L'instauration de droits de propriété sur les données personnelles : une légitimité économique contestable

Granting property rights to personal data: An economic dead-end

Arnaud Anciaux, Joëlle Farchy et Cécile Méadel

Édition électronique

URL : <https://journals.openedition.org/rei/6540>

DOI : 10.4000/rei.6540

ISSN : 1773-0198

Éditeur

De Boeck Supérieur

Édition imprimée

Date de publication : 15 juin 2017

Pagination : 9-41

ISBN : 9782807391420

ISSN : 0154-3229

Référence électronique

Arnaud Anciaux, Joëlle Farchy et Cécile Méadel, « L'instauration de droits de propriété sur les données personnelles : une légitimité économique contestable », *Revue d'économie industrielle* [En ligne], 158 | 2e trimestre 2017, mis en ligne le 15 juin 2019, consulté le 02 juin 2022. URL : <http://journals.openedition.org/rei/6540> ; DOI : <https://doi.org/10.4000/rei.6540>

L'INSTAURATION DE DROITS DE PROPRIÉTÉ SUR LES DONNÉES PERSONNELLES : UNE LÉGITIMITÉ ÉCONOMIQUE CONTESTABLE

Arnaud Anciaux, Université Laval, Centre de recherche interuniversitaire
sur la communication, l'information et la société

Joëlle Farchy, Université Paris 1, Centre d'économie de la Sorbonne

Cécile Méadel, Université Paris 2, Centre d'analyse et de recherche
interdisciplinaire sur les médias

Mots clés : données personnelles, droits de propriété, économie numérique, plateformes numériques, économie du droit.

Keywords: personal data, property rights, digital economy, online platforms, law and economics.

Pas un jour désormais sans que de nombreux observateurs ou médias ne vantent les potentialités du « big data » ou ne s'alarment de ses dangers supposés. Le big data est d'abord le croisement entre deux dynamiques techniques : une production brute de données de plus en plus massive, disséminée dans des dispositifs décentralisés ou concentrés, et générée par des acteurs individuels et collectifs toujours plus nombreux ; une capacité de recueil, traitement, croisements et analyse accessible à différents acteurs issus de mondes différents et parfois séparés (entreprise commerciale, administration publique, recherche scientifique, etc.). Ces données, informations et contenus font l'objet d'un intérêt grandissant de la part de divers acteurs pour accroître leur productivité, leur compétitivité et doper la croissance économique. Au-delà des potentialités techniques, le big data fait en effet apparaître l'émergence d'une troisième révolution industrielle liée à l'informatique et aux réseaux numériques.

Si la triple activité (recueil, traitement et valorisation des données) est visée par un grand nombre d'acteurs, toutes les données n'ont pas la même valeur économique ou ne renvoient pas aux mêmes enjeux sociaux et toutes les organisations ne les utilisent pas de la même manière. Dans le cadre de cet article, nous limiterons la réflexion aux données personnelles exploitées par les « plateformes » du numérique¹. Fragile équilibre, la protection des données personnelles, ou plus exactement celle du caractère personnel des données, est-elle compatible avec le développement économique ? Le régime français adopté en 1978 avec la loi dite informatique et libertés et la création de la Commission nationale de l'informatique et des libertés (CNIL) s'est avant tout construit autour d'une volonté de protection des personnes, de leurs droits fondamentaux et de leur vie privée, et non dans une logique patrimoniale. Créé dans un contexte où il s'agissait surtout de protéger les citoyens de la collecte de données par les administrations et de leur fichage, il doit s'adapter désormais à l'essor de pratiques marchandes et à la volonté des acteurs qui souhaitent construire tout ou partie de leur activité économique autour de l'exploitation de ces données personnelles. Des tensions sont inévitables².

Quels formes et régimes peuvent désormais accompagner et encadrer les données et leurs traitements pour préserver les libertés fondamentales des individus sans pour autant porter atteinte au dynamisme économique des organisations ? Pour amorcer des réponses à cette vaste interrogation, nous verrons dans un premier temps comment les données personnelles sont désormais au cœur des modèles économiques de marchés à plusieurs versants, dominants dans les activités des plateformes numériques. Nous tenterons ensuite de comprendre, dans une perspective de « *law and economics* », les enjeux économiques d'une logique de droit de propriété sur les données personnelles. Nous avancerons que cette possibilité, envisagée par ses promoteurs pour protéger les internautes, est marquée par certaines incohérences ou incompréhensions, et qu'elle ne manquerait pas de

1 Nous ne traiterons pas non plus de l'importante question de l'ouverture des données publiques qui, si elles peuvent faire l'objet de traitements spécifiques de la part des plateformes et être valorisées, n'emportent pas les mêmes questionnements vis-à-vis des individus.

2 Ainsi par exemple de la décision remarquée de la Cour de cassation, qui a estimé qu'un fichier de clientèle non déclaré à la CNIL est hors commerce et ne peut être cédé. COUR DE CASSATION, Cass. com., 25 juin 2013, 12-17.037.

produire des effets éloignés de ceux recherchés. C'est pourquoi nous proposerons dans une dernière partie des pistes pour construire un marché des données personnelles respectueux de la vie privée.

1. LES DONNÉES PERSONNELLES AU CŒUR DES MODÈLES ÉCONOMIQUES DE MARCHÉS MULTI-VERSANTS

Au sein de l'Union européenne, le règlement 2016/679³, applicable à compter du 25 mai 2018, encadre le traitement de ces données, c'est-à-dire leur collecte et leur exploitation, en retenant une définition de la « donnée à caractère personnel » comme étant :

toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale⁴.

Le champ d'acception des données personnelles conduit ainsi à inclure des informations nominatives, mais également plus largement celles qui peuvent permettre d'identifier les individus (comprenant en cela la date de naissance, le sexe, la profession, les adresses postales par exemple, ou encore les adresses IP⁵), sans que ces délimitations ne connaissent nécessairement une définition arrêtée. L'identifiabilité⁶ peut théoriquement

3 Remplaçant la Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, adoptée le 24 octobre 1995, et une partie de ses différentes transpositions nationales.

4 Art. 4, Règlement 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données).

5 COUR DE JUSTICE DE L'UNION EUROPÉENNE, 3^e chambre, 24 novembre 2011, C-70/10 Scarlet Extended SA c/ Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM).

6 Art. 2, Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés, 6 janvier 1978.

concerner toute donnée attachée à une personne, même anonymisée *a posteriori* (Conseil d'État, 2014, p. 165 et s.), ou faisant l'objet d'une pseudonymisation⁷. Ainsi, seul un anonymat *ab initio* pourrait être séparé du champ des données personnelles – et constituer en ce sens un marché particulier, pouvant favoriser l'émergence d'acteurs économiques spécialisés et de nouvelles valorisations (Lemoine, 2014, pp. 135-137).

Par ailleurs, au niveau européen, le G29⁸ a fourni une acception relativement large des données personnelles, retenant ainsi des renseignements objectifs (particularité sanguine, donnée biométrique, frappe sur un clavier, élocution, etc.) et subjectifs (fiabilité d'une personne, de ses finances, de son travail).

Cela signifie que tant les informations objectives que subjectives concernant une personne, à quelque titre que ce soit, peuvent être considérées comme « données à caractère personnel », indépendamment du support technique sur lequel elles se trouvent. [...] Dans son avis, le groupe de travail avance trois autres éléments – le contenu, la finalité ou le résultat – pour déterminer si les informations « concernent » une personne physique. Ils s'appliquent également aux informations susceptibles d'avoir une influence manifeste sur la manière dont une personne physique est traitée ou évaluée⁹.

Si le type de données, matières premières ou territoires à conquérir demeure encore ouvert, leur intérêt économique pour les plateformes apparaît aujourd'hui bien assuré.

7 Considérants 26 et s., Règlement 2016/679 précité.

8 Groupe de travail rassemblant des représentants de différentes autorités indépendantes de protection des données, mis en place par l'art. 29 de la directive précitée, et qui doit être remplacé par un Comité européen de la protection des données, tel que prévu par l'art. 68 du Règlement 2016/679 précité.

9 GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, 20 juin 2007, Avis 4/2007 sur le concept de données à caractère personnel. Cette position a été maintenue par la suite, notamment au travers de plusieurs avis : GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, 4 avril 2008, Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche ; GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, 22 juin 2010, Avis 2/2010 sur la publicité comportementale en ligne. Elle a été également reprise dans le rapport du CONSEIL D'ÉTAT précité.

1.1. De nouveaux modèles économiques

Le terme de « plateforme » du numérique est assez large pour regrouper en réalité un grand nombre d'acteurs (Conseil national du numérique, 2014).

Une première acception couvrirait notamment les « écosystèmes d'applications », les sites de partage de contenus et la place de marché, bref tous les sites qui permettent à des tiers de proposer des contenus, des services ou des biens ; une seconde acception, plus large, [...] couvrirait également tous les sites qui servent de point de passage pour accéder à d'autres contenus, notamment les moteurs de recherche, les agrégateurs ou les comparateurs de prix. Tous ces sites ont en commun d'être des portes d'entrée, soit pour l'expression des internautes, soit pour l'accès des internautes à d'autres biens et services, soit les deux (Conseil d'État, 2014, pp. 215-126).

