle française a plus de mal à s'en passionner, alors même que ces matières s'avèrent décisives pour notre avenir à tous. **Rappelons les échéances précises. En Europe**, la fin de plus de trois ans de discussions acharnées et houleuses se profile, qui amènera à l'adoption du règlement européen relatif à la protection des données, antérieurement évoqué. Il réformera, de façon uniforme dans toute l'Union européenne, les textes actuellement applicables. **En France**, un projet de « Loi numérique » se trouve actuellement en discussion, qui comprend également des mesures relatives aux données personnelles (qui ne peuvent cependant venir empiéter sur celles du règlement européen, ces dernières primant le texte français). Enfin, **internationalement**, il faut prendre garde aux discussions relatives au **Traité** ou « **Partenariat de libre échange** » (ou encore TTIP pour *Transatlantic Trade and Investment Partnership*) entre les Etats-Unis et l'Union européenne, destiné à créer une zone de libre échange entre ces deux versants de l'Atlantique. Même si les questions relatives au transfert des données personnelles des européens vers

27 N'est-il pas légitime, pour un opérateur commercial, de rechercher son intérêt économique par le biais des traitements de données à caractère personnel de ses utilisateurs ? Selon l'interprétation qui sera donnée de cette disposition, la protection se fera donc plus ou moins efficace.
28 Il leur donne en effet la souplesse de se positionner dans un environnement qu'ils jugent le plus favorable à leurs intérêts et présente un risque de *Forum Shopping* étant donné les niveaux de protection divergents dans les différents Etats à l'heure actuelle. Schématiquement, les opérateurs auraient tout intérêt à éviter de s'implanter — ils le font déjà d'ailleurs (*adde* les raisons fiscales) — en France, en Allemagne ou en Espagne et à continuer de privilégier l'Irlande, par exemple. Cette orientation pourrait cependant être remise en question car, dans la deuxième version du texte, des critères de rattachement ont été ajoutés qui limitent quelque peu cette faculté (une autorité nationale pourrait être compétente dès lors que l'opérateur ciblerait les résidents de son Etat, pour ses offres de biens ou de services ou pour analyser leurs comportements).
29 Le texte en appelle à une possibilité de représentation collective, voire d'actions collectives, sa dernière version évoquant l'action de « *tout organisme, organisation ou association qui agit dans l'intérêt public* », sans préciser toutefois si les résultats de l'action seraient au bénéfice d'une collectivité de consommateurs.

les Etats-Unis ont été écartées des discussions en tant que telles, elles s'insinuent partout par ailleurs (quand on aborde le futur des télécoms, du e-commerce ; quand tous les objets du quotidien comme nos frigos et nos voitures — dont pour beaucoup les normes sont alignées dans le TTIP — seront connectés et leur circulation porteuse de données). Des arbitrages sont donc déjà effectués, qui n'empêchent pas cependant de se mobiliser pour réaffirmer des valeurs et exigences à préserver.

4 directions pourraient, sur ces fondements, être particulièrement explorées, dans une protection qui ne se voudrait pas défensive mais également positive du point de vue des internautes (ce afin que les *Digital Natives* y adhérent au maximum).

Mais avant d'entrer dans les détails de celles-ci, il serait au préalable nécessaire d'affirmer **l'importance d'une protection des données personnelles de chacun, au travers de la reconnaissance par le Conseil constitutionnel d'un droit fondamental.** La Charte des droits fondamentaux de l'Union européenne y procède, au travers de son article 8 dédié au droit au respect des données personnelles (et distinct de son article 7, consacré quant à lui au droit au respect de la vie privée). La Cour européenne des droits de l'homme a pallié l'absence de texte spécifique dans la Convention EDH (datant de 1950) en reconnaissant, sur le fondement de son article 8 (portant le droit au respect de la vie privée et familiale), une protection des données personnelles. La Cour constitutionnelle fédérale de l'Allemagne a également reconnu très tôt, le 15 décembre 1983 (relativement à une loi sur le recensement), qu'il fallait constitutionnellement garantir un tel droit et a exactement consacré la nécessaire « *capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel* », autrement appelée « autonomie informationnelle », (ce, sur le fondement des articles 1er — dignité de l'homme — et 2 — droit au libre développement de sa personnalité — de la Loi fondamentale). Ce serait donc vers une telle constitutionnalisation de cette autonomie qu'il faudrait également aller en France. Les directions qui suivent ne font que développer les composantes de ce droit.

