DONNÉES PERSONNELLES : SORTIR DES INJONCTIONS CONTRADICTOIRES

dimanche 13 avril 2014, par Valérie Peugeot

En matière de données numériques, trois vagues médiatiques se sont succédées sous nos yeux en l'espace de moins de 3 ans. La première nous a fait scintiller les merveilles associées aux big data, source inépuisable de nouveaux gisements de richesse de l'économie numérique - déluge de données, nouvel or noir, fin de la science… - l'escalade métaphorique semblait sans fin. La seconde a été liée au coup de tonnerre déclenché par la suite des révélations d'Edward Snowden : en quelques heures, les cris d'alarme négligés des associations de défense des libertés devenaient réalité, en pire. Nul n'avait anticipé l'ampleur et la diversité des données collectées par la NSA. Si big data il y a, ce sont bien celles interceptées et analysées par les autorités américaines, dans une logique de « big surveillance ».
Aujourd'hui, troisième vague, nous voyons se multiplier les articles qui tentent de dégonfler l'enthousiasme exagéré suscité par le projet big data, entre démonstration de l'inexactitude des Google Flue Trendset analyse des biais méthodologiques du big data (iciet là). Mais ces critiques ne disent rien du problème précédent : comment dénouer le lien entre production, analyse de données de masse d'une part et logique de surveillance de l'autre. Car c'est bien de cela qu'il s'agit : plus notre économie inventera des services qui auront besoin de s'appuyer sur de la donnée pour fonctionner – et nous en voyons fleurir tous les jours – plus nous mettrons en place les infrastructures passives qui rendent les logiques de surveillance techniquement possibles, quel que soit le tiers qui décide de s'en servir.

De fait, si les critiques du big data se gardent bien d'attaquer la question de la surveillance c'est que, comme beaucoup, ils se trouvent confrontés à un nœud apparemment gordien : vouloir empêcher le recueil de données, c'est bloquer l'innovation, et donc freiner l'économie numérique. Tous les lobbys qui se pressent à Bruxelles autour de la négociation du nouveau règlement en matière de données personnelles ne disent pas autre chose : ne nous empêchez pas d'innover ! Et en l'état, ils ont raison : tout renforcement de la protection des données personnelles peut apparaître comme un frein à la création de nouveaux services. À moins que nous ne changions radicalement notre manière d'aborder le problème.

Pour commencer, rappelons-nous que de plus en plus de ce qui constitue les big data est et sera de fait des données coproduites par des individus et des services, ce qui signifie que la problématique de la donnée personnelle sera de plus en plus prégnante. Au fur et à mesure que nos objets se mettront à communiquer – compteur, balance, montre, porte d'entrée, voiture etc – nous participeront à cette inflation de la masse de données. Toutes les données ne sont certes pas personnelles (ex : les données météos ne le sont pas), mais de plus en plus de données entreront dans ce régime, ce qui renforce le risque de surveillance.

Face à cela, il nous faut tout d'abord éviter plusieurs impasses.
La première consisterait à rester dans ce que l'on peut qualifier de « faible régime » actuel : de fait nous sommes dans une zone d'incertitude juridique, qui encourage les logiques de « prédation » de la donnée par les plates-formes pour les monétiser, avec des approches plus ou moins délicates (opt in / opt out). Cette situation accule à une vision « innovation contre vie privée », qui pousse le droit, dans une course sans fin, à galoper derrière l'innovation sans jamais être à temps pour protéger les utilisateurs. C'est une approche défensive peu efficace dans une période d'affaiblissement de la puissance publique face aux acteurs du marché. Nous ne pouvons que saluer les dernières prises de position du Parlement européen avec l'adoption en mars dernier du rapport Albrecht concernant le règlement général sur la protection des données, rapport qui rejette les propositions préjudiciables à la vie privée. Mais de fait le rythme du politique et du droit ne sont pas celui de la technologie, et même si le prochain règlement constitue une avancée, il peut en quelques années se révéler impuissant face à de nouveaux dispositifs techniques.