Ces acteurs, très diversifiés, organisent la fourniture de services, en ne demandant aucun paiement au consommateur ou, parfois, seulement d'un montant relativement limité¹⁰. Ils financent principalement leur activité par la vente de biens et services auprès d'autres acteurs, intéressés par la présence des consommateurs sur la plateforme, suivant ainsi un modèle de marché à deux ou plusieurs versants (Evans, 2003 ; Rochet et Tirole, 2003 ; Jullien, 2004 ; Armstrong, 2006 ; Hagiu et Wright, 2011). Rappelant en partie le modèle du financement publicitaire des médias et du journalisme (Gabszewicz et Sonnac, 2010), le financement repose en partie sur cette logique tout en s'appuyant sur des interrelations plus dynamiques entre les différents versants et la plateforme. Les marchés multi-versants sont en effet caractérisés par des externalités de réseau intergroupes : l'utilité d'un agent économique qui appartient à un groupe donné ne dépend pas seulement du nombre de membres de ce groupe mais aussi du nombre d'agents appartenant à un autre groupe.

¹⁰ La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique a plus récemment précisé, en son art. 49, la qualité d'opérateur de plateforme en ligne : « toute personne physique ou morale proposant, à titre professionnel, de manière rémunérée ou non, un service de communication au public en ligne reposant sur : 1^{er} Le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers ; 2^e ou la mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service. »

Cette caractéristique a des conséquences sur la formation des prix, puisqu'elle peut conduire à subventionner le versant de la demande pour laquelle l'élasticité prix est la plus forte ou suscite le plus d'externalités afin d'attirer des utilisateurs sur l'autre versant (Perrot, 2011). Dans le cas d'une subvention totale, les services rendus sur un versant du marché sont proposés gratuitement au consommateur. Le numérique a permis le développement à grande échelle de modèles de « gratuité marchande » dans lesquels la gratuité des services offerts aux internautes n'est nullement incompatible avec l'activité hautement profitable d'entreprises commerciales dont les GAFAM^{II} sont le symbole le plus éclatant (Acquisti, 2011 ; Farchy, Méadel et Sire, 2015 ; Smyrnaio, 2017). Dans ce modèle, la gratuité des services en ligne a pour contrepartie – certes peu visible – la collecte et l'exploitation de données obtenues grâce aux contributions, conscientes ou non, volontaires ou non, des internautes. En effet, le consommateur consent – ou est supposé consentir – au recueil d'un certain nombre d'informations. Celles-ci peuvent être traitées par la plateforme afin d'améliorer ses services, que ceux-ci soient mis à disposition des consommateurs ou qu'ils soient destinés à l'autre versant du marché, le plus souvent des annonceurs souhaitant toucher les consommateurs de la manière la plus fine et efficace possible. Les données peuvent également, dans certains cas, être directement transmises, vendues à d'autres acteurs, annonceurs ou intermédiaires de données (*data brokers*).

Dans ce cadre, les plateformes numériques peuvent développer leur modèle d'affaires sur un ou plusieurs versants (Brousseau et Pénard, 2007). Néanmoins, les conséquences à l'échelle du marché sont encore discutées. Ainsi, certains voient dans l'acquisition des données une composante essentielle de logiques de concentration et de domination du marché ; la maîtrise croissante des informations fournit à la fois une ressource financière et une connaissance précise sur le marché et sur les consommateurs, formant une barrière à l'entrée de plus en plus forte (Newman, 2014). Au contraire, certains contestent cette logique en soulignant qu'elle semble plus fondée théoriquement qu'empiriquement ; les données, si elles peuvent faire l'objet de nombreuses valorisations, ne sont que rarement l'objet d'une exclusivité dont bénéficierait un seul acteur économique (Lerner, 2014).

II Acronyme regroupant Google, Amazon, Facebook, Apple et Microsoft, bien que chacune de ces entreprises développe des modèles d'affaires distincts.

1.2. L'exploitation de données personnelles, un contrat faustien

Les internautes ont, quant à eux, un rapport paradoxal à la protection, ce que résume l'idée du *privacy paradox* fondée sur l'opposition apparente entre les déclarations de nombreux internautes valorisant leur vie privée, souhaitant conserver le contrôle de leurs données, et la promptitude avec laquelle ils y renoncent, par leurs actions autant que leurs inactions, en révélant toujours plus d'informations.

Une sorte de « contrat faustien » semble passé entre l'internaute et les entreprises. Le traitement et l'exploitation, voire la transmission des données obtenues sur les utilisateurs des plateformes, permettent aux entreprises à la fois d'améliorer leurs services, afin de conserver leur position centrale sur les marchés, mais aussi de fournir un grand nombre d'informations à de potentiels annonceurs cherchant à toucher les internautes consommateurs. Cet équilibre est souvent présenté comme la contrepartie de la mise à disposition gratuite des services des plateformes auprès des internautes, et mettant ces derniers aux prises avec les enjeux d'une « gratification immédiate » (Acquisti, 2011).

Alain Rallet et Fabrice Rochelandet (2011) soulignent que les individus ne mobilisent pas toujours les droits qui leur sont offerts non seulement parce qu'ils ne disposent pas nécessairement d'une information suffisante sur ces droits, qu'ils ne possèdent pas les compétences mais surtout parce qu'ils ne bénéficient pas d'incitations pour le faire ; arbitrant entre ces coûts et l'utilité immédiate des services qui leur sont proposés, les individus ont une forte propension à ne pas contrôler le respect de leurs droits.

Le *privacy paradox* est ainsi expliqué par la faculté des individus à renoncer à la vie privée en échange de services, d'avantages en nature, de suppressions de publicités voire de contreparties financières (Norberg et al., 2007 ; Lancelot et Miltgen, 2011). Le « travail » gratuit des internautes (voir *infra*) prend la forme d'une externalité au profit des entreprises qui elles-mêmes fournissent des services gratuits aux internautes. Le « contrat faustien » peut donc être lu en termes économiques comme un jeu d'externalités croisées entre internautes et plateformes conduisant à des interprétations différentes sur la nature du gain de chacun.

Sur le plan juridique, les questionnements autour de la nature des informations ne sont pas nouveaux. Avec l'informatisation progressive de la société, et surtout avec le développement rapide des réseaux numériques à compter du début des années 1990, les juristes se sont progressivement emparés du sujet engageant une réflexion sur l'opportunité de l'instauration de droits de propriété sur les données personnelles. Nous en présentons le principe avant d'interroger la légitimité économique d'une telle démarche.

2. UN DROIT DE PROPRIÉTÉ ENVISAGÉ POUR PROTÉGER LES INTERNAUTES

L'idée d'un droit de propriété est fréquemment évoquée, notamment au travers d'une « appropriation de l'information personnelle », concept permettant à tout citoyen d'être « propriétaire des droits d'exploitation commerciale des renseignements le concernant » (Mallet-Poujol, 1997)¹². Avec l'essor des données personnelles et de leurs traitements à partir des années 2000, cette idée a été réaffirmée par un certain nombre d'acteurs en France. L'argument principalement mis en avant repose sur une protection des acteurs individuels qui serait, par ce biais, accrue :

En pratique, ces droits [d'accès, de rectification...] sont très rarement exercés, malgré leur gratuité. Cette situation, qui perdure depuis plus de trente ans, illustre le déficit pédagogique de la loi, la complexité des droits et l'absence de respect de l'obligation d'information. [...] Pour sortir de cet écueil, il suffirait de mettre en perspective les risques avec le droit, en reconnaissant un droit de propriété des individus sur leurs données personnelles. À l'ère de l'Internet, les données sont des biens incorporels dont la propriété permettrait, par analogie aux biens « moléculaires », d'organiser la protection et les modalités de détention et d'échanges de toute nature, sous réserve du respect des règles d'ordre public. (Bensoussan, 2010)

¹² Reprenant Hunter et Rule, *Vers un droit de propriété des renseignements personnels*, l'auteur conteste cependant cette proposition : « La démarche est légitime en ce qu'elle a pour objectif d'assurer un droit de contrôle de la diffusion commerciale de ses données. Elle n'en demeure pas moins excessivement dangereuse sur le plan des principes. » N. Mallet-Poujol (1997) défend cependant la consolidation d'un droit de la personne sur ses informations « dans le même esprit que le droit à l'image ». On pourra d'ailleurs noter une certaine constance argumentative, chez de nombreux analystes et juristes français s'intéressant aux données personnelles, consistant à évoquer un possible droit de propriété sans y être pour autant particulièrement favorable.

Cette idée se retrouve également dans les propositions mises en avant par Pierre Bellanger (2014, pp. 202-203) :

L'appropriation par les individus eux-mêmes des données informatiques qu'ils génèrent leur donne la possibilité d'en recueillir la valeur, de les utiliser, d'en interdire l'usage, de les céder ou de les détruire. Dès lors que les données sont un bien attribué au citoyen qui en est à l'origine, il reprend le pouvoir et il en décide librement de l'usage dans les limites du droit. Ces limites à définir associeront les doctrines de la propriété de soi-même (le don du sang) [sic !] à la propriété intellectuelle (le droit d'auteur).

