Les glissements du droit à la vie privée. De Feydeau à Facebook : de la comédie de mœurs à l'économie des données

Karim Benyekhlef*

* Professeur, Titulaire de la Chaire LexUM et directeur du Laboratoire de cyberjustice, Faculté de droit, Université de Montréal.

Introduction

Le droit à la vie privée n'a pas manqué d'intéresser Patrick Molinari[1]. Voilà un droit qui, à partir des années 1970, a suscité un vif intérêt de la doctrine juridique d'ici et d'ailleurs en raison notamment de l'évolution des techniques qui posait alors un rapport inédit d'immédiateté et de facilité d'accès entre l'information, la donnée raffinée et l'organisation sociale, soit-elle privée ou publique. Il n'en fallait pas plus pour interpeller Patrick Molinari et l'inciter à réfléchir à ces nouveaux rapports.

I. La révolution numérique et l'accélération du temps

La révolution numérique de l'information, induite par les développements technologiques des quarante dernières années et, en particulier l'essor de l'Internet grand public grâce au *World Wide Web*, ne cesse de transformer nos manières de faire, d'écouter, de lire ou de regarder. Des stratégies industrielles et économiques tentent d'imposer des modèles au nom d'un concept aujourd'hui largement galvaudé de l'innovation. On recourt ainsi aux notions d'innovation ou de *disruption* pour justifier la mise au rancart de régulations qui, en fait, constituent des obstacles à des stratégies industrielles. Une rhétorique vaguement conceptuelle de la nouveauté se met en place, dérisoire cache-sexe d'intérêts commerciaux et industriels. Un *story-telling* qui fait la part belle à la nouveauté, à la modernité, au changement, au progrès et qui suggère de nouvelles façons de faire, des solutions qui correspondent aux produits ou services à écouler... Les travaux d'Evgeny Morozov démontrent à l'envi que le *solutionnisme* des industriels du web propose des solutions à des problèmes qui n'existent pas vraiment[2]. Ainsi, certains, comme Martin Wolf, estime que la révolution numérique ne porte pas autant d'innovations et de changements que la seconde révolution industrielle qui apparaît vers 1870 et se termine au début du XX^{e} siècle :

---

1 Lire notamment : Patrick A. MOLINARI et Pierre TRUDEL, « Le droit au respect de l'honneur, de la réputation et de la vie privée : aspects généraux et applications », dans *Applications des chartes des droits et libertés en matière civile*, Cowansville, Éditions Yvon Blais, 1988, p. 197 et Patrick A. MOLINARI, « Les nouveaux moyens de reproduction et les droits de la personnalité », (1986) 46 *R. du B*. 717.

2 Lire notamment Evgeny MOROZOV, *To Save Everything, Click Here*, New York, Public Affairs, 2013.

> Indeed, past innovations generated vastly greater unmesuared value that the relatively trivial innovations of today. Just consider the shift from a world without telephones to one with them, or from a world of oil lamps to one with electric light. Next to that, who cares about Facebook or the iPad? Indeed, who really cares about the Internet when one considers clean water and flushing toilets?[3]

Et Wolf énumère les inventions de cette seconde révolution industrielle : la voiture, le réfrigérateur, l'eau courante, les vaccins, le gaz, la cuisinière électrique, la machine à laver, l'aspirateur, le chemin de fer, la radio, le gramophone, la télévision etc. L'auteur note que ces inventions ont modifié radicalement la vie quotidienne. En fait, ajoute Wolf pour illustrer cette radicale évolution, « an ancient Roman would have understood the way of life of the United States of 1840 fairly well. He would have found that of 1940 beyond his imagination »[4]. Ces clarifications devraient tempérer la propension bien actuelle à glorifier et à surestimer l'innovation technologique. Chaque époque est évidemment obsédée par elle-même et la nôtre n'échappe pas à cet égotiste constat. Au contraire. S'il est peut-être vrai que les inventions de la seconde révolution industrielle ont modifié plus radicalement la vie et les rapports sociaux que ne le font celles d'aujourd'hui, l'observateur attentif ne peut manquer de noter l'accélération permanente des interactions individuelles et collectives, des rapports sociaux, des exigences du travail etc. de l'époque contemporaine. Et cette accélération induit sans doute des changements plus radicaux dans les manières de faire et d'être. Harmut Rosa note que cette accélération du temps, que chacun ressent bien dans sa vie quotidienne, n'est pas causée par les inventions technologiques récentes ; ces dernières sont plutôt « des réponses au problème croissant du manque de temps »[5]. Pourtant, ces réponses ne nous ont pas apporté plus de temps, elles participent en fait à une course encore plus effrénée. Rosa identifie trois causes générales à cette accélération du temps dans laquelle la modernité est enga-

---

3 Martin Wolf, « Same as It Ever Was. Why the Techno-Optimist Are Wrong », (2015) July/August *Foreign Affairs*, 15, 16.

4 *Id*., 17. On lira aussi avec intérêt l'ouvrage de Robert J. Gordon, *The Rise and Fall of American Growth*, Princeton, Princeton University Press, 2016, p. 566, duquel Martin Wolf s'inspire largement.