La seconde impasse consisterait à vouloir glisser vers un régime de propriété (intellectuelle et/ ou commerciale) des données par l'utilisateur. Fleurissent actuellement les prises de positions qui vont en ce sens (cf. par exemple la tribune conjointe de Babinet et Bellangerou les prises de position répétées de l'avocat Bensousan). Cette approche me semble à combattre car elle soulève plusieurs problèmes imbriqués :

- un problème de conception politique d'une part : en renvoyant sur l'individu la responsabilité de gérer et protéger ses données, au lieu de trouver des réponses collectives à un problème de société, elle participe d'une vision qui renforce l'individualisme et nie les rapports de force entre les consommateurs et les entreprises
- conséquence du point précédent, surgit un problème très concret : ceci déboucherait sur un renforcement des inégalités entre citoyens numériques, entre ceux en capacité de gérer leurs données, de les protéger, les monétiser, et ceux qui par manque de littératie, de temps, ou toute autre raison, laisserait faire par défaut le marché. Le scénario plausible qui se met en place est celui d'une société numérique dans laquelle les personnes en bas de l'échelle économique et/où culturelle commercialisent leurs données (pas forcément sous forme monétaire, mais en échange de services), pendant que ceux qui disposent de moyens économiques et/où culturels les enferment à double tour numérique. C'est déjà ce qui se met en place (ex : Doodle) ou se profile (ex : YouTube, Apple) avec des services premiums payants sans publicité. Finalement ce choix

entre deux moyens de paiement pour l'accès à un même service (monétisation directe versus attention) ne serait pas un problème en soi si la circulation des données de l'utilisateur ne soulevait pas chaque jour un peu plus des problèmes de vie privée. Sans compter que ce régime n'offre pas de garantie de non traçage à l'image de ce qui se pratique avec le « do not track » (dont l'interprétation par les grands opérateurs publicitaire laisse dubitatif : la collecte de données reste active, certes sans utilisation directe par la publicité sur le navigateur concerné, ce qui n'empêche pas à leurs yeux la revente sur des places de marché de données).

- Ce scénario de la propriété sur les données est poussé par des acteurs qui y voient une opportunité d'affaires plus qu'une sortie par le haut dans une économie numérique en recherche d'équilibre. On voit ainsi apparaître des entreprises qui promettent aux internautes une monétisation directe de leurs données en les louant à des tiers (ex : Yesprofile). Ces acteurs ont pour l'heure un positionnement ambigu : ils promettent simultanément une reprise de contrôle sur les données par l'utilisateur et une source de revenus. S'ils partagent avec les acteurs du VRM (Vendor Relationship Management) le premier objectif, la promesse financière les en démarque. Cette promesse financière semble illusoire, les simulations montrant un taux de retour de quelques euros, mais ce n'est pas la question essentielle. Dans cette approche, la régulation ne passe que par un modèle commercial, entre entités en situation d'asymétrie informationnelle et de rapport de force, ce qui se traduit inévitablement au désavantage du consommateur/utilisateur.
- À l'inverse, si comme nous le pensons, cette monétisation directe des données par les individus génère des revenus anecdotiques, on peut imaginer de voir émerger un autre type d'intermédiaires qui se chargeraient non plus de la commercialisation mais de la « gestion protectrice de données numériques », c'est à dire de la vérification de qui collecte, qui en fait quoi. De la même manière que des entreprises se sont positionnées sur le marché de la réputation et proposent aux internautes des services de « nettoyage » de réputation (ex : RéputationVIP), d'autres pourrons se positionner sur la gestion protectrice. Là encore, certains utilisateurs pourraient se payer les services de ces « gestionnaires de données », pendant que d'autres devraient laisser leurs données circuler au bon vouloir des plates-formes et de leur marché secondaire de la donnée. Nous rebouclons ainsi avec la question des nouvelles inégalités numériques induites par un glissement d'un régime de droit vers un régime de propriété.
- Par ailleurs, scénario du pire, si le choix était fait d'un passage en régime de propriété intellectuelle, cela supposerait, par analogie avec le droit d'auteur ou le brevet, que le droit exclusif de l'individu sur ses données soit temporaire. En effet par définition les régimes de propriété intellectuelle sont des exceptions de monopole concédées à un créateur ou un innovateur, délai au terme duquel les données passeraient dans le domaine public. On voit bien ici qu'un régime de propriété intellectuelle est totalement inapproprié : au bout de quel délai les données sortiraient-elles de la propriété de leur (co)producteur qu'est l'utilisateur ? Au moment où elles n'ont plus de valeur sur le marché de l'économie de l'attention ? De plus le droit d'auteur ne fonctionne que parce qu'il est assorti de nombreuses limites et exceptions pour des usages dits légitimes (recherche, éducation…). Est-ce que l'usage des données serait lui aussi « légitime » quand il est fait sous forme de statistiques agrégées (génomique par exemple ?).
- De plus cela risque de pervertir la logique du droit de propriété intellectuelle : actuellement les informations brutes et les données ne sont pas couvertes ; le droit d'auteur ne concerne que la forme que l'on donne aux informations, et en Europe, le droit sui generis rend propriétaire la cohérence dans une base de données, et non les données elles-mêmes. En élargissant aux données personnelles, on risque de provoquer un glissement général vers une mise sous propriété de toutes les données et informations brutes, ce qui aurait des conséquences sur les données scientifiques, publiques… Très exactement l'inverse de ce que nous défendons avec l'open data, la science ouverte etc.
- Une alternative avancée par certains serait la mise en place de sociétés de gestion des droits sur les données, à l'image des sociétés de gestion de droits d'auteurs. Outre le fait que les sociétés de gestion de droits d'auteurs sont loin d'être la panacée et sont régulièrement critiquées (cf. par exemple JF Bert), cette solution semble totalement irréaliste. Alors que sur les œuvres, les coûts de transaction pour la redistribution des droits aux auteurs sont tels que par exemple 68% des sociétaires de la SACEM ne reçoivent aucune rémunération, on a du mal à imaginer un système de redistribution, même numérique, de quelques euros entre des millions d'utilisateurs.