Ces propositions visent ainsi principalement une volonté de protection des individus, en cherchant à leur attribuer une forme de responsabilisation (au sens moral) sur leurs données, ainsi qu'une éventuelle possible gestion de nature patrimoniale. La création et la reconnaissance de marchés dédiés avec l'appui de diverses « solutions » technologiques pouvaient ainsi être envisagées dès les premières années du web grand public :

Today, the cost of invading individual privacy is far lower than the true social cost of invading that privacy. While market-based approaches cannot solve all our privacy problems, they can help strengthen individual control over personal information while strengthening (not replacing) the legal foundations of privacy protection. In the end, privacy should be easily achieved, and there should be as much use of private personal information for commercial purposes as is socially efficient. Today, personal privacy is expensive and in short supply, while the use of personal information is wasteful and inefficient. (Laudon, 1996, p. 93)

L'encadrement juridique existe déjà en partie pour les bases de données, au travers d'une double protection, droit d'auteur et droit *sui generis*, ce dernier étant bien spécifiquement attribué au producteur « qui prend l'initiative et le risque des investissements correspondants » et donc « bénéficie d'une protection du contenu de la base lorsque la constitution, la vérification ou la présentation de celui-ci atteste d'un investissement financier, matériel ou humain substantiel »¹³. Si le processus industriel de constitution de la base fait l'objet d'une protection, la qualification juridique de chaque donnée de la base reste en question. Aussi, à l'instar

¹³ Art. L341-I, Code de la propriété intellectuelle.

de la suggestion de Bellanger, plusieurs propositions se rapprochent des approches bien connues en termes de propriété intellectuelle :

Concernant la donnée brute, on peut s'interroger sur la reconnaissance éventuelle d'un droit de propriété [...] ou de la consécration d'un droit fondamental sur la donnée à caractère personnel. [...] Une alternative pourrait consister à préconiser la transposition du modèle propre au droit de propriété intellectuelle en distinguant, en faveur de l'utilisateur, la reconnaissance d'un droit patrimonial cessible et d'un droit de la personnalité pour sa part incessible. (Bensamoun et Zolynski, 2014)

Le rapprochement avec le régime de la propriété intellectuelle a également été effectué dans le contexte américain (Zittrain, 2000). Ce lien a cependant été contesté (voir notamment Samuelson, 2000) en raison des différences notables dans les objectifs et objets visés. Le questionnement sur le droit de propriété est par ailleurs marqué par une certaine différenciation entre les logiques européennes et américaines, la dernière inscrivant davantage les données personnelles dans une logique de propriété. L'aliénabilité, presque consubstantielle au droit de propriété, est cependant questionnée, puisque paraissant non souhaitable dans une visée de protection des données personnelles et des individus concernés. Une législation générale dans le contexte américain a également été présentée comme une solution trop peu réaliste¹⁴, au profit d'un recours aux actions en réparation des dommages¹⁵ causés aux individus (Litman, 2000), rejoignant les interrogations liées aux difficultés d'évaluation par les individus de la valeur des données les concernant autant que des conséquences possibles de leur circulation (Schwartz, 2004). Il n'existe ainsi pas de règle générale sur les données personnelles aux États-Unis, mais seulement des réglementations sectorielles limitées, se concentrant par exemple sur l'absence de conditions frauduleuses (Rochelandet, 2010, pp. 90-91), ou le nécessaire consentement des consommateurs à l'utilisation et la revente de données personnelles par les fournisseurs d'accès à Internet (mis en place par la *Federal Communications Commission* en octobre 2016, mais suspendu temporairement depuis et remis en cause devant le Congrès en 2017). Autant

14 Notamment par crainte d'une législation construite sous l'influence de certains intérêts particuliers, et en particulier des acteurs industriels contre lesquels s'est initialement construite la revendication d'une protection accrue.

15 La *tort law* regroupe aux États-Unis les régimes de responsabilité contractuelle et délictuelle alors qu'ils sont différenciés dans le système français.

de considérations qui ne permettent pas de se prononcer clairement sur l'existence ou l'absence d'un droit de propriété sur les données personnelles.

En France, certains juristes, notamment à l'appui de la décision de la Cour de cassation précitée, analysent les données comme des biens à part entière (à tout le moins, dans le cadre d'un échange commercial) :

À l'égard d'une chose, inappropriable, le droit n'admet pas de circulation (la chose ne pouvant pas être détenue par un propriétaire qui en disposerait). [...] s'il est possible d'imaginer que les données à caractère personnel soient saisies comme des éléments dérivant de la personne et participant de sa personnalité, rien n'est simple en la matière : leur qualification peut osciller entre celle de « bien » (pour la valeur qu'elles représentent ainsi que pour leur circulation) et de « personne » (pour ce lien avec leur titulaire) ; elles composent donc des biens teintés de personne [...]. Pour autant, les textes européens de la matière penchent nettement en faveur de la première qualification en promouvant, jusque dans leur intitulé, la « libre circulation » des données. Celles-ci composent donc des biens aliénables. (Rochfeld, 2014)

À côté de ces réflexions ouvertes, des positions plus fermes ont également été prises à l'encontre d'un possible droit de propriété, à construire ou à reconnaître pour les données personnelles. Perçu comme « irréaliste » (Brughière, 2014), son principe comme son efficacité sont contestés par certains acteurs institutionnels ; ainsi notamment du Conseil national du numérique (2014, p. 37) et du Conseil d'État (2014, pp. 264-269). Les deux instances se positionnent principalement au regard d'une inefficacité à protéger les internautes, un droit de propriété ne faisant que confirmer les attentes et revendications de nombreuses plateformes dans les conditions générales d'utilisation qu'elles mettent en place, tout en n'ouvrant qu'à une rétribution financière très faible à l'échelle d'un individu.

À la suite de ces débats, la perspective d'un droit de propriété formel et formalisé en droit sur les données personnelles semble écartée en Europe (voir *infra*, la position adoptée dans le règlement européen). Cela n'épuise pas les interrogations sur la titularité des éventuels droits de propriété que l'on retrouve au cœur des débats économiques (voir *infra*) : « *As the extensive use of consumer information has become prevalent in the modern marketplace and the*

value of the information increases, the issue of who “owns” and controls consumer information is raised » (Gabisch et Milne, 2014, p. 14). En dehors des (éventuelles) revendications d'un contrôle de leur vie privée, les individus dont les données sont captées sont-ils – vraiment – ceux qui valorisent le plus ces données et qui maximisent le surplus social, ce qui ferait d'eux les récipiendaires logiques des droits afférents (Friedman, 2000) ? Est-ce dès lors entre leurs mains qu'il faudrait remettre les droits ou entre celles des plateformes qui organisent la récolte, la production de ces données et qui leur donnent une valeur par leur traitement et leur éventuelle circulation ?

Dans le débat juridique, en France comme aux États-Unis, la crainte de laisser un marché ouvert sans droits délimités est fortement présente, touchant à la fois aux opportunités pour les plateformes et aux libertés fondamentales des internautes. Elles reviennent à soulever un questionnement économique ancien, celui des fondements des droits de propriété.

3. UNE INCITATION LIMITÉE À PRÉSERVER OU À PRODUIRE DES DONNÉES

Dans son argumentation sur la *Tragedy of the Commons*, Garrett Hardin (1968) s'inspire de travaux sur la démographie réalisés dans l'Angleterre du XIX^e siècle¹⁶, en mettant en avant l'exemple d'un pâturage utilisé par de nombreuses personnes pour leurs troupeaux. Chacune a alors intérêt à augmenter son utilisation du bien mis en commun, puisqu'elle dégage par là un bénéfice individuel (profit tiré d'un plus grand troupeau) toujours supérieur au coût (usure du pâturage jusqu'à son épuisement) partagé entre tous. Seul alors le droit de propriété permet de sauvegarder les biens : « *An alternative to the commons need not be perfectly just to be preferable. [...] We must admit that our legal system of private property plus inheritance is unjust – but [...] injustice is preferable to total ruin* » (Hardin, 1968, p. 1247). Il est essentiel ici de voir que, contrairement à certaines compréhensions usuelles¹⁷, la propriété privée n'est pas en soi synonyme de liberté, mais

16 Lloyd W. F. (1832) [1980], « W. F. Lloyd on the Checks to Population », *Population and Development Review*, vol. 6, n° 3, pp. 473-496.

17 Qui semblent par exemple pouvoir se retrouver dans les propositions d'Alain Bensoussan (2010). Cf. *supra*.

constitue bien une restriction, une *mutual coercion*, encadrée et sanctionnée par l'État dans l'objectif de lutter contre le pillage et la surexploitation de ressources à la disposition de tous. Le raisonnement formé autour de la tragédie des *commons*, en dehors de ses approximations empiriques, relevées notamment par les travaux d'Elinor Ostrom (Ostrom et al., 1999), permet de mieux percevoir l'intérêt de mettre en place des droits de propriété, afin de réguler les utilisations en organisant des *enclosures*. Elles permettent de rendre chaque titulaire de droits responsable de sa propriété : il peut seul en jouir et en disposer ; il peut jouir et disposer d'elle seule. La surutilisation d'une ressource existante nécessite donc des formes d'arrangements institutionnels pouvant prendre la forme de droits de propriété (Demsetz, 1967).