5 Harmut Rosa, *Aliénation et accélération. Vers une théorie critique de la modernité tardive*, Paris, La Découverte, 2012, p. 33.

gée. Celle qui nous intéresse au premier chef a partie liée à la technique[6] : « Ainsi, l'accélération sociale en général et l'accélération technique en particulier sont une conséquence logique d'un système de marché capitaliste concurrentiel »[7]. Cette concurrence « excède largement la sphère économique » pour devenir « le mode dominant de distribution dans à peu près toutes les sphères de la vie sociale et par conséquent un principe central de la modernité »[8]. Il existe ainsi, selon l'auteur, une véritable compétition « dans la lutte pour les liens sociaux ». Les réseaux sociaux, comme Facebook ou Twitter notamment, exercent une pression sociale concurrentielle très forte. Cette « logique sociale de la compétition est telle que les concurrents doivent investir une énergie accrue pour rester compétitifs, jusqu'au point où cet effort n'est plus un moyen de mener une vie autonome en fonction de buts autodéfinis, mais le seul but général de la vie, tant sociale qu'individuelle »[9]. Ces constats sociologiques doivent servir d'arrière-plan obligé à toute réflexion sur la portée et le déploiement du droit à la vie privée aujourd'hui. On y reviendra.

II. Un web centralisé et la publicité comme modèle d'affaires

L'Internet d'aujourd'hui a bien sûr considérablement évolué depuis le milieu des années 1990 et son ouverture au monde commercial avec l'apparition du *world wide web*. Beaucoup des préventions de l'époque n'ont plus cours aujourd'hui. Ainsi, il était courant d'affirmer que le souverain devait s'abstenir de toute intervention normative sur Internet car les acteurs étaient encore émergents et les modèles d'affaires à définir. On se souviendra en effet que, dans les débuts du web grand public, on entendait souvent le commentaire selon lequel toute intervention du souverain

---

6 Il s'agit là pour Harmut Rosa de « la principale force motrice de l'accélération sociale » (*id*., p. 38). Un autre moteur, culturel celui-là, a partie liée à la promesse d'éternité. Rosa écrit à la p. 38 : « (...) dans la société moderne séculaire, l'accélération sert d'équivalent fonctionnel à la promesse (religieuse) de *vie éternelle* ». La technique et la promesse d'éternité constituent des forces motrices externes, nous explique l'auteur. La troisième cause est cette fois interne en ce qu'elle s'incarne dans l'accélération elle-même, créant ainsi une boucle autoalimentée : « Cependant, dans la modernité tardive, l'accélération sociale s'est transformée en un système autopropulsé qui n'a plus besoin de la moindre force motrice externe », (*id*., p. 40).

7 *Id*., p. 34.

8 *Id*., p. 35.

9 *Id*., p. 37.

serait dangereuse, car elle aurait pour effet d'inhiber l'innovation et la détermination des stratégies industrielles des acteurs. De même, il était dit que la nature décentralisée d'Internet s'opposait à toute intervention efficace du souverain. Bien que ces prétentions conservent une certaine pertinence, elles doivent être nuancées au regard de la centralisation effective d'Internet par les grands joueurs que sont Google, Amazon, Facebook, Apple, etc. L'appropriation quasi littérale du web par ces géants a pour effet de centraliser Internet et de le rendre ainsi beaucoup plus perméable à une régulation, que celle-ci émane des acteurs eux-mêmes (et ils ne s'en privent pas) ou des régulateurs habituels que sont les États et leurs composantes. Un facteur psychologique fait aussi son œuvre depuis quelque temps déjà : Internet a perdu de sa mystique technologique et est bien mieux compris par les États qu'il ne le fut à ses débuts. Par conséquent, il devient plus difficile d'enfumer le souverain, de le leurrer par un discours technologique qui avait aussi pour objectif de le *ringardiser*, même si le *story-telling* des acteurs industriels continue d'opérer dans les cercles du pouvoir. Les modèles d'affaires de ces géants sont aujourd'hui clairs : ce sont essentiellement des régies publicitaires qui récoltent des données personnelles et les vendent ou les utilisent pour des publicités ciblées[10] (Google et Facebook entre autres). Apple et Amazon ont créé des écosystèmes de commerce électronique autour, pour le premier, de ses propres produits et services et, pour le second, d'une formidable variété de produits et services. Mais ces deux entreprises utilisent également les données afin de les transformer en informations à valeur ajoutée pour diverses fins, dont bien sûr celle de la publicité. En acquérant la régie publicitaire Doubleclick en 2008, Google se serait accaparé environ 69 % du marché publicitaire du web[11]. Le modèle d'affaires de Facebook se fonde d'abord et avant tout sur les données personnelles générées par les activités de ses abonnés. On doit ici reconnaître, à l'instar de Martin Wolf, que ces modèles d'affaires ne se signalent pas par leur nature innovante.