La troisième fausse piste, réside dans les solutions techniques de type cryptographie

Pour l'heure plusieurs acteurs poussent aux solutions techniques. Il s'agit essentiellement des acteurs institutionnels (cf. les déclarations du premier ministre à l'ANSSI en février) et des acteurs venus des communautés technologiques (IETF, W3C, etc.) dont c'est le métier (cf. les nombreux papiers scientifiquesproposés à la rencontre STRINT de Londres).
Si pour ces derniers, il est cohérent d'aller dans cette direction puisque c'est là que réside leur savoir-faire et leur gagne-pain, il est plus surprenant de voir des acteurs politiques dépolitiser ainsi une question aussi centrale.
• La réponse technique à un problème rendu possible par la technique est une course en avant sans fin, qui tend à éluder le fait que le numérique est un produit éminemment socio-technique. Pas plus que les DRM ne sauvent des industries culturelles qui refusent de prendre la mesure de la profondeur de la mutation à l'œuvre en matière de circulation des œuvres, la cryptographie ou autre solution technique ne saurait être une réponse à une problématique socio-économique.
• Il y aura toujours une technologie capable de défaire la précédente. Jusqu'à présent aucun verrou numérique n'a su résister. De plus, comme le rappelle très justement Snowden « « Le chiffrement fonctionne […]. Malheureusement, la sécurité au point de départ et d'arrivée [d'un courriel] est si dramatiquement faible que la NSA arrive très souvent à la contourner. » Et rappelons-nous que la NSA (ou ses consœurs) installe des backdoors dans les logiciels de chiffrement eux-mêmes.

Alors que pouvons-nous envisager pour nous prémunir de la société de surveillance tout en continuant à créer, inventer ? Voici quatre pistes, qui sont autant d'invitations à débattre.