Dans la proposition de Hardin, la mise en cause des *commons* est construite de manière incrémentale, suivant une dynamique que l'on pourrait qualifier de développementaliste, accompagnant l'évolution dans le temps long des sociétés : « *As the human population has increased, the commons has had to be abandoned in one aspect after another. First we abandoned the commons in food gathering, enclosing farm land. [...] Somewhat later we saw that the commons as a place for waste disposal would also have to be abandoned* » (Hardin, 1968, p. 1248). C'est ainsi un autre argument que développe Hardin pour justifier le recours aux droits de propriété : la nécessité de préserver les *commons* des diverses formes de pollution (ou autres externalités négatives) qui pourraient transformer les ressources communes disponibles en « *waste disposal* » (déposer par exemple des déchets sur un terrain commun) :

Here it is not a question of taking something out of the commons, but of putting something in—sewage, or chemical, radioactive, and heat wastes into water; noxious and dangerous fumes into the air; and distracting and unpleasant advertising signs into the line of sight. The calculations of utility are much the same as before. The rational man finds that his share of the cost of the wastes he discharges into the commons is less than the cost of purifying his wastes before releasing them. [...] The tragedy of the commons as a food basket is averted by private property, or something formally like it. But the air and waters surrounding us cannot readily be fenced, and so the tragedy of the commons as a cesspool must be prevented by different means, by coercive laws or taxing devices. (Hardin, 1968, p. 1245)

Dans la lignée des travaux de Hardin, la proposition d'instauration d'un droit de propriété sur les données personnelles pourrait être lue comme une réponse directe à la situation actuelle d'incertitude sur le statut des données et sur les personnes, morales ou physiques, pouvant en user et en tirer les fruits. À défaut d'un droit clair sur ces prérogatives, les données peuvent en effet faire l'objet d'un « pillage » sans contrainte : « Les pouvoirs publics menacent de vous couper l'accès à l'Internet pour la duplication de quelques chansons ; ils laissent, dans le même temps, un peuple entier se faire dérober sa vie privée » (Bellanger, 2014, pp. 201-203). Cependant, l'instauration de droits de propriété sur cette base repose sur deux justifications successives, auxquelles nous semblent, en réalité, échapper les données personnelles.

En premier lieu, la nécessité économique d'un droit de propriété inspirée de la tragédie des *commons* s'applique d'abord aux biens qualifiés de rivaux, c'est-à-dire à ceux dont la consommation par un acteur diminue la possibilité de consommation par d'autres. La construction exposée par Hardin vise précisément à garantir l'existence des biens rivaux, en accordant aux acteurs une possibilité de consommation limitée sur les ressources prises dans leur ensemble. C'est l'usure potentielle par des usages répétés d'une ressource limitée qui justifie l'instauration de droits de propriété. Cependant, les données personnelles ne constituent pas des biens rivaux ; leur utilisation par un individu ou une organisation ne les abîme, ne les use ou ne les détruit pas. Aussi, aucune restriction n'est nécessaire pour préserver les données personnelles, leur existence n'étant pas mise en péril par leur utilisation, aussi extensive soit-elle¹⁸.

En second lieu, les données personnelles peuvent engendrer des externalités négatives pour certains acteurs, par exemple lorsqu'elles « fuient » : « *We have already seen “data spills” happen (when large amounts of personal data are inadvertently leaked). Will it be much longer until we see dangerous data drilling practices? Or until we start to see long term effects from “data pollution”?* » (Thorp, 2012). Les risques et dommages, pour la vie privée notamment, sont à la fois réels et connus. Pour autant, ces dommages et leur possible réparation ne se situent pas sur le plan d'un bien, mais de l'individu, à l'instar de la santé par exemple. Au travers d'un droit de propriété sur les données, ce n'est pas tant ces dernières que l'on souhaite protéger que la vie privée des

¹⁸ Sauf le cas d'une recherche d'un usage exclusif sur certaines données.

individus concernés. Or, pour protéger la vie privée des externalités négatives, les logiques de responsabilités, contractuelle ou délictuelle (*tort law*, voir *supra*), existent déjà dans les différents systèmes juridiques, sans qu'il soit pour autant nécessaire de proclamer une propriété des individus sur eux-mêmes.

En dehors des travaux de Hardin, une analyse spécifique a été développée pour les biens non rivaux que sont les biens collectifs ou informationnels (Arrow, 1962). Pour ces biens dont chacun peut profiter sans nuire aux autres usagers, se posent les questions de la disposition à payer des consommateurs et de l'incitation à produire des biens lorsqu'on ne peut exclure de leur usage les agents économiques qui ne contribuent pas à leur financement. Coûteuse à produire, l'information est peu coûteuse à reproduire ou à diffuser. Le risque est alors celui, non de la surutilisation d'une ressource existante comme dans la tragédie des *commons*, mais de la sous-production de biens pourtant eux aussi utiles à la collectivité. Face à cette « défaillance de marché », la création d'un monopole via des droits de propriété permet de restaurer l'incitation des entreprises à produire de tels biens non rivaux, en excluant de la consommation les agents ne payant pas (Demsetz, 1970).

En ce qui concerne les données personnelles, il n'y a pas plus de risque de sous-production que d'usure des données liée à une utilisation intensive, deux cas qui justifieraient, sur la base de mesures d'incitation, le recours à des droits de propriété. Les internautes « fournissent » de la donnée en quantité et continueront à le faire (voir partie 1). Par ailleurs, dans l'exploitation des données personnelles, les plateformes possèdent déjà un intérêt suffisamment incitatif pour la raison qu'elles n'obtiennent pas les données en soi, existantes à un état quasi naturel, mais ont l'ardente obligation, afin de développer des modèles économiques performants, d'en être en grande partie les productrices et les gestionnaires.

4. UNE EFFICACITÉ ÉCONOMIQUE EN FAVEUR DE LA TITULARITÉ DES DROITS ACCORDÉS AUX PLATEFORMES

Au-delà de la fonction incitative à préserver les ressources existantes ou à en produire de nouvelles, toutes utiles à l'ensemble de la collectivité, une

autre approche de la propriété, plus industrielle, a été développée. La propriété constitue une institution dont la finalité est d'organiser de manière économiquement efficace les transactions et la circulation des biens sur les marchés. Les travaux de Ronald Coase (1960) et l'abondante littérature économique qu'ils ont suscitée permettent d'avancer quatre idées majeures en matière de droits de propriété :

- Tout d'abord, les droits de propriété viennent principalement organiser et combler les risques d'incomplétude sur les contrats, afin de permettre les négociations entre acteurs – et éventuellement, l'intervention d'une autorité judiciaire en cas de blocage. Il revient aux pouvoirs publics de faire en sorte que les droits de propriété soient clairement attribués afin que les négociations soient possibles.
- L'attribution initiale des droits de propriété à une catégorie d'agents économiques plutôt qu'à une autre influence la répartition des revenus entre ces agents mais nullement l'allocation optimale des ressources.
- Lorsque les coûts de transaction sont nuls ou négligeables, pour peu que les droits de propriété soient clairement attribués et cessibles, les agents vont en effet négocier spontanément sur le marché une solution qui établit l'allocation optimale des ressources. Dans l'hypothèse d'une absence relative de coûts de transaction, la négociation entre acteurs permet donc de parvenir au même résultat (un surplus social maximisé) que la présence de règles juridiques favorisant telle ou telle catégorie d'agents.
- Au terme de ce processus, les ressources seront exploitées non pas forcément par les titulaires de droits de propriété originels mais par les agents économiques capables de les valoriser au mieux. Les droits de propriété seront alors entre les mains des acteurs les plus efficaces dans une perspective de maximisation du surplus social.

Si l'on se situe dans la perspective de ces travaux, l'absence de droit de propriété sur les données peut au premier abord évoquer une situation de flou, néfaste à l'activité économique, qu'il conviendrait de corriger.

C'est là où le droit intervient : aujourd'hui ces données sont ce qu'on appelle « res nullius », c'est-à-dire qu'en droit elles ne sont propriété de personne. Il faut rappeler que les pères fondateurs des États-Unis, lorsqu'ils ont rencontré les Indiens, ont décrété que comme ils n'avaient pas de titres de propriété, leurs terres étaient

« *terra nullius* ». Donc, méfions-nous quand nos données sont « *res nullius* » et qu'il y a des intérêts impériaux en face. (Interview de Pierre Bellanger¹⁹)

Selon cette argumentation, l'absence de droits de propriété serait nécessairement favorable aux acteurs en position de pouvoir. Ce que semble cependant oublier l'auteur, c'est justement l'historique des droits de propriété, et notamment ceux issus des *Homestead Acts*²⁰. La perte des terres évoquées n'est pas due à l'absence de droit de propriété mais elle est, bien au contraire, la conséquence directe de leur instauration²¹. Sans même souscrire à une conception proudhonienne de la propriété, celle-ci participe le plus souvent d'un renforcement *de jure* des rapports de forces existants *de facto*. Surtout, à l'endroit des données personnelles, cette revendication oublie trop rapidement que la titularité des droits ne serait pas acquise aux internautes, comme cela a déjà été évoqué plus haut :

Quant au résultat du traitement, doit-on le dissocier de la donnée brute ? Doit-on penser un statut pour la donnée valorisée ? Doit/peut-elle faire l'objet d'un droit subjectif ? Dans l'affirmative, il conviendrait d'en déterminer le titulaire : devrait-il s'agir de l'entreprise qui a réalisé l'investissement (exploré le gisement) ou bien de la personne qui a fourni la matière première (l'or noir que constituent les données) ? (Bensamoun et Zolynski, 2014)

L'argumentation de Coase conduit, elle, à retenir que la question de la titularité initiale des droits de propriété importe peu. Le marché permettra de les attribuer *in fine* à ceux capables de les valoriser au mieux. Dans ce cadre, le droit de propriété bénéficierait certainement aux plateformes et, plus généralement, aux organisations plus qu'aux internautes. En effet, ce sont elles qui sont à même de recueillir, traiter et analyser les données, puisqu'elles sont très souvent à l'origine de leur création au travers des dispositifs sociotechniques dédiés. De plus, si la prémisse de Coase d'absence

19 Barroux, D., Georges, B. et Rauline, N. (2014), « Gilles Babin et Pierre Bellanger : la régulation des données, défi majeur du XXI^e siècle », *Les Échos*, 12 février 2014.

20 Selon cette législation, mise en œuvre à partir de 1862 aux États-Unis, un droit de propriété était établi dès lors que la preuve était apportée de l'utilisation et de la mise en valeur d'une parcelle de territoire.