---

10 « Lorsque ces plateformes ont fini par acquérir une position d'oligopole (GAFA [Google, Apple, Facebook, Amazon]), les gouvernements ont constaté que tout leur modèle économique reposait sur la prédation de ces traces d'activités, et parfois de données nominatives, qui étaient soit exploitées pour proposer des placements publicitaires sur les plateformes elles-mêmes soit revendues à d'autres partenaires. », Dominique BOULLIER, *Sociologie du numérique*, Paris, Armand Colin, 2016, p. 278.

11 https://searchenginewatch.com/sew/news/2054513/google-doubleclick-69-online-advertising-market (consulté le 1er septembre 2016)

Dominique Boullier estime, pour sa part, que Google et Facebook sont en compétition pour devenir l'état civil numérique du XXIe siècle en centralisant des fonctions d'identification et d'accès (accès à partir de son compte Facebook à des services à accès restreint), les rapprochant alors de la première génération des sciences sociales (selon la classification de Boullier) préoccupées par le recensement et la quantification de la société humaine. Alors qu'Apple et Amazon ont pour ambition une connaissance totale des goûts et des connaissances, les rapprochant cette fois des sciences sociales de la seconde génération marquées par le recours aux sondages et les *mass media*[12]. Toujours selon Boullier, Twitter préfigure la troisième génération des sciences sociales annoncée par la réplication, les traces et les marques. Dans tous ces cas, le capitalisme financier est le modèle de ces plateformes[13].

Le marché des données personnelles a permis l'émergence d'acteurs et d'activités ayant pour objet de collecter, apparier, raffiner, entrecouper, traiter, louer, vendre des informations personnelles. Internet, aventure d'abord universitaire, a permis les échanges commerciaux sur le réseau dès 1995. Les premiers usagers grand public, habitués à la gratuité des échanges, caractéristique essentielle de l'Internet universitaire, rechignent encore aujourd'hui à payer pour l'obtention d'informations ou de services. Les opérateurs ont alors fait de la publicité leur moyen premier pour générer des profits[14]. Les données personnelles constituent à cet égard une

---

12 Dominique BOULLIER, *Sociologie du numérique*, Paris, Armand Colin, 2016.

13 La doctrine évoque l'émergence d'un capitalisme cognitif intrinsèquement lié à l'émergence des biens dématérialisés et à l'économie dite du savoir : lire notamment Michael A. PETERS et Ergin BULUT (dir.), *Cognitive Capitalism, Education and Digital Labor*, New York, Peter Lang Publishing, 2011 et Yann MOULIER-BOUTANG, *Le capitalisme cognitif : la nouvelle grande transformation*, Paris, Éditions Amsterdam, 2007.

14 Il faut reconnaître, avec Dominique Boullier, que le modèle gratuit a cédé le pas dans certains secteurs offrant des contenus (musique, film et séries télé et on pense à Spotify, Deezer ou Netflix), mais que ce modèle aura pris une quinzaine d'années à s'établir : « Le gratuit ne serait donc qu'une phase transitoire d'Internet qui cherche son modèle économique. À partir du moment où les offres commerciales proposent un accès illimité à tous les catalogues, le consentement à payer augmente considérablement et réduit l'intérêt du piratage, qui suppose encore quelques efforts techniques. La musique en continu qui ressemble finalement à l'écoute de la radio, les catalogues de films ou de séries télé sans limites sont désormais installés dans les habitudes et les abonnements deviennent attractifs. Mais il a fallu quinze ans pour réorganiser toute cette chaîne et rien ne dit qu'elle ne sera pas bouleversée par d'autres innovations. », Dominique BOULLIER, *Sociologie du numérique*, Paris, Armand Colin, 2016, p. 198.

matière première de grande importance et leur numérisation les rend encore plus propices à une utilisation publicitaire. La commercialisation des données devient donc la pierre d'assise des modèles d'affaires de l'Internet. Le courtage de données (*data brokerage*), l'émergence des données massives (*big data*), les modes de stockage et de gestion des données (*cloud computing*), l'analyse/forage de données (*data analytics/mining*) ou la volonté de faciliter un accès sans entrave aux données publiques (*open data*) constituent des déclinaisons de cette commercialisation débridée. Dominique Boullier écrit à ce propos :

> Pourtant, en restant au plus près de l'architecture technique et des modèles économiques de ces plateformes, il apparaît que la clé du succès financier de ces plateformes réside avant tout dans leur capacité de prédation des données et traces personnelles pour les revendre aux marques (...) Ce moment que l'on présente comme l'âge des foules et de leurs contributions ouvertes est en fait devenu une carrière de données à ciel ouvert, données que l'on peut fouiller gratuitement (*data mining*) et qui génèrent d'autant plus de revenus que ces plateformes sont devenues des « points de passage obligés » (pour les utilisateurs et pour les marques) et écrasent et dévorent leurs concurrents comme l'ont fait Facebook et Google (...)[15].