La première piste consiste à orienter l'économie numérique le plus loin possible de l'économie de l'attention pour revenir à une économie servicielle. Aujourd'hui l'économie du Web repose en très grande partie sur une monétisation de « notre temps de

cerveau disponible » via de la publicité pour nous inciter à consommer. Google, Facebook, Twitter, et même Amazon qui pourtant commercialise des biens, vivent sur des marchés dits bifaces ou multifaces : d'une main ils offrent un service non monétisé (moteur de recherche, microblogging, réseau social…), de l'autre ils revendent les traces de leurs utilisateurs soit en direct à des annonceurs, soit via des places de marché de la donnée sur lesquelles opèrent des data brokers. Parmi les plus gros opérateurs aux États-Unis on peut citer Axicom, dont on estime qu'elle dispose d'environ 1500 informations sur 200 millions d'américains ou encore Epsilon, BlueKai, V12 Group, Datalogix. Ce déport d'une part croissante de l'économie semble sans fin : un jour c'est un banquier qui émet l'idée de ne plus faire payer les frais de carte bancaire aux clients en échange d'un droit de réutilisation de leurs données ; demain ce sera un organisateur de concert qui vendra des entrées à bas prix en échange d'un accès aux données du spectateur, etc. En raisonnant par l'extrême, si des secteurs entiers de l'économie pré numérique se mettent à basculer vers cette illusion du gratuit et à commercialiser de la donnée en sus et place d'un bien ou d'un service, à qui les data brokers revendront-ils leurs données ? Cette information ne perdra-t-elle pas progressivement de la valeur au fur et à mesure que des pans entiers de l'économie basculeront vers des marchés bifaces basés sur l'attention ?
Sans aller jusqu'à cet extrême, il nous faut aujourd'hui inverser trois choses : sortir de l'illusion que ce qui est gratuit pour le consommateur est bon pour lui ; revenir autant que faire se peut à de la commercialisation de services, ce qui participe à désenfler la tentation de captation des données personnelles (en ce sens, les services dits d'économie collaborative, en se rémunérant pour la plupart par un pourcentage sur la prestation sur le covoiturage, sur l'hébergement…, au lieu de pratiquer l'illusion de la gratuité assortie de publicité, participent à une forme d'assainissement de l'économie numérique) ; encadrer très fortement les marchés de data brokers, qui sont aujourd'hui totalement opaques et non régulés. Le marketing prédictif est le meilleur ami de la surveillance car il recueille et traite les données toujours plus fines sur l'individu qui rendent cette dernière techniquement possible. Tout ce qui peut contribuer à affaiblir ce marché est bon pour notre société et les libertés individuelles.

Plus généralement, une régulation du marché des données, si l'on considère la transparence comme élément d'un contrôle social de l'usage des données, peut passer par une obligation de documentation technique très forte – quelles données collectées, où sont-elles stockées, combien de temps sont-elles conservées, … ? –. Cette documentation serait le support à l'intervention d'un corps d'inspecteurs des données, dont les prérogatives iraient bien au-delà de celles de la CNIL. C'est, dans un tout autre domaine, ce qui vient d'être fait par la justice américaine, qui a condamné Apple à être surveillé pendant 2 ans, suite à des pratiques d'entente illicite sur les livres numériques. Le principe met toutes les entreprises à égalité puisque celles-ci ont la responsabilité d'appliquer par défaut le bundle of rights, mais peuvent être soumises à des audits aléatoires.

La seconde piste est certes technique, mais à l'opposé de la cryptographie, va chercher du côté des infrastructures ouvertes et libres (au sens logiciel du terme). Il s'agit, première brique, autant que possible d'utiliser des logiciels libres car ils assurent une surveillance horizontale par les communautés de ce que fait et comment peut être utilisé un logiciel, comme le rappel l'APRIL dans sa tribune dans Libération du 25 février 2014. La transparence du logiciel libre et sa capacité d'appropriation par d'autres que ses concepteurs initiaux en fait une brique d'une reconstruction d'une relation de confiance entre l'utilisateur et un logiciel. Mais au-delà des logiciels, ce sont aussi les normes qui doivent être pensées sur un modèle ouvert, pour qu'elles ne deviennent pas de nouvelles boites noires génératrices d'insécurité sur les données (en laissant une poignée d'acteurs nord-américains prendre le leadership de cette normalisation, nous n'en prenons pas le chemin). Ceci est particulièrement vrai pour les normes encore à construire pour l'internet des objets. Si nous laissons s'installer des standards propriétaires, nous donnons le fer pour nous faire battre. On peut aller plus loin en suivant les pistes de Van Kranenburg dans son rapport sur l'internet des objets où il propose d'aller vers des infrastructures globales ouvertes, depuis le RFID jusqu'au GPS (page 50 du rapport). Sur la base de ces infrastructures on peut alors imaginer des outils de gestion de sa vie privée comme ce RFID Guardian, imaginé par Melanie Rieback (page 49 du rapport) qui permet de régler l'usage du RFID quand on circule dans un environnement connecté (supermarché, ville…). Il s'agit enfin et surtout pour protéger nos données personnelles, de construire des infrastructures de management de ces données qui redonnent la main et le contrôle à l'utilisateur, infrastructures que certains appellent les PIMS – Personal information mangement systems, à l'instar de ce que développe une entreprise comme Cozy cloud.