21 De manière quelque peu semblable, le mouvement d'enclosure dans l'Angleterre du XVIII^e siècle a exclu des *commons* les possibles exploitations légères et activités de subsistance, qui ont alors rejoint les tresspass condamnés par la loi (Polanyi, 1944).

de coûts de transaction a été fréquemment, et à juste titre, critiquée pour sa fragilité empirique, elle semble cependant pouvoir rencontrer une applicabilité grandissante dans le cadre du numérique. L'analyse de Coase conduit donc à soutenir la dévolution des droits de propriétés éventuels entre les mains des organisations plus qu'entre celles des internautes, soit l'inverse de l'effet de protection revendiqué par les promoteurs de l'instauration de droits de propriété sur les données personnelles.

D'autres pistes pour concilier protection de la vie privée des individus et développement de l'économie numérique doivent donc être étudiées.

5. VERS LA CONSTRUCTION D'UN MARCHÉ DES DONNÉES PERSONNELLES RESPECTUEUX DE LA VIE PRIVÉE

Un des enjeux des données personnelles tient aux nombreux revenus, de natures très diverses, qui peuvent en être tirés. La question de la valorisation de ces données, et surtout du potentiel partage de cette valorisation, est donc posée sans que les conséquences de la marchandisation sur la vie privée ne soient toujours au cœur des réflexions.

5.1. Marchandisation des données et partage de la valeur

La transmission et la mise en valeur des données personnelles sont en partie faites, au travers des dispositifs déployés sur les plateformes, par les internautes eux-mêmes. Partout, l'internaute est « au travail »²², fournissant une contribution non rémunérée. L'interaction entre le service et l'utilisateur est l'une des sources de création de valeur faisant écho aux théories du « capitalisme cognitif » (Moulier-Boutang, 2010) qui correspond à une économie de pollinisation et de contribution.

Les rapports commerciaux construits autour des données sont fortement critiqués, notamment au travers des recherches liées au *digital labor*

²² On notera cependant que la référence à la notion de « travail » est ambiguë dans la mesure où il s'agit d'une contribution sans contrat, sans hiérarchie ou donneur d'ordre et souvent sans effort particulier de l'internaute (traces passives).

(Scholz, 2013 ; Rey, 2012 ; Casilli, 2010 et 2014). Suivant ces perspectives critiques, les différentes formes de travail qui permettent le recueil et le traitement des données devraient être soit combattues en tant que telles, soit faire l'objet – *a minima* – d'un retour vers les internautes concernés. De manière presque paradoxale, elles peuvent ainsi partager avec certaines perspectives marchandes une interrogation sur la juste valeur des données personnelles, bien que les conclusions et revendications tirées en soient différentes. La conception d'un *digital labor* porte avant tout un regard particulier sur les rapports entre internautes et plateformes, mais rejette par exemple la perspective de micropaielements, qui lui apparaît comme une « provocation ou vision dystopique » (Casilli, 2014, p. 433), au profit notamment d'un partage plus global de la valeur, organisé par l'État et la collectivité publique.

D'autres contributions envisagent en effet que les internautes soient les bénéficiaires des données qu'ils fournissent en les monétisant directement auprès des annonceurs publicitaires ou des organismes intéressés, au lieu de laisser des entreprises comme Facebook s'en charger – à leur place. Ainsi notamment de la proposition de Jaron Lanier (2014) de favoriser des micropaielements pour toute information transmise par les individus à d'autres acteurs.

La perspective de construction de nouveaux revenus pour les individus rejoint les propositions précurseuses de Kenneth C. Laudon visant à établir un *National Information Market* « *in which information about individuals is bought and sold at a market clearing price freely arrived at, in which supply equals demand. Institutions gathering information about individuals would be allowed to sell baskets of information to other institutions willing to pay for it* » (Laudon, 1996, p. 99).

Cette idée se retrouve chez des acteurs économiques qui se sont d'ores et déjà constitués comme intermédiaires afin de proposer aux internautes de monétiser leurs données. Ils proposent un service – de nature ambiguë – entre protection des données personnelles (*data locker*), revente maîtrisée de celles-ci et outils de négociation avec les vendeurs de biens et services (*VRM*, pour *vendor relationship management*)²³. Ces propositions rejoignent un

23 Ainsi des propositions – encore un peu floues – de Datacoup ou YesProfile par exemple. Pour une liste de nombreux services, voir le wiki du *ProjectVRM* du Berkman Center for Internet & Society : <http://cyber.law.harvard.edu/projectvrn/>

marché émergent de la confiance et de la réputation, où des acteurs proposent de contrôler – en partie à la place des utilisateurs eux-mêmes – les données qui les concernent, pour diminuer les coûts liés à un contrôle direct (CTRL – SHIFT, 2014).

La logique de monétisation connaît certaines limites. Les revenus dégagés par les plateformes, pour la part issue de l'exploitation des données, dépendent de l'importance des quantités agrégées. La valorisation financière revendiquée pour l'internaute semble illusoire, les simulations montrant un taux de retour pour chacun de quelques euros ou quelques dizaines d'euros par an seulement. Là n'est cependant pas la question essentielle. La monétisation directe ou par des intermédiaires ne modifie pas en soi les équilibres de marchés qui profitent aux plateformes. La vente de données ne fait que déplacer ces dernières vers un marché d'oligopsonie (les grandes plateformes dominantes qui produisent, organisent et encadrent les données constituent un faible nombre de demandeurs, tandis que les internautes constituent un très grand nombre d'offreurs).

Si la question du partage de la valorisation des données est au cœur de l'ensemble de ces réflexions, celle des conséquences de cette économie naissante sur la vie privée est plutôt abordée par d'autres approches. Pour envisager la marchandisation sous l'angle plus précis de la vie privée, nous présentons trois pistes qui éclairent le débat : la première passe par le développement de solutions techniques, la seconde par une nouvelle définition institutionnelle et collective de la vie privée. Ces deux premières pistes sont en partie encore embryonnaires. La troisième présente le nouveau Règlement européen entrant en vigueur en 2018 qui donne un cadre juridique concret aux évolutions à court terme.

VRM_Development_Work. Pour un certain nombre d'offres, marché de la confiance et marché de la monétisation se rejoignent dans les mêmes entreprises. Les propositions de ces dernières regroupent mise en ligne protégée des données personnelles (proche du *cloud computing*) et monétisation envers des tiers. Mélange des genres particuliers qui pourrait évoquer une agence bancaire faisant de son coffre-fort une place de marché...

5.2. La technique au service des internautes et des plateformes

La régulation des données est d'ores et déjà assurée en grande partie par un ensemble de dispositifs que Lawrence Lessig (2000) appelle l'architecture (du code, des logiciels, des matériels...). Cette architecture est donc également porteuse d'un certain nombre de choix (ou d'absence de choix) en matière de vie privée. L'idée de régulation par le code a conduit à la notion de *privacy by design* (Cavoukian, 2006), ou encore, dans une acception plus strictement technique, de *privacy by architecture*. Cette dernière approche vise à inscrire des choix concernant la vie privée dans l'architecture d'un système en réseau, grâce à un certain nombre de modalités d'anonymat, d'obscurcissement, de stockage décentralisé, d'attribution d'identités multiples et d'effacement, etc. (Musiani, 2015), soumettant *de facto* tous les acteurs impliqués à ses normes ; il s'agit donc d'une régulation par le code (et non d'une régulation du code) qui est désormais explorée dans de nombreux projets.

La *privacy by architecture* peut conduire, de manière radicale, à empêcher la constitution de données personnalisables traçables. De nombreux dispositifs permettent, au moins en théorie, à l'internaute de masquer son identité ou de refuser d'être « tracké » : réseaux privés virtuels (VPN), serveur proxy, robot txt, réseau TOR, paywebcard²⁴, chiffrement des données, voire obfuscation²⁵ ou données éphémères... Mais outre que leur paramétrage ou leur usage sont souvent complexes (ou qu'ils ne permettent en général pas l'utilisation efficiente du service), leur efficacité en matière de protection est mise en cause et a montré de nombreuses failles (Anciaux N. et Nguyen, 2015) ; en outre, ils ne permettent aucune utilisation des données personnelles, quelles que soient les garanties données ou la volonté des internautes. Sont donc explorées des solutions techniques qui permettent l'utilisation et la valorisation des données personnelles en étant porteuses de prescriptions de *privacy*. Deux grandes voies sont ouvertes.

24 Qui permet de rompre le lien entre l'identité d'un acheteur et son paiement en ligne.

25 Défini par Helen Nissenbaum comme le fait d'ajouter des données fausses ou ambiguës pour se soustraire aux agrégateurs de données ou les tromper. Idée reprise par exemple dans l'application TrackMeNot.

La première voie fait porter l'obligation de respect de la vie privée aux serveurs détenteurs des données. Cela passe par exemple par des techniques d'anonymisation sachant que la suppression du nom des personnes est loin de garantir automatiquement qu'elles ne pourront pas être identifiées. C'est pourquoi différents outils d'anonymisation sont proposés par les chercheurs, en particulier la « k-anonymisation », la « l-diversité », ou, celle aujourd'hui considérée comme la plus solide, la « confidentialité différentielle » qui s'appuie sur la génération de données fictives. Ces techniques ne sont que partiellement satisfaisantes : la qualité des outils dépend principalement du modèle choisi (et non de la quantité de données ou de leur précision) ; on peut les évaluer en fonction de leur efficacité (résistance de la protection), mais aussi des traitements des données qu'elles permettent (Nguyen, 2014). D'autres approches inscrivent dans le serveur détenteur des données des fonctionnalités de chiffrement, de masquage partiel de données, de brouillage de certains éléments, etc., dans le but d'un meilleur respect de la *privacy* (Anciaux N. et Nguyen, 2015).