La maîtrise de la donnée devient l'objectif et le défi de l'entrepreneur de ce début de siècle.

III. Du folklore du droit à la vie privée : un glissement perceptible

La question de la protection des données personnelles relève, en droit, de l'ensemble plus général du droit à la vie privée. Les données personnelles constitueraient la dimension *informationnelle* du droit à la vie privée. Les deux autres dimensions, nous dit le juge La Forest dans l'arrêt *Dyment*[16], se rattachent à la personne et à l'espace (domicile, bureau etc.). Dans cet arrêt et dans l'affaire *Hunter*[17], la Cour suprême nous rappelle que l'article 8 de la *Charte canadienne des droits et libertés*, qui assure une protection contre les perquisitions, les fouilles ou les saisies abusives, ne saurait être restreint, malgré ses origines de *common law*, à une con-

---

15 *Id*., p. 83.

16 *La Reine* c. *Dyment*, [1988] 2 R.C.S. 417.

17 *Hunter* c. *Southam Inc*., [1984] 2 R.C.S. 145.

ception purement spatiale ou propriétaire. Autrement dit, on ne saurait limiter l'application de cette disposition constitutionnelle à une simple protection contre les intrusions de l'État au domicile des citoyens, dans leur *espace* privé. Ainsi, l'article 8, malgré un libellé fort étroit, institue un véritable droit à la vie privée en matière constitutionnelle au Canada. On ne reviendra pas ici sur les difficultés relatives à la définition d'un droit qui échappe naturellement à ces tentatives car il relève plus du principe que de la règle. Le juge La Forest l'a bien compris dans *Dyment* en se contentant de simplement circonscrire les dimensions ou les espaces où le droit à la vie privée peut jouer et se déployer : le corps (protection contre les intrusions corporelles), l'espace (le domicile, le bureau, les lieux publics selon certaines conditions, etc.) et l'information. Il a sciemment évité de donner un sens plus précis à une notion qui doit être fluctuante car elle relève essentiellement du contexte social et des interactions qui se nouent dans et entre les espaces publics et privés.

Cette difficulté d'assigner un sens précis au droit à la vie privée explique-t-elle l'approche longtemps inactuelle, pour ne pas dire désuète, de la Cour suprême dans son appréhension de ce droit au plan constitutionnel ? L'arrêt *Plant*[18] et son concept de *biographical core* (cœur biographique) en est une saisissante illustration. Il s'agit là d'une décision fondamentale en matière d'attente raisonnable du droit à la vie privée au regard de sa dimension informationnelle. Dans cet arrêt, la Cour suprême du Canada élabore l'approche dite du « biographical core » ; approche selon laquelle les individus ne peuvent revendiquer une attente raisonnable en matière de vie privée informationnelle qu'à l'égard des renseignements personnels qui sont de nature biographique et qui révèlent des détails intimes sur leur mode de vie. Dans cette affaire, une source anonyme a indiqué aux policiers la présence d'une culture de chanvre indien dans le sous-sol d'une maison. Les policiers ont vérifié le niveau de consommation d'électricité à l'adresse donnée et ont constaté que celle-ci était quatre fois supérieure au niveau de consommation moyen pour cette période. Ils ont ensuite obtenu un mandat de perquisition sur la foi d'une dénonciation comprenant les renseignements sur le niveau de consommation d'électricité. La question se pose alors de savoir si les informations relatives à la consommation d'électricité sont couverts ou non par une attente raisonnable à la vie privée. La majorité de la Cour estime que ce type d'informations n'est pas protégé par l'article 8 :

---

18 *R.* c. *Plant*, [1993] 3 R.C.S. 281.

> [P]our que la protection constitutionnelle s'applique, les renseignements saisis doivent être de *nature « personnelle et confidentielle »*. Étant donné les valeurs sous jacentes de dignité, d'intégrité et d'autonomie qu'il consacre, il est normal que l'art. 8 de la *Charte* protège un ensemble de renseignements biographiques d'ordre personnel que les particuliers pourraient, dans une société libre et démocratique, vouloir constituer et soustraire à la connaissance de l'État. Il pourrait notamment s'agir de renseignements tendant à révéler des *détails intimes* sur le mode de vie et les choix personnels de l'individu. Or, on ne saurait raisonnablement prétendre que les dossiers informatisés consultés dans la présente affaire, lesquels font état du niveau de consommation d'électricité dans une résidence, dévoilent des détails intimes de la vie de l'appelant, la consommation d'électricité ne révélant que très peu de chose du mode de vie ou des décisions privées de l'occupant de la résidence[19].