1) L'accroissement de la transparence : connaître ses données

Laissez nous donc disposer de vos données et profitez de nos services plaident les tenants américains de la « mort de la vie privée » ; l'échange est équilibré, chacun a la contrepartie qu'il souhaite. C'est oublier que tout est fait pour rendre ces services absolument indispensables aux internautes et les tenir captifs au sein de silos de systèmes fermés (Androïd-Chrome-Google-Gmail-etc. ; IOS-Safari-iTunes ; etc.) ; c'est faire peu de cas, surtout, **de l'opacité entretenue sur l'existence même de cet échange et sur ses conditions** : le donnant-donnant ne s'affiche guère au grand jour et, même si davantage d'utilisateurs ont pris conscience de son existence — en témoignent les réactions de plus en plus rapides et courroucées aux changements intempestifs des termes des conditions générales et/ou des chartes de confidentialité des grands réseaux sociaux —, la plupart s'en accommodent, délaissant la protection de leurs données et ignorant

les tractations ou manipulations dont elles font l'objet.

Or, il conviendrait désormais que **chacun puisse s'exprimer sur l'échange proposé.** Il est vrai que depuis août 2011 les internautes français doivent être prévenus de la pose de cookies et qu'ils ont pris l'habitude de voir apparaître ces petites fenêtres d'avertissement sur la plupart des grands sites, au fil de leur navigation (l'obligation est européenne). Mais **la transparence devrait se renforcer et réellement porter sur les données collectées, leurs types, leurs quantités ; sur les finalités ainsi que sur la durée des traitements**. Ces exigences ne sont guère que la répétition des celles légales, de sorte que le renforcement doit bien davantage provenir des modalités de cette transparence.

Ici, il faut convoquer le droit de la consommation et son **contrôle des conditions générales** : il faut vérifier celles des grands opérateurs en termes d'accessibilité, de clarté et d'exhaustivité des énonciations relatives au données (ce qui est loin d'être le cas en pratique). L'UFC-Que choisir a commencé à le faire, contre Facebook, Twitter et Google +, en mars 2014 et on ne peut que la saluer d'aller dans une direction peu empruntée jusqu'alors.

Il serait également bienvenu de **simplifier et d'uniformiser, par des icônes et sur les pages de navigation ordinaires des sites (non sur celles dédiées aux conditions générales que personne ne lit), les indications relatives aux données** (cf. le système des « *Privacy Icons* » judicieusement mis en avant par le Conseil national du numérique, dans son avis 2014-2, précité, p. 41, destiné à fournir des pictogrammes simples, immédiatement compréhensibles part l'internaute moyen).
On pourrait, plus loin, instituer un **système de *reporting* annuel**, c'est-à-dire de synthèses individualisées relatives à toutes les données d'un internaute, détenues par un opérateur, et à tous les traitements et circulation dont elles font l'objet.

L'exigence de transparence devrait également s'appliquer au lien effectué par l'opérateur entre l'accès au service (ou la fluidité de cet accès) et la collecte des données (il faut rappeler qu'il est interdit de bloquer l'accès à un site si l'internaute refuse de livrer ses données, à moins que les données soient nécessaires à cet accès).

Allons encore un pas plus loin car nous n'avons pour l'instant raisonné qu'au regard d'un seul site. Or, dans cet effort de transparence, **un internaute devrait pouvoir connaître toutes les données qui le concernent, susceptibles d'être mises en relation** : en l'état il « ne peut effectuer une recherche globale sur l'ensemble de ses informations présentes sur (...) différents systèmes », relevait justement le Conseil national du numérique ; il « ne peut pas lister les sites détenant ses informations sensibles (comme ses informations bancaires) ». En prenant en compte le fonctionnement en silos des grands opérateurs et les potentialités de révélation qu'il renferme, l'internaute devrait pouvoir connaître l'ensemble

des données détenues par un « système » (Androïd-Chrome-Google-Gmail-etc. par exemple). Il devrait pouvoir connaître également, pour éventuellement sélectionner ses utilisations en fonction de ces critères, les lieux et les acteurs des traitements (sous-traitants, régies, etc.). Il faut également souligner les stratégies de partage des données mises en place par les opérateurs sans que l'internaute ne soit informé de ce partage (C. Google Now).

Un dernier point encore, majeur : **la transparence devrait aussi porter sur les distorsions d'usages résultant du traitement des données**. Quels internautes savent que les résultats de recherche que leur livre un moteur diffèrent de ceux d'autres individus en raison du traitement de leurs mots de recherches passées ou de leur profil ? Que les propositions ou conditions de vente ou de service de certains sites marchands se différencient pour les mêmes raisons ? Les algorithmes mis en œuvre, et leur soubassement de données, méritent eux aussi de passer au tamis de la transparence afin que soit révélé l'absence de neutralité pourtant si fortement revendiquée.