Cette première voie se heurte à un double problème :

- d'une part, la protection de la *privacy* est entièrement entre les mains du détenteur des données (ce qui pose des questions de transparence ou d'absence de contrôle) comme l'ont montré les controverses autour de la plateforme P3P (Platform for Privacy Preferences Project) développée par le W3C qui permettait aux sites d'afficher leurs politiques de *privacy* et aux internautes d'indiquer quelles utilisations commerciales pouvaient être faites de leurs données (Cranor et al., 2002 ; Rallet et al., 2015) ;
- d'autre part, la résistance des bases ou des serveurs centralisés est considérée comme sujette à caution.

La deuxième voie s'appuie donc sur la décentralisation et les architectures distribuées pour protéger les données personnelles d'utilisations non autorisées ou dissimulées (Méadel et Musiani, 2015). Les données peuvent par exemple être collectées sur un serveur personnel, comme dans le « web personnel sécurisé » de l'INRIA qui passe par un tiers de confiance recueillant les prescriptions du détenteur des données et délivre les « permis de traitement », soit de manière automatique, soit à la demande (Anciaux N. et Nguyen, 2015 ; de Montjoye et al., 2014). La décentralisation n'est pas totale et toutes les contraintes ne semblent pas résolues pour l'exploitation

de données massives et le traitement de requêtes complexes et diversifiées. Des requêtes vérifiées distribuées de manière décentralisée à des bases de données pourraient permettre de mieux garantir la sécurité des traitements. D'où le recours à la technologie blockchain exploré par exemple dans le projet Opal/Enigma du MIT. Comme résumé par sa formule « *bring the code to the data, not the data to the code* », il s'agit d'inverser la logique actuelle de circulation des données et de faire remonter le traitement vers les données par l'utilisation d'un « *auditable, tamper-proof distributed ledger (a permissioned blockchain) [who] records and controls access through smart contracts and digital identities* » (Ackerman Shrier et al., 2016).

Ces solutions sont des pistes ouvertes pour que les prescriptions liées au respect de la *privacy* soient « *embedded* », encastrées dans les outils techniques et s'imposent donc à tous par la force du code. Cependant, outre les problèmes techniques non encore résolus, cela laisse ouvertes des questions sur la formulation des normes. Sans transparence sur les principes et sans discussion collective autour des choix techniques, rien ne garantira que l'architecture aboutisse à mieux protéger les données personnelles des prédatons et usages abusifs (Brousseau et al., 2013). Les *infrastructures studies* (Star, 1999), poursuivant les recherches sur les *Sciences and Technology Studies*, ont en effet montré à quel point les objets communicants sont porteurs de conceptions politiques du monde.

5.3. Les communs ou l'invention de nouveaux arrangements institutionnels

En se situant dans un cadre collectif, plutôt que de confirmer l'analyse d'un *privacy paradox*, il est possible d'estimer que les internautes sont entrés dans une nouvelle appréhension d'une vie privée « négociée ». Cela rejoint la construction historique de la frontière entre vie privée et vie publique dont les historiens (Philippe Ariès, Alain Corbin Norbert Elias et d'autres) ont montré l'émergence sociale au cours du XVIII^e siècle. Il ne s'agit pas de prendre acte de la supposée disparition la vie privée sur Internet²⁶ mais d'en comprendre les nouveaux contours (Casilli, 2013 et 2014). Ainsi, la

26 Position soutenue par le PDG de Facebook, affirmant que les normes imposées par la plateforme ne font que suivre des évolutions sociales extrinsèques (Kirkpatrick M., January 9, 2010, « Facebook's Zuckerberg Says The Age of Privacy is Over », *Readwrite*).

vie privée n'apparaît plus seulement comme un attribut de la personne, ou plus exactement comme un attribut de la personne seule, qu'un individu conserve et préserve en tant que tel, ouvre et transmet en partie, ou encore abandonne quasiment. Elle est toujours le résultat d'une transformation collective des normes et des mœurs. La vie privée ne saurait alors que plus difficilement encore faire l'objet d'une monétisation sur la base de revendications individuelles, mais cela ouvre la voie à des négociations collectives, constamment redéfinies, pour délimiter ce qui est acceptable et souhaitable. Dans cette logique, les usagers peuvent prendre eux-mêmes l'initiative de nouveaux arrangements institutionnels.

Certaines formes de régulation des données peuvent en effet être envisagées dans une direction – encore largement à construire – inspirée des problématiques de recherche issues de l'économie institutionnelle et plus précisément des travaux d'Ostrom (1999) sur la gouvernance et les biens communs.

Dès lors, il est possible d'envisager que la prise en charge des données personnelles se construise au travers de formes institutionnelles également négociées collectivement, sous la forme de « commons ». Institution particulière, les *commons* possèdent la difficulté première de ne pouvoir être institués *ab initio*, par une décision du législateur notamment ; elles sont une construction – parfois étendue pendant un temps très long – d'arrangements entre différents acteurs. Une voie possible est ainsi évoquée pour les données personnelles :

Ni privé, ni public, comment penser des données personnelles en biens communs ? Car c'est une piste peu étudiée : celle de faire de ces fameuses données personnelles des biens communs, quelque chose qui appartient à tous et à personne. Ne pas les sanctuariser par la loi, ni les commercialiser sans vergogne mais bien de repenser autour de leurs usages un faisceau de droits. Il ne s'agit pas de refuser de leur appliquer un régime de propriété mais d'en repenser la nature. Et s'il fallait inventer des creative commons des données personnelles, des privacy commons ? Reste à définir une gouvernance partagée de cette ressource commune. (Mercier, 2014)

Les recherches d'Ostrom insistent non pas tant sur la définition et la délimitation d'un bien commun, mais sur l'importance des mécanismes de négociation, gestion et disposition collective, l'institution en tant que telle de règles et de régimes particuliers (Allaire, 2013 ; Weinstein, 2013). Ainsi,

« seul l'acte d'instituer les communs fait exister les communs, à rebours d'une ligne de pensée qui fait des communs un donné préexistant qu'il s'agirait de reconnaître et de protéger, ou encore un processus spontané et en expansion qu'il s'agirait de stimuler et de généraliser » (Laval, 2011).

Ces questions se retrouvent dans plusieurs projets²⁷ visant à expérimenter les usages possibles des données personnelles lorsqu'elles sont mises à disposition des individus, et soulevant des questions de nature institutionnelle : quelles sont à la fois les valeurs créées par la mise en partage de ces données, les régulations souhaitées par les individus, et les institutions mises en avant pour organiser la gestion de ces relations entre individus et entreprises ? Dans cette perspective, la mise de côté d'un droit de propriété au profit de « faisceaux de droits » (Orsi, 2013) peut permettre de préserver et de construire des arrangements originaux autour d'un commun.

On retrouve cette possibilité en filigrane dans le système de licences sur le modèle des licences libres existantes dans le secteur du logiciel (GPL) ou culturel (Creative Commons) envisagé par Thomas Saint-Aubin :

S'il s'agit d'un contrat bilatéral, la licence proposée s'inscrit également dans le cadre des relations juridiques de l'individu avec un producteur et un gestionnaire d'entrepôt. Sa mise en œuvre nécessite donc parallèlement l'acceptation par le réutilisateur des conventions générales d'utilisation de l'entrepôt et le cas échéant, de celles des API, déterminées par le gestionnaire. La licence est donc une concession de droits d'usages à un réutilisateur, sur les données personnelles d'un individu. Il lui concède un droit personnel, non exclusif et non transférable, de réutilisation de ses données pour les finalités et les moyens présélectionnés par ses soins. Cette opt-in (c'est-à-dire cette option d'adhésion qui a fait l'objet d'un consentement préalable) est temporaire et révocable unilatéralement par l'utilisateur en opt-out (accord tacite, sans consentement préalable)²⁸.

Conformément à l'apport de l'approche néo-institutionnelle qui montre la diversité des formes de gestion des ressources, il convient cependant de

27 Tels le projet MesInfos mené par la FING en France, ou le projet MiData au Royaume-Uni.

28 Saint-Aubin, T., « Design your privacy : pour une licence de partage des données personnelles », *InternetACTU.net*, 22 juin 2012.

noter que, pas plus qu'en matière de logiciels ou de biens culturels (Farchy et de la Taille, 2017), tous les projets concernant les données personnelles ne seront pas propices à la constitution de communs. Il n'en reste pas moins qu'en s'éloignant peu ou prou d'une perspective de monétisation, ces revendications viennent proposer des formes nouvelles de négociation et de gestion des données.

5.4. Les deux piliers du Règlement européen

Dès les premières dynamiques de la législation française en la matière, une grande partie de la protection des données à caractère personnel repose sur la possible action des individus concernés. Outre les obligations de déclaration, et parfois de demande d'autorisation, pesant sur les exploitants de ces données, la législation fondatrice de 1978 dispose en effet que la personne auprès de laquelle sont recueillies des données à caractère personnel la concernant en est informée. Ayant connaissance des potentiels usages de leurs données personnelles, les individus peuvent bénéficier ensuite de plusieurs droits, respectivement qualifiés de droit d'opposition, d'accès et de rectification.