Cette approche du droit à la vie privée nous ramène à une conception pittoresque du droit à la vie privée, celle de la bourgeoisie du XIX^{e} siècle soucieuse de sa réputation et effrayée à l'idée que les maris cocufiés, les enfants bâtards, les épouses infidèles et les amants dans le placard ne soient l'objet de la risée générale. Ces *détails intimes*, que la Cour suprême évoque, relèvent d'une véritable comédie de mœurs à la Feydeau. La vie privée, dans un tel contexte, relève du secret des familles et d'une morale bourgeoise qui déplore le dévoilement des infidélités ou des pratiques sexuelles, des informations financières (salaire, fortune etc.), des addictions (alcool, drogue, médicaments, jeu etc.), des particularismes familiaux et autres détails qui font le sel des potins de la bourgeoisie. Sans vouloir diminuer la nature intime de ces détails et l'importance de les protéger, il faut noter que ceux-ci ne constituent plus aujourd'hui que la partie émergée de la vie privée, sa face la plus immédiate et celle qui la fonde, dans un imaginaire modelé par les pratiques sociales, religieuses et culturelles. L'avènement de l'Internet et du numérique, sans remettre en cause ces tabous de la vie sociale, déplace en quelque sorte le curseur public/privé de la stricte morale bourgeoise vers la prise en compte de détails anodins ou triviaux qui, ensemble, instituent des mécanismes de surveillance, de contrôle, de conformité sociale et d'enrégimentation qui remisent Feydeau au rayon du folklore. La vie privée ne relève plus simplement de la morale ; elle revêt une claire dimension politique. Il est inu-

---

[19] *Id.*, 293 [nos italiques].

tile de revenir sur les multiples traces laissées par l'individu lorsqu'il navigue sur Internet : historique de navigation, cookies, numéro d'IP, recherches enregistrées sur Google et autres moteurs de recherche etc. Ces traces anodines et malgré le fait qu'elles soient souvent anonymes permettent de suivre l'individu, d'en tirer un clair portrait et profil et, en fait, assurent une filature de tous les instants dans tous les champs de l'activité humaine. Par ailleurs, l'anonymisation n'est pas une garantie, car il est aujourd'hui démontrée que des données anonymes peuvent être désanonymisées[20] et permettent l'identification des personnes.

Cette réalité numérique tisse un faisceau d'observations que la Cour suprême a longtemps ignoré. Ainsi, l'approche de la Cour dans *Plant* fait qu'elle doit ignorer ces bribes d'informations qui ne révèlent rien directement et isolément sur la vie intime des individus : elles ne sont pas « des détails intimes sur le mode de vie et les choix personnels de l'individu », pour reprendre l'expression de la Cour. Elles ne relèvent donc pas de l'attente raisonnable en matière de vie privée. Ce constat n'a pas échappé à Jane Bailey lorsqu'elle affirme :

> While law enforcement's use of a surveillance technology in a single instance may seem relatively unconcerning when considered in the context of a single use against a single individual, the social implications of surveillance practices that involve the collection and assembly of seemingly harmless bits of information go largely unnoticed. Once a section 8 violation has been found, the current analysis seems to allow greater latitude for Canadian courts to move beyond the immediate implications for the individual claimant in order to take into account the broader social implications of the state surveillance practice involved. Unfortunately, the paradigmatically narrow individualistic focus that searches for personally or territorially intrusive practices vis-à-vis the individual claimant may reduce the chance of a court finding that a section 8 violation has occurred in relation to data gathering and collection in the first place[21].

---

20 Arvind Narayanan et Vitaly Shmatikov, « Robust De-Anonymization of Large Sparse Datasets (How to Break Anonymity of the Netflix Prize Dataset) », (2008) *Proc. 29th IEEE Symposium on Security & Privacy* 111, en ligne : https://arxiv.org/pdf/cs/0610105.pdf (consulté le 1er septembre 2016).

21 Jane Bailey, « Framed by Section 8 : Constitutional Protection of Privacy in Canada », (2008) *R.C.C.J.P.* 279, 302.

Ce faisceau d'observations des individus, induit par le numérique et Internet pose dorénavant une question *politique* essentielle. Bien que le droit à la vie privée ne soit pas dénué d'une dimension politique, pensons, par exemple, à la question du discours politique anonyme, il ne s'agissait là que d'un aspect mineur de ce droit. Les libertés d'expression et d'opinion prenaient, en effet, rapidement le relais afin d'assurer un accès libre au marché des idées et une autonomie propre à permettre à l'individu de se forger sa propre opinion. La question devient politique car elle pose celles de l'équilibre des pouvoirs dans une démocratie, du degré de liberté et d'autonomie de l'individu, de sa capacité à échapper au regard de l'autre (que ce soit l'État, les entreprises ou les citoyens), de son refus du conformisme social et de l'étiquetage behavioral, bref du type de société dans laquelle vivre. Ces arrangements socio-politiques relèvent du débat public démocratique et non des politiques industrielles prônées par les géants d'Internet. Dans un article récent, Elizabeth Stoycheff démontre que les révélations d'Edward Snowden concernant la surveillance systématique pratiquée par la NSA ont eu un effet délétère sur l'autonomie des individus en les forçant à un conformisme et à une *doxa* politiques : « This is the first study to provide empirical evidence that the government's online surveillance programs may threaten the disclosure of minority views and contribute to the reinforcement of majority opinion »[22] . Elle ajoute :

> These individuals [les participants à l'étude] expressed that surveillance was necessary for maintaining national security and they have nothing to hide. However, when these individuals perceive they are being monitored, they readily conform their behavior – expressing opinions when they are in the majority, and suppressing them when they're not[23].