La troisième piste, qui déborde le cadre stricte des données personnelles pour s'intéresser aux données numériques en général, consiste, en s'inspirant des travaux d'Elinor Ostrom et de l'école de Bloomington autour des biens communs, à développer une sphère de données en Communs, c'est-à-dire de données qui peuvent être considérées comme une ressource collective, et qui n'entrent ni dans le régime des biens gérés par la puissance publique strico sensu, ni dans un régime de marché.
Ce régime de Communs repose sur une gestion par une communauté de la ressource considérée, qui organise ses règles de gouvernance, en s'appuyant sur un « faisceau de droits » (bundle of rights »). Ces faisceaux de droits rendent possibles des régimes de propriété partagée. Un faisceau de droits c'est un ensemble de relations sociales codifiées autour de quelque chose à protéger comme le rappelle Silvère Mercier. Ils permettent de penser les usages indépendamment de la notion de « propriété », et d'adapter les règles de droit pour servir au mieux les usages en protégeant les ressources mises en partage. La grande force des Communs est d'ouvrir une troisième voix à côté de la propriété privée et de la propriété publique, un espace dans lequel des ressources, ici des données, ne sont pas soumises à un régime de droits exclusifs, mais peuvent être réutilisées selon certaines conditions fixées par la communauté qui en a la gestion et qui veille à leur protection. Il ouvre un espace protégé dans lequel les individus et les collectifs peuvent choisir de placer leurs données.

Ces ressources sont ainsi soustraites au marché *stricto sensu* et aux logiques oligopolistiques qui sous-tendent le capitalisme que nous connaissons dans sa forme actuelle. Ce qui ne signifie pas que des porosités n'existent pas avec le marché ou que les Communs se font contre le marché. Les deux peuvent non seulement cohabiter mais également se compléter. Ainsi Flickr, plateforme de partage de photos, filiale de Yahoo !, héberge des photos placées par des internautes en régime de Communs via une licence Creative Commons, de même que des fonds d'archives photographiques du domaine public placées là par des institutions publiques (musées, bibliothèques…).
De même ces ressources échappent au régime de pure administration publique qui laisse reposer l'entière responsabilité de leur

gestion et de leur protection sur les épaules de la puissance publique. Les Communs impliquent une co-responsabilité de la part des acteurs qui en assurent la gouvernance, permettant ainsi un glissement de logiques purement délégatives à des approches plus contributives. De la même manière que pour le marché, sphère publique et Communs n'ont pas vocation à s'opposer mais à se compléter. Ainsi lorsqu'une communauté d'habitants en Bretagne décide de mettre en place et d'autofinancer en crowdfunding une éolienne sur leur territoire pour assurer une fourniture d'énergie autonome et durable au village, tout en utilisant un terrain de la municipalité, le Commun est coproduit par cette dernière et par les habitants, et se réalise en partenariat avec les entreprises privées qui vont construire l'éolienne et gérer les flux électriques sur les réseaux, sous le contrôle des citoyens qui auront financé le projet.