Les logiques de contrôle tournées vers l'individu se heurtent à un certain nombre de limites déjà évoquées, à savoir que les plateformes opérant des services en réseau, portées par la masse de consommateurs, sont dans une situation favorable et asymétrique vis-à-vis des internautes. Dans ce contexte de déséquilibre des forces, les régulations tournées vers une responsabilisation de la partie en situation de faiblesse ne semblent pas pouvoir seules résoudre la question. Les actions de groupe envisagées au niveau européen visant à permettre à des internautes de saisir collectivement la justice sur des questions de données personnelles seraient un premier pas pour renverser ce déséquilibre. Il apparaît cependant nécessaire de tourner plus encore les régulations et les obligations vers les exploitants de données personnelles et leurs marchés.

À cet égard, le Règlement européen 2016/679, qui entrera en vigueur en mai 2018, et qui suscite une grande effervescence dans le monde des entreprises, constitue un changement majeur ; son architecture s'appuie en effet à la fois sur un renforcement des droits des individus et sur une nouvelle dialectique sanction – responsabilisation des organisations.

5.4.1. Renforcer le pouvoir des individus

C'est dans le sens d'un renforcement du pouvoir des individus que peuvent se comprendre les propositions du Conseil d'État (2014, p. 267 et s.) autour de l'idée de droit à l'autodétermination informationnelle inspirée de la Cour constitutionnelle fédérale allemande²⁹. Présentée comme une alternative au droit de propriété, l'autodétermination informationnelle est considérée comme un « objectif permettant d'offrir une véritable protection des données personnelles », en prolongeant une protection construite autour de l'individu, en dehors de toute appropriation patrimoniale. De l'aveu même de ses promoteurs, il s'agit donc d'un objectif général, une sorte de « droit chapeau » auquel il convient de donner consistance pour le rendre opératoire.

C'est dans cette perspective que le Règlement, reprenant à son compte le concept d'autodétermination informationnelle, conforte les droits existants et en crée de nouveaux pour les individus. Ainsi de la mise en place d'un droit à l'oubli numérique ou d'un droit à la portabilité des données. Ce dernier vise à permettre aux utilisateurs d'un fournisseur de service de pouvoir transférer vers un autre les données le concernant au moyen d'une conception qui lie les données directement à la personne plus qu'à l'exploitant ; ce droit à la portabilité permet ainsi de diminuer les « barrières à la sortie » pour l'internaute et de stimuler la concurrence entre les entreprises.

5.4.2. Du contrôle ex ante à une logique de responsabilisation – sanction des plateformes

Alors que la directive de 1995 reposait en grande partie sur la notion de formalités préalables (déclarations, autorisations), le Règlement repose prioritairement sur une logique de conformité dont les acteurs sont responsables sous le contrôle et avec l'accompagnement des régulateurs nationaux. Cette notion de responsabilisation³⁰ se traduit par des obligations sur l'archi-

29 BUNDESVERFASSUNGSGERICHT, Urteil des Ersten Senats, 15 décembre 1983, 1 BvR 209/83 u. a.

30 Le terme « accountability », difficilement traduisible dans toutes ses nuances en français, renvoie en réalité à la fois à l'affirmation de la responsabilité de l'entreprise mais surtout à sa faculté à démontrer qu'elle a bien respecté les exigences réglementaires.

teature des plateformes au travers d'une « Protection des données dès la conception et protection des données par défaut » (*Data protection by design and by default*). Parallèlement, le mécanisme de sanctions est fortement renforcé puisque celles-ci peuvent atteindre, pour les manquements les plus graves, jusqu'à 4 % du chiffre d'affaires mondial.

Derrière l'idée explicite de *privacy by design* se rejoignent deux dynamiques : la recherche par les utilisateurs de plateformes pouvant composer avec le respect de la vie privée ; l'intérêt des plateformes existantes ou potentielles d'adapter leurs dispositifs pour répondre à cette attente, afin de conserver leurs utilisateurs en faisant de la confiance et de la transparence des clés de voûte de leurs stratégies marketing. La gratuité des services proposés peut en effet, à terme, conduire à une forme de contradiction interne du système rendant incompatible une économie de l'attention fondée sur la tentation de captations de données à grande échelle et le respect des libertés. Conscientes des enjeux pour l'avenir de leur modèle économique, les plateformes sont dès lors incitées à intégrer le respect de la vie privée dans leurs stratégies.

Une forme d'autorégulation pourrait se développer sous la pression de la demande. Le « contrat faustien » laisserait ainsi la place à des contrats plus librement négociés, ou plus exactement à un choix plus large entre les offreurs de services pour lesquels le traitement des données et le rapport à la vie privée apparaîtraient comme des caractéristiques concurrentielles discriminantes permettant à l'internaute de faire ses choix.

CONCLUSION

Peu prisée des Européens, l'idée de droits de propriété sur les données personnelles trouve un écho plus favorable outre Atlantique. L'analyse économique, quant à elle, conclut que les droits de propriété apparaissent, sur le plan des incitations, dispensables ; de plus, en termes d'organisation des transactions sur un marché, l'approche coasienne conduit à conclure que l'instauration de droits de propriété aurait pour conséquence d'attribuer les droits aux plateformes, soit l'inverse des objectifs recherchés en termes de protection de la vie privée.

La mise en place de droits de propriété sur les données personnelles peut dès lors apparaître comme une revendication mort-née. Cependant, ces questions mettent en réalité en avant un ensemble de revendications de natures et visées bien plus variées. Au-delà de l'organisation économique d'un marché, émergent des revendications sociales visant à replacer l'internaute et l'ensemble de la collectivité au cœur des transformations de l'économie numérique. Ces revendications concernent aussi bien la préservation de la vie privée que le partage des valorisations et des revenus ou encore le rééquilibrage des relations de pouvoir entre plateformes et individus. Autant d'objectifs qui, tout en constituant des chantiers majeurs pour l'avenir, peuvent être atteints par d'autres moyens que l'instauration de droits de propriété, qui confine la vie privée dans un paradigme individualiste. Ce paradigme renvoie à deux aspects différenciés. D'un côté, le constat que le numérique offre la possibilité – nouvelle – d'un renoncement à certains aspects de sa vie privée en « échange » de services efficaces et souvent gratuits ou presque. C'est donc dans le sens de cette marchandisation que l'on peut parler d'individualisation de la vie privée à l'ère numérique. D'un autre côté, le débat porte sur le mode de régulation optimal de la vie privée numérique. Cette régulation passe-t-elle par une individualisation de la vie privée, c'est-à-dire par des négociations des internautes avec les offreurs de services, ou par des processus plus collectifs ?

La patrimonialisation des données s'inscrit dans une démarche individualiste, faisant de chacun le propriétaire de ses données et plaçant l'individu face à des plateformes qui ont un pouvoir de marché bien plus important. À l'inverse, si l'on prône une solution collective, on peut faire l'hypothèse qu'émergera une vie privée négociée dans un cadre impliquant à la fois les internautes qui sont entrés dans une phase non plus uniquement de consentement éclairé *ex ante*, cher au législateur français, mais de comportement éclairé et les plateformes qui, au fur et à mesure que le processus d'apprentissage des internautes se développe, vont devoir adapter leurs offres aux nouvelles demandes de respect de la vie privée. Ainsi pourraient être définies de nouvelles relations entre internautes, plateformes et instances de régulation, prenant en compte à la fois les individus et la nature en réalité très collective de la vie privée.

Les différentes pistes évoquées viennent ouvrir plusieurs voies qui, loin de constituer chacune LA réponse possible aux problématiques soulevées,

semblent devoir être empruntées et suivies en parallèle. On peut espérer que le Règlement européen parvienne à mettre progressivement en place un écosystème vertueux d'« autorégulation sous pression » et contribue à inventer la recette d'un plat savoureux, mêlant subtilement opportunités de l'économie numérique à l'heure du *big data* et respect de la vie privée ; les principaux ingrédients en seraient : une bonne dose de régulation publique articulant responsabilisation des acteurs et sanctions dissuasives, un zeste de techniques et une pincée d'arrangements institutionnels négociés collectivement.

BIBLIOGRAPHIE

- AARON GABISCH, J., MILNE, R. G. (2014), « The impact of compensation on information ownership and privacy control », *Journal of Consumer Marketing*, vol. 31, n° 1, pp. 13-26.
- ACKERMAN SHRIER, A., CHANG, A., DIAKUN-THIBAUT, N., FORNI, L., LANDA, F., MAYO, J., VAN RIEZEN, R. (2016), *Blockchain and Health IT: Algorithms, Privacy, and Data*, White paper for the Office of the National Coordinator for Health Information Technology U.S. Department of Health and Human Services.
- ACQUISTI, A. (2011), « Les comportements de vie privée face au commerce électronique. Une économie de la gratification immédiate », *Réseaux*, vol. 3, n° 167, pp. 105-130.
- AGRAWAL, R. (2002), « Why is P3P Not a PET? », W3C Workshop on the Future of P3P, Dulles, Virginia.
- ALLAIRE, G. (2013), « Les communs comme infrastructure institutionnelle de l'économie marchande », *Revue de la régulation*, 14, 2^e semestre.
- ANCI AUX, N., NGUYEN, B. (2015), « Gestion sécurisée de données personnelles », *Bulletin de la Société Informatique de France*, 1024, pp. 17-41.
- ARMSTRONG, M. (2006), « Competition in Two-Sided Markets », *RAND Journal of Economics*, vol. 37, n° 3, pp. 668-691.
- ARROW, K. (1962), « Economic welfare and the allocation of resources for invention », *The rate and direction of inventive activity: Economic and social factors*, Nber, pp. 609-626.
- BELLANGER, P. (2014), *La souveraineté numérique*, Paris, Stock, 253 p.
- BENSAMOUN, A., ZOLYNSKI, C. (2014), « Big data et privacy : comment concilier nouveaux modèles d'affaires et droits des utilisateurs ? », *Petites affiches*, 18 août, n° 164, pp. 8-12.
- BENSOUSSAN, A. (2010), « Propriété des données et protection des fichiers », *Gazette du Palais*, vol. 23, n° 296, p. 2.
- BROUSSEAU, E., MARZOUKI, M., MÉADEL, C. (2012), *Governance, Regulations and Power on the Internet*, Cambridge, Cambridge University Press.
- BROUSSEAU, E., PÉNARD, T. (2007), « The Economics of Digital Business Models: A Framework for Analyzing the Economics of Platforms », *Review of Network Economics*, vol. 6, n° 2, pp. 81-114.