Ainsi, même ceux qui plastronnent qu'ils n'ont rien à cacher ont finalement des choses à cacher, qu'elles relèvent du comportement ou de l'opinion. Daniel Solove avait bien démontré que cet argument (*nothing to hide*) ne se limite pas à cacher des actes délictueux ou criminels, mais bien tout *fait* qui peut ou risque de pouvoir nous mettre dans l'embarras

---

22 Elizabeth STOYCHEFF, « Under Surveillance : Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring », (2016) *Journalism & Mass Communication Quaterly* 1, 12.

23 *Id.*

ou nous nuire[24]. Et, bien évidemment à cet égard, nous avons tous quelque chose à cacher.

Les réseaux numériques facilitent certes la surveillance et le contrôle par les autorités publiques, mais accroissent également la surveillance latérale[25], c'est-à-dire la surveillance des individus par les individus. Ceci apparaît très clairement dans les réseaux sociaux, comme Facebook. On semble revenir à un environnement propre aux régions rurales, les petits villages ou les petites communautés, dans lesquels chacun sait ce que fait, voire pense, l'autre. L'urbanisation nous avait délivré en partie des commérages propres aux petites communautés fermées. Dans l'univers des réseaux, cette promiscuité réapparaît avec plus de force encore, puisque ces réseaux rassemblent souvent un nombre important d'agents. Les effets de cette surveillance sont nombreux et, avec Dominique Cardon[26], il faut reconnaître que les agents sont conscients de celle-ci. Le jeune âge des agents fait parfois croire que ceux-ci méconnaissent les paramètres généraux de la vie privée. Il n'en est rien. Les agents se mettent en scène et veulent bien montrer ce qui leur convient. Il ne faut pas en effet interpréter « l'actuation de formes de dévoilement stratégique d'informations personnelles à des fins de gestion du capital social en ligne » comme une forme de « renonciation intégrale à la privacy »[27]. Il importe alors d'éviter de confondre une stratégie de gestion du capital social qu'entretiennent les usagers des réseaux sociaux avec une méconnaissance du droit à la vie privée.

---

24 Daniel J. SOLOVE, *Nothing to Hide. The False Tradeoff between Privacy and Security*, New Haven, Yale University Press, 2011.

25 Sur les réseaux sociaux et la visibilité, lire Dominique CARDON, « Le design de la visibilité : un essai de typologie du web 2.0 », en ligne : http://www.internetactu.net/2008/02/01/le-design-de-la-visibilite-un-essai-de-typologie-du-web-20/ (consulté le 1er septembre 2016).

26 Dominique CARDON, *La démocratie Internet. Promesses et limites*, Paris, Seuil-La République des Idées, 2010, p. 64 et suiv. Cardon évoque aussi l'idée d'un « panoptisme horizontal » pour désigner la « surveillance » par les pairs.

27 Antonio A. CASILLI, « Contre l'hypothèse de la "fin de la vie privée". La négociation de la privacy dans les médias sociaux », (2013) 3 *Revue française des sciences de l'information et de la communication* 5, en ligne : http://rfsic.revues.org/630 (consulté le 1er septembre 2016).

Mais, la gestion d'un capital social suppose bien entendu le regard de l'autre. Cette conscience du regard de l'autre, qui est une condition d'appartenance à ces communautés, participe donc d'une surveillance qui, là aussi, ne manque pas d'induire un profond effet de conformisme. Une *spirale du silence* se met alors en place. Cette notion, introduite en 1974, par Elizabeth Noelle-Neumann[28], veut que les individus policent, voire censurent, leurs discours et leurs actions en fonction de l'inclination de l'auditoire :

> It fundamentally contends that individuals, motivated by fear of isolation, continuously monitor their environments to assess whether their beliefs align with or contradict majority opinion (...) Consequently, perceptions of an incongruent, or hostile, opinion climate reduce individuals' willingness to speak out, leading to a silencing of minority attitudes over time and posing a threat to democratic discourse[29].

Cette spirale du silence perdure dans les espaces numériques, ainsi que l'ont démontré plusieurs études citées par Elizabeth Stoycheff, et constitue une réfutation de l'affirmation selon laquelle les réseaux libèrent totalement la parole :

> Participants confronted with hostile opinion climates have been equally as unlikely to express their opinions online as they are offline, lending additional evidence that computer-mediated spiral of silence effects may be just as pervasive as those that occur face to face (...) In sum, these initial studies provide little evidence that online contexts significantly liberate the expression of minority opinions or reduce conformist behavior[30].