Pour éviter que l'ensemble des données ne soient aspirées dans cette course à la marchandisation de la donnée et favorise ainsi une société de surveillance, il est essentiel qu'une sphère de données « en Communs » puisse fleurir, s'enrichir et être protégée contre des tentatives d'enclosures.

L'existence de cette sphère de données en Communs présente plusieurs avantages : elle constitue un gisement d'informations dans laquelle d'autres acteurs extérieurs à la communauté des producteurs peuvent puiser pour créer, innover, proposer d'autres services ; elle permet de tirer parti des spécificités contributives du monde numérique

Quelles données pourraient appartenir à cette sphère des communs ?
Trois catégories semblent possibles en premier regard :

- Des données produites par la sphère publique et partagées en open data, sous réserve qu'elles soient assorties d'une licence de partage à l'identique (share alike). C'est déjà le cas de la licence choisie par un grand nombre de collectivités locales mais à notre grand regret pas par Etalab, ce qui veut dire que ces données peuvent être à nouveau « encloses ». Les données produites pas la puissance publique avec l'argent public doivent rester libres de réutilisation.
- La seconde catégorie est constituée des données produites par les individus qui désirent placer ces ressources en bien commun. C'est déjà le cas des données produites dans OpenStreetMap, dans Wikipédia, qui de fait constituent une œuvre collective, pour lesquelles les communautés ont choisi un régime juridique qui protège les ressources en biens communs. Sur Wikipédia la communauté a fait le choix de deux licences compatibles, la licence CC by-sa et la licence de documentation libre GNU, qui dans les deux cas contiennent cette obligation du partage aux mêmes conditions.
- Dans une moindre mesure, des données produites par des entreprises pour les besoins de leur activité – un catalogue de magasin, une liste de point de vente, un taux de fréquentation de ses magasins – et qui choisissent de les mettre à disposition de tiers dans une logique écosystémique. C'est ce qu'ont commencé à faire la SNCF ou La Poste, qui expérimentent autour de l'open data. Je dis dans une moindre mesure, car les données des entreprises peuvent à tout moment être ré-enfermées (ex : via une fermeture d'API comme l'a fait Twitter) et ne font pas l'objet d'une gouvernance collective, mais d'une gouvernance privée par l'entreprise qui décide de les mettre à disposition. On peut craindre, comme cela s'est déjà passé pour d'autres services numériques, qu'une fois l'écosystème constitué, les données ne redeviennent privées, l'ouverture ne constituant alors qu'une phase transitoire, un « produit d'appel ».

La quatrième piste, proche dans sa source d'inspiration de la précédente, consiste à imaginer une gestion des données personnelles par un régime de « bundle of rights ». Le Bundle of rights, ou « faisceaux de droits » puise à un courant juridique qui a émergé aux États-Unis au début du XXe siècle et qui trouve ses racines dans la pensée juridique américain dite du « legal realism » (ou réalisme juridique) qui conçoit la propriété comme un ensemble complexe de relations légales entre des personnes, ainsi que l'explique Fabienne Orsi. Cette approche par le « faisceau de droits » permet, autour d'une même ressource matérielle ou immatérielle, d'identifier différents droits : ex : droit de posséder, d'utiliser, de gérer, de monétiser, de transmettre, de modifier… Cette approche est un des piliers de la pensée des Communs.

Appliqués aux données produites sur le web par les actions des individus, les faisceaux ou bouquets de droits permettraient d'imaginer trois ensembles de droits :