- BRUGHIÈRE, J.-M. (2014), « Le “droit à” l’oubli numérique, un droit à oublier », *Recueil Dalloz*, p. 299.
- CASILLI, A. (2010), *Les liaisons numériques. Vers une nouvelle sociabilité ?*, Paris, Seuil, coll. « La couleur des idées », 131 p.
- CASILLI, A. (2013), « Contre l’hypothèse de la “fin de la vie privée” », *Revue française des sciences de l’information et de la communication*, 3.
- CASILLI, A. (2014), « Quatre thèses sur la surveillance numérique de masse et la négociation de la vie privée », in Conseil d’État, *Le numérique et les droits fondamentaux*, Paris, La Documentation française, pp. 423-434.
- CAVOUKIAN A. (2006), « Privacy by Design: The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices », https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.
- COASE, R. H. (1960), « The Problem of Social Cost », *Journal of Law and Economics*, vol. 3, pp. 1-44.
- CONSEIL D’ÉTAT (2014), *Le numérique et les droits fondamentaux*, Paris, La Documentation française, coll. « Les rapports du Conseil d’État », 441 p.
- CONSEIL NATIONAL DU NUMÉRIQUE (2014), *Neutralité des plateformes. Réunir les conditions d’un environnement numérique ouvert et soutenable*, Rapport remis au ministre de l’Économie, du Redressement productif et du numérique et à la secrétaire d’État chargée du numérique, 118 p.
- CRANOR, LORRIE FAITH (2002), *Web Privacy with P3P*, Sebastopol, California, O’Reilly & Associates, 344 p.
- CTRL-SHIFT (2014), *Personal Information Management Services: An analysis of an emerging market*, 38 p.
- DE MONTJOYE, Y.-A., SHMUELI, E., WANG, S. S., PENTLAND, A. S. (2014), « OpenPDS: Protecting the Privacy of Metadata through SafeAnswers » *PLoS ONE*, 9(7).
- DEMSETZ, H. (1967), « Toward a theory of property rights », *The American Economic Review*, pp. 347-359.
- DEMSETZ, H. (1970), « The Private Production of Public Goods », *Journal of Law and Economics*, vol. 13, n° 2, pp. 293-306.
- EVANS, D. S. (2003), « Some Empirical Aspects of Multi-Sided Platform Industries », *Review of Network Economics*, vol. 2, n° 3, pp. 191-209.
- FARCHY, J., DE LA TAILLE, M. (2017), *Libres (petits) enfants du numérique*, Paris, Presses des mines, à paraître.
- FARCHY, J., MÉADEL, C., SIRE, G. (2015), *La gratuité, à quel prix ?*, Paris, Presses des Mines, coll. « Les cahiers de l’EMNS », 132 p.
- FRIEDMAN, D. (2000), « Privacy and Technology », *Social Philosophy and Policy*, vol. 17, n° 2, pp. 186-212.
- HAGIU, A., WRIGHT, J. (2011), *Multi-Sided Platforms*, Harvard Business School, 38 p.
- HARDIN, G. (1968), « The Tragedy of the Commons », *Science*, vol. 162, n° 3859, pp. 1243-1248.
- JULLIEN, B. (2004), *Two-Sided Markets and Electronic Intermediaries*, CESifo Working Paper Series n° 1345.
- LANCELOT MILTGEN, G. (2011), « Vie privée et marketing », *Réseaux*, n°167, pp. 131-166.
- LANIER, J. (2014), *Who owns the Future?* London, Penguin Books, 372 p.
- LAUDON, K. C. (1996), « Markets and privacy », *Communications of the ACM*, vol. 39, n° 9, pp. 92-104.

- LAVAL, C. (2011), « La nouvelle économie politique des communs : apports et limites », *Journal du MAUSS* (en ligne).
- LEMOINE, P. (2014), *La nouvelle grammaire du succès. La transformation numérique de l'économie française*, Rapport au Gouvernement, 326 p.
- LERNER, A. V. (2014), *The Role of Big Data in Online Platform Competition*, 26 août, <https://ssrn.com/abstract=2482780>.
- LESSIG, L. (2000), « Code Is Law », *Harvard Magazine*, January-February.
- LITMAN, J. (2000), « Information Privacy/Information Property », *Stanford Law Review*, vol. 52, n° 5, pp. 1283-1313.
- MALLET-POUJOL, N. (1997), « Appropriation de l'information : l'éternelle chimère », *Recueil Dalloz*, p. 330.
- MÉADEL, C., MUSIANI, F. (DIR.) (2015), *Abécédaire des architectures distribuées*, Paris, Presses des Mines, 246 p.
- MERCIER, S. (2014), « Biens communs et données personnelles : il nous faut inventer ! », *Bibliobsession*, 12 mars.
- MOULIER-BOUTANG, Y. (2010), *L'abeille et l'économiste*, Paris, Carnets Nord, 256 p.
- MUSIANI, F. (2015), « Les architectures P2P. Une solution européenne originale pour la protection des données personnelles ? », *Réseaux*, n° 189, pp. 47-75.
- NEWMAN, N. (2014), « Search, Antitrust and the Economics of the Control of User Data », *Yale Journal on Regulation*, vol. 30, n° 3.
- NGUYEN, B. (2014), « Techniques d'anonymisation », *Statistique et société*, vol. 2, n° 4, décembre.
- NORBERG, P., HORNE, D. R., HORNE, D. A. (2007), « The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors », *Journal of Consumer Affairs*, vol. 41, n° 1, pp. 100-126.
- ORSI, F. (2013), « Elinor Ostrom et les faisceaux de droits : l'ouverture d'un nouvel espace pour penser la propriété commune », *Revue de la régulation*, vol. 14, 2^e semestre.
- OSTROM, E., BURGER, J., FIELD, C. B., NORGAARD, R. B., POLICANSKY, D. (1999), « Revisiting the Commons: Local Lessons, Global Challenges », *Science*, vol. 284, n° 5412, pp. 278-282.
- PERROT, A. (2011), « Le numérique : enjeux et questions de concurrence », *Concurrences*, n° 3.
- PEUGEOT, V. (2014), « Données personnelles : sortir des injonctions contradictoires », *vecam.org*, 13 avril.
- POLANYI, K. (1944), *La Grande Transformation*, Paris, Galimard, coll. « Tel » [1983], 476 p.
- RALLET, A., ROCHELANDET, F. (2011), « La régulation des données personnelles face au web relationnel : une voie sans issue ? », *Réseaux*, vol. 3, n° 167, pp. 17-47.
- RALLET, A., ROCHELANDET, F., ZOLYNSKI, C. (2015), « De la Privacy by Design à la Privacy by Using », *Réseaux*, vol. 3, n° 189, pp. 15-46.
- REY, P. J. (2012), « Alienation, Exploitation, and Social Media », *American Behavioral Scientist*, vol. 56, n° 4, pp. 399-420.
- ROCHELANDET, F. (2010), *Économie des données personnelles et de la vie privée*, Paris, La Découverte, coll. « Repères », 125 p.
- ROCHET, J.-C., TIROLE, J. (2003), « Platform competition in two-sided markets », *Journal of the European Economic Association*, vol. 1, n° 4, pp. 990-1029.

- ROCHFELD, J. (2014), « Une nouvelle source en droit des contrats : la loi Informatique et libertés », *Revue des contrats*, n° 1, pp. 119.
- SAMUELSON, P. (2000), « Privacy As Intellectual Property? », *Stanford Law Review*, vol. 52, n° 5, pp. 1125-1173.
- SCHOLZ, T. (DIR.) (2013), *Digital Labor: The Internet as Playground and Factory*, London, Routledge, 258 p.
- SCHWARTZ, P. M. (2004), « Property, Privacy, and Personal Data », *Harvard Law Review*, vol. 117, n° 7, pp. 2056-2128.
- SMYRNAIOS, N. (2017), *Les GAFAM contre l'Internet : une économie politique du numérique*, Paris, INA Éditions, 131 p.
- SONNAC, N., GABSZEWICZ, J. (2010), *L'industrie des médias à l'ère numérique*, Paris, la Découverte, coll. « Repères », 126 p.
- STAR, S. L. (1999), « The Ethnography of Infrastructure », *American Behavioral Scientist*, vol. 43, n° 3, pp. 377-391.
- THORP, J. (2012), « Big Data is Not the New Oil », *Harvard Business Review*, 30 novembre.
- WEINSTEIN, O. (2013), « Comment comprendre les “communs” : Elinor Ostrom, la propriété et la nouvelle économie institutionnelle », *Revue de la régulation*, n° 14, 2^e semestre.
- ZITTRAIN, J. (2000), « What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication », *Stanford Law Review*, vol. 52, n° 5, pp. 1201-1250.