Ainsi, la spirale du silence se vérifie dans les réseaux sociaux, les « chatrooms », les sites de blogues etc. Tous ces phénomènes doivent bien entendu être pris en compte dans une appréhension contemporaine du droit à la vie privée. Il ne s'agit plus dès lors de protéger simplement une liaison adultère, des mœurs sexuelles singulières, un revers de fortune ou

---

28 Elizabeth NOELLE-NEUMANN, « The Spiral of Silence. A Theory of Public Opinion », (1974) 24 :2 *Journal of Communications* 43.

29 Elizabeth STOYCHEFF, « Under Surveillance : Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring », (2016) *Journalism & Mass Communication Quaterly* 1, 2.

30 *Id*., 3.

une dispute familiale, mais d'assurer que l'ensemble des gestes quotidiens de la vie d'un internaute, pris dans la nasse de la surveillance et du monitoring, soit l'objet d'une analyse plus fine qui s'intègre dans la définition du périmètre du droit à la vie privée. À cet égard, il faut reconnaître que la jurisprudence récente de la Cour suprême évolue dans le bon sens et recoupe, sous certains aspects, certaines déterminations établies par les agences de protection des données personnelles.

Dans l'affaire *Morelli*[31], la Cour suprême du Canada perçoit clairement l'importance des traces numériques conservées dans un ordinateur. Le détenteur d'un ordinateur peut entretenir des attentes raisonnables élevées en matière de vie privée :

> [105] Comme je l'ai souligné tout au début, il est difficile d'imaginer une atteinte plus grave à la vie privée d'une personne que la perquisition de son domicile et la fouille de son ordinateur personnel. En effet, nos ordinateurs contiennent souvent notre correspondance la plus intime. Ils renferment les détails de notre situation financière, médicale et personnelle. Ils révèlent même nos intérêts particuliers, préférences et propensions, enregistrant dans l'historique et la mémoire cache tout ce que nous recherchons, lisons, regardons ou écoutons dans l'Internet. [106] On peut donc difficilement concevoir une violation de l'art. 8 ayant des répercussions plus graves sur le droit à la protection de la vie privée que la *Charte* garantit à l'accusé que celle dont il est question en l'espèce.

La Cour suprême réitère l'attente raisonnable en matière de vie privée à l'égard des ordinateurs et englobe aussi les téléphones dits intelligents dans l'arrêt *Vu*[32]. Dans cette affaire, la question se pose de savoir si un mandat de perquisition dans une maison d'habitation permet de saisir et de fouiller un ordinateur et un téléphone intelligent qui ne sont pas mentionnés dans la demande de mandat. Le *Code criminel*, à son article 487, permet en effet au détenteur d'un mandat de perquisition de fouiller tout contenant se trouvant sur les lieux de la perquisition (un placard fermé, un classeur, un coffre etc.). La Cour rappelle l'importance des données numériques dans le contexte contemporain et la quantité phénoménale de données stockées dans les ordinateurs[33]. Le téléphone peut être saisi,

---

31 *R.* c. *Morelli*, [2010] 1 R.C.S. 253.

32 *R.* c. *Vu*, [2013] 3 R.C.S. 657.

33 *Id.*, par. 41.

mais il ne saurait constituer un contenant *ordinaire* ; on doit donc obtenir un *autre* mandat pour en fouiller le contenu. Le juge Cromwell poursuit en évoquant les traces numériques que chacun sème souvent à son insu :

> (...) il arrive souvent que les logiciels de traitement de texte génèrent automatiquement des fichiers temporaires permettant aux analystes de reconstituer l'élaboration d'un fichier et d'avoir accès à des renseignements indiquant qui a créé le fichier et qui y a travaillé. De même, la plupart des navigateurs utilisés pour consulter Internet sont programmés pour conserver automatiquement des renseignements concernant les sites Web que l'utilisateur a visités dans les semaines précédentes, ainsi que les syntagmes de recherche qu'il a utilisés pour y accéder. Normalement, ces renseignements peuvent aider l'utilisateur à retracer ses démarches cybernétiques. Dans le contexte d'une enquête criminelle, toutefois, ils peuvent également permettre aux enquêteurs d'avoir accès à des détails intimes concernant les intérêts, les habitudes et l'identité de l'utilisateur, à partir d'un dossier que ce dernier a créé sans le savoir[34].

L'évolution de l'analyse de la Cour suprême du droit à la vie privée dans un contexte criminel est marquée. La position de *Vu* est réitérée dans *Fearon*, sous la plume majoritaire du juge Cromwell. Mais la dissidence, sous la plume de la juge Karakatsanis, va plus loin en identifiant clairement la *variété* des traces numériques que nous pouvons semer et, surtout, les recoupements et les croisements qui peuvent être faits à partir de ces traces anodines produisant des profils complets de l'utilisateur :

> Les appareils numériques personnels enregistrent non seulement nos renseignements biographiques, mais aussi nos conversations, nos photos, les sites sur le Web qui nous intéressent, les données concernant nos achats ainsi que nos loisirs. Notre empreinte numérique est souvent suffisante pour reconstituer les événements de notre vie, nos relations avec les autres, nos goûts et nos aversions, nos craintes, nos espoirs, nos opinions, nos croyances et nos idées. Nos appareils numériques sont en quelque sorte des fenêtres sur notre vie privée intérieure[35].