- Certains usages assortis de droits sont garantis par défaut à l'utilisateur, comme par exemple, le droit de savoir ce que l'on collecte sur lui ; le droit de rectification de ses données ; le droit à la portabilité des données ; le droit de placer ses données en Communs (cf. supra).
- D'autres usages peuvent être à l'inverse garantis à la plate-forme, au producteur du service, comme par exemple le droit de gestion pour une amélioration de la relation client ;
- Enfin, les usages intermédiaires qui sont ceux qui dégagent le plus de valeur d'usage à la fois pour l'entreprise et pour l'individu (ex : le graphe social) peuvent quant à eux faire l'objet d'un usage par l'entreprise sous deux régimes possibles :
    - Une ouverture de la donnée individuelle à un tiers sur base d'une autorisation explicite de la part de l'individu coproducteur, en échange d'un service ex : j'autorise une marque d'électroménager à accéder à mes données pour me proposer une machine à laver qui correspond à mes besoins, dans une approche dite VRM – Vendor relationship management. Cette approche fait l'objet d'une expérimentation à travers le projet MesInfos, porté par la FING.
    - Une ouverture de la donnée agrégée et anonymisée à des tiers sous condition de partage limité dans le temps. Sur une très courte période, quand la donnée est « chaude », la plateforme aurait le droit de monétiser celle-ci agrégée à d'autres, mais à l'expiration de cette période, la donnée ne pourrait plus être mobilisée directement ou indirectement par la plateforme productrice. La donnée devrait alors soit être détruite (pas de possibilité de stockage) soit être transférée vers un espace de type cloud personnel où l'individu pourrait la conserver s'il la juge utile, voire la partager s'il le souhaite.

Cette approche par une discrimination à la fois temporelle des droits (donnée chaude, droits d'usage à l'entreprise, donnée froide,

exclusivité de l'usager) et spatiale (stockage dans la plateforme, stockage dans un espace contrôlé par l'individu) pourrait ouvrir la voir à un bundle of rights positif, c'est-à-dire à la fois protecteur pour l'individu et en même temps ne tuant pas d'entrée de jeu le modèle d'affaires des entreprises du web qui proposent des services (hors marketing) construits autour de la donnée (ex : trouver un vélib).

Enfin, de façon encore plus prospective, pour aller plus loin dans la réflexion, nous ne voulons pas placer ce régime d'usage sous le signe de la propriété partagée mais sous celui d'un nouveau « droit du travail contributif ».
En 1936 Jean Zay avait défendu dans une loiqui n'a pas pu voir le jour à cause d'une opposition des éditeurs puis de l'explosion de la Seconde guerre mondiale, une conception du droit d'auteur basée non pas sur un régime de propriété intellectuelle mais sur la reconnaissance du travail accompli. Cette approche avait pour objectif de protéger les créateurs tout en défendant le domaine public, source de renouvellement créatif dans lequel puisent les nouvelles générations d'artistes (domaine public que l'on peut considérer comme l'une des composantes d'une sphère des Communs). En considérant l'auteur non plus comme un propriétaire, mais comme un travailleur, cette approche permettait à Jean Zay de dissocier les droits des descendants sur d'une part le droit moral à longue durée, et d'autre part sur les droits patrimoniaux pour lesquels il séparait (forme de bundle of rights) le droit à percevoir des revenus par les ayant-droits, qui devaient durer jusqu'à ce que l'œuvre entre dans le domaine public, de l'existence d'un monopole sur l'usage de l'œuvre, qui pour sa part était limité à dix ans après le décès de l'auteur, permettant ainsi aux œuvres de faire l'objet de nouvelles exploitations rapidement.

Dans le cas qui nous occupe, si l'on accepte les hypothèses suivantes :

- que le Web des données est le fruit du labeur conjoint des plates-formes et des utilisateurs, comme c'est affirmé entre autres dans le rapport Colin et Collin ;
- que le travail est en train de muter profondément à l'heure du numérique, effaçant la frontière entre amateur et professionnel ;
- que les travailleurs vivant hors du système classique du salariat vont se massifier
  …alors nous devons inventer ce droit du travail contributif qui pourrait s'appuyer sur un bundle of rights adapté à la nouvelle situation.

*****

Refus de la propriétarisation de la donnée, déplacement du capitalisme informationnel vers une économie servicielle, montée en puissance des infrastructures ouvertes de recueil et traitement des données personnelles, développement d'une sphère des données en régime de Communs, construction d'un droit des données personnelles appuyé sur un « faisceau de droits d'usage »… Chacune de ces pistes vise à empêcher la construction d'une société de surveillance. Certaines sont déjà en cours d'exploration. A nous de multiplier les recherches et de faire se rencontrer les acteurs qui œuvrent à une sortie par le haut de la société des données de masse. Pour que données puisse rimer avec libertés.