2. L'accroissement de la gouvernance individuelle : maîtriser ses données

Il serait également judicieux d'insister, techniquement comme juridiquement, sur les outils de contrôle individuel des données.
Techniquement, ces outils se multiplient d'ailleurs, qu'ils proviennent des grands opérateurs, jouant le jeu de la restauration de la confiance des utilisateurs (Google met ainsi à disposition des tableaux de bord permettant ce contrôle), ou, de façon plus neutre, des gouvernements (le gouvernement britannique soutient le projet MiData), ou encore d'organisations non gouvernementales. Le Conseil national du numérique, quant à lui, en appelait justement au soutien des initiatives « PIMS » (*Personal information Management System*), c'est-à-dire de **services hébergés sur des serveurs gérés pour l'utilisateur** (à son service), plutôt qu'hébergés sur les serveurs de grandes plateformes.

Juridiquement, il faut se demander s'il faut renforcer l'effectivité du consentement (quand il est la cause légitime du traitement), lors de la collecte et durant toute la durée de traitement des données. L'idée serait d'insister des **procédures de réaffirmations périodiques** de ce consentement, aux traitements en cours. **Au-delà d'une période moyenne, l'on pourrait également présumer que le consentement a cessé et il y aurait lieu d'instaurer un « droit à l'effacement cyclique de l'ensemble des données détenues par la plateforme, qui suivrait un rythme de péremption moyen des données »** (CNN, avis 2014, précité, fiche 2, p. 34). Par ailleurs, le Conseil d'Etat évoque justement, dans son rapport 2014, le consentement confronté à l'hypothèse du *Big Data* : on fait valoir que ces analyses de données à grandes échelles s'effectuent pour des finalités variées, changeantes au fil du temps ; qu'on ne pourrait s'y embarrasser du consentement. C'est vrai pour celles statistiques ; ça ne peut pas l'être — et il faut saluer le Conseil de le réaffirmer — pour celles qui conservent un lien entre la donnée et la personne (Conseil d'Etat, précité, p. 18). Pour autant, le consentement ne constitue pas une panacée, tant il peut lui-même être automatisé ou peu

regardant.
Par ailleurs, il s'agit d'être vigilant quant à **l'effectivité des droits reconnus** à chacune des personnes concernées (droits énumérés par la Loi « Informatique et Libertés » en France aujourd'hui et protégés par la CNIL) : le droit d'information ; le droit d'accès, de rectification et d'effacement ; le droit d'opposition à un traitement pour « motif légitime ». Cette effectivité et son renforcement composent des préoccupations du règlement européen antérieurement évoqué. Il serait nécessaire, en outre, d'insister sur un droit devenu capital, que reconnaît également le règlement européen : celui à la **portabilité de ses données**. Chacun doit en effet pouvoir quitter son opérateur en emportant ses données et, dans une certaine mesure, en étant certain que celles-ci ne restent pas à la disposition de cet opérateur (cette mesure n'est pas sans soulever de problème à l'heure où le *Big data* se nourrit précisément de grandes masses de données mais elle est reconnue comme importante dans le Règlement européen).

Faut-il aller plus loin dans ce contrôle et obliger chaque opérateur à proposer des services alternatifs qui ne procèdent pas à des traitements de données ? Des voix plaident en ce sens, ce qui équivaut à pousser vers une **régulation par le marché** : soit vous nous laissez l'accès à vos données, soit vous payez pour des solutions plus respectueuses de votre intimité et pour sortir du modèle de la fausse « gratuité ». Le marché de « l'anonymat » s'étend d'ailleurs : des moteurs de recherche se sont lancés tôt avec pour mot d'ordre d'effacer les données des utilisateurs (Ixquick dès 2006) ; Snapchat a promis la mémoire éphémère des contenus échangés, ceux-ci devant disparaître après quelques minutes (mais il a été condamné pour tromperie par La *Federal Trade Commission*...). La France a aussi connu des tentatives du genre. Qui ne se souvient de la carte de transport Navigo à 5 euros — plutôt que gratuite —, censée rester muette sur les circulations de son porteur (ce qu'elle n'a jamais été vraiment) ? Pas vous ? C'est qu'elle n'a pas remporté un vif succès... et, de façon plus large, c'est que peu de personnes estiment, encore aujourd'hui, que la protection de leurs données vaut paiement. Une étude allemande et anglaise de 2012 chiffrait ainsi à un infime pourcentage des personnes interrogées celles qui accepteraient de payer quelque 50 cents pour échapper à un traitement de données lors de l'accès à un service numérique gratuit. Il semble donc que le marché ne soit pas encore le mieux placé pour installer une forte régulation des usages. Quand bien même le serait-il, on rejoindrait les critiques émises précédemment sur le risque de protection à plusieurs vitesses, en fonction des moyens et de la conscience de chacun.

3. L'accroissement de la représentation et des actions collectives : défendre ses données

Enfin, il serait nécessaire de promouvoir les techniques juridiques de représentations et d'action collectives, et partant de convoquer à nouveau le droit de la consommation.
De négociation tout d'abord. D'un côté, en effet, l'aspect collectif de la valorisation des données est nettement apparu : pour les opérateurs, les données ne

composent un matériau appréciable que groupées ; le groupe concerné peut donc avoir des revendications à porter. D'un autre côté, le déséquilibre des relations entre consommateurs et opérateurs induit qu'une éventuelle négociation des pratiques se fasse, pour être efficace, à cette échelle collective. On suivra donc Antonio Casilli pour plaider pour un nouveau modèle de « *privacy* en tant que négociation ». On entend un écho identique, venu d'outre-Atlantique, où Melanie Swan incite les internautes américains à devenir des sujets actifs : « Quand nous laissons une entreprise s'emparer de nos données personnelles », explique-t-elle, « nous effectuons une transaction, nous livrons une matière première qui a de la valeur. Or, nous n'avons aucun pouvoir de négociation, nous acceptons les conditions imposées par l'industrie. » Et de tracer le même chemin que celui proposé par Antonio Casilli : « Je pense que les internautes vont s'unir et s'organiser pour défendre leurs intérêts en tant que fournisseurs de données. Pour cela, ils vont s'inspirer des associations de défense des consommateurs, ou même des syndicats ouvriers. Seule une réponse collective et solidaire pourra rétablir l'équilibre. »

Il faut promouvoir **des actions collectives ensuite**. Le constat est frappant : peu d'internautes ont, pour l'heure, manifesté de l'intérêt en justice pour ce matériau qu'ils génèrent (exceptons Max Schrems, cet étudiant devenu avocat, qui mène des actions multiples contre Facebook, dont la dernière, collective, a rassemblé 25 000 personnes et s'est jugée devant le Tribunal civil de Vienne qui s'est malheureusement reconnu incompétent) ; c'est que les intérêts en jeu, dans les litiges individuels, sont trop faibles pour justifier le coût d'une action (remarquons par ailleurs que les autorités de contrôle, pour beaucoup, se sont imposées comme des recours gratuits et efficaces). Il est évident que le terrain est plus propice pour les actions collectives. Pour l'heure, la loi française relative à la consommation dite « Hamon », du 17 mars 2014, ne les permet pas, qui circonscrit le domaine de ce type d'actions aux dommages matériels (avec toutes les ambiguïtés que le qualificatif recouvrerait ici). Il faut donc plaider pour une ouverture de ces actions à la matière.

CONSTRUIRE L'EUROPE NUMÉRIQUE

L'ambition de la Digital New Deal Foundation est d'éclairer le futur numérique de nos sociétés. C'est ainsi en premier lieu une mission de déchiffrage que se sont fixée les concepteurs de la fondation. Forts de la diversité de leurs expertises, ils font le vœu de mettre à la disposition du public et des décideurs leur lecture des enjeux numériques, en ce qu'ils bouleversent l'ensemble de notre économie et de notre société.

Au-delà de cette détermination pédagogique, les professionnels reconnus qui composent le Conseil d'administration de la fondation partagent la conviction qu'un futur numérique brillant est à la portée de l'Europe, pourvu qu'elle sache dessiner elle-même l'environnement et la régulation propice à son développement. Il s'agit dès lors de nourrir le débat et de contribuer à la réflexion collective sur des enjeux dont la portée ne peut plus être sous-estimée.
La révolution numérique produisant ses effets dans l'ensemble de l'économie, ce sont des personnalités de haut niveau issus de secteurs divers qui se sont rassemblés au sein de la Digital New Deal Foundation, créée en … 2015 sous un statut d'association de loi 1901.

Les membres du conseil d'administration

Les membres du Conseil d'administration de la Digital New Deal Foundation sont tous membres fondateurs. Bien qu'issus d'horizons divers, leur prise directe avec la transformation digitale des entreprises et des organisations les rassemble au sein de la fondation. Forts de leur intérêt commun pour les questions numériques, ils ont décidé de prolonger leurs débats en formalisant un cadre de production et de publication au sein duquel la complémentarité de leurs expérience pourra être mise au service du débat public et politique. Ils s'impliquent personnellement dans la vie de la Digital New Deal Foundation.


Olivier **Sichel**


Michel **Combes**


Laurent **Alexandre**


Nicolas **Dufourq**


Alain **Minc**


Yves **Poilane**


Judith **Rochfeld**


Sébastien **Bazin**


Robert **Zarader**