La juge Karakatsanis affirme, avec justesse, que le droit doit évoluer au même rythme que les technologies numériques afin d'assurer une pro-

---

34 *Id*., par. 42.

35 *R*. c. *Fearon*, [2014] 3 R.C.S. 621, par. 101.

tection effective du droit à la vie privée[36]. Évoquant les téléphones intelligents, qui sont aujourd'hui aussi puissants que des ordinateurs, la juge reconnaît que, tous les jours, « nos téléphones cellulaires documentent à tel point nos activités qu'il est possible d'en tirer un large éventail de données – de nos interventions sur les médias sociaux à nos habitudes alimentaires, des fils de nouvelles que nous suivons aux médicaments que nous consommons »[37]. Ces appareils ont une telle capacité de captation des détails les plus anodins de nos activités quotidiennes que « toute intrusion dans ces appareils constitue une atteinte sans précédent à notre vie privée »[38].

Dans l'arrêt *Spencer*[39], la Cour suprême tranche finalement la question de savoir si le numéro d'IP d'un ordinateur relève d'une attente raisonnable en matière de vie privée. On se souviendra que les autorités publiques ont longtemps soutenu que le numéro d'IP était comme un numéro de téléphone et ne pouvait donc constituer une composante de la vie privée d'un individu. La Cour rejette cet argument et cite avec approbation le juge de première instance :

> [Traduction] Qualifier de tels renseignements de simples « renseignements relatifs à l'abonné » ou de « renseignements sur le client » ou encore de rien d'autre que de « renseignements sur le nom, l'adresse et le numéro de téléphone » tend à occulter leur véritable nature. Je tiens à le préciser, parce que ces qualifications font abstraction de l'importance d'une adresse IP et des renseignements que cette adresse, une fois liée à une personne en particulier, peut révéler sur cette personne, notamment les activités en ligne que celle-ci pratique dans sa résidence[40].

En effet, un numéro d'IP est une porte ouverte vers une kyrielle de données qui, assemblées, permettent de suivre les navigations sur Internet d'un individu[41]. Dans le contexte de la protection des données personnelles,

---

36 *Id*., par. 102.

37 *Id*., par. 129.

38 *Id*.

39 *R*. c. *Spencer*, [2014] 2 R.C.S. 212.

40 *Id*., par. 32.

41 Le juge Cromwell ajoute au paragraphe 46 de *Spencer* : « De plus, Internet a augmenté de façon exponentielle la qualité et la quantité des renseignements stockés concernant les internautes. L'historique de navigation, par exemple, permet d'obtenir des

les agences de protection des données personnelles avaient, depuis un certain temps déjà, déterminé que le numéro IP d'un ordinateur constituait une donnée nominative.

On doit saluer cette nette évolution de l'analyse de la Cour suprême qui semble ainsi s'éloigner de la notion de « biographical core » dans la paramétrisation du droit à la vie privée et embrasser une approche prenant en compte les particularités des univers numériques et leur formidable capacité à croiser des données et à produire des portraits totaux de l'individu.

La vie privée *dématérialisée* représente aujourd'hui l'essence du droit à la vie privée. Sans négliger les aspects plus classiques du champ de protection de ce droit, il faut aujourd'hui accorder toute notre attention à ces dimensions *dématérialisées* qui concentrent les activités individuelles et collectives de nos sociétés. Les réflexions de la Cour suprême s'inscrivent certes dans une trame de droit criminel, fondée sur l'interprétation de l'article 8 de la Charte canadienne, mais doivent pénétrer l'éthos général du droit à la vie privée afin d'assurer son adéquation au contexte contemporain. Leur portée est en effet constitutionnelle et devrait donc irriguer la réflexion entourant le droit à la vie privée Ceci dit, pour plusieurs, la bataille de la vie privée ne saurait reposer sur le seul vecteur juridique. La marchandisation croissante des activités humaines, induite par les politiques néolibérales des trente dernières années, ne manque pas d'emporter la vie privée ou, plus précisément, les données personnelles.

---

renseignements détaillés sur les intérêts des utilisateurs. Les moteurs de recherche peuvent recueillir des renseignements sur les termes recherchés par les utilisateurs. Les annonceurs peuvent suivre leurs utilisateurs à travers les réseaux de sites Web et obtenir un aperçu de leurs intérêts et de leurs préoccupations. Les fichiers témoins peuvent être utilisés pour suivre les habitudes de consommation et peuvent fournir des renseignements sur les options sélectionnées dans un site Web, sur les pages Web consultées avant et après avoir visité le site d'accueil et tout autre renseignement personnel fourni. L'utilisateur n'est pas en mesure d'exercer un contrôle total à l'égard de la personne qui peut observer le profil de ses activités en ligne et il n'est pas toujours informé de l'identité de celle-ci. Or, sous le couvert de l'anonymat – en protégeant le lien entre l'information et l'identité de la personne qu'elle concerne –, l'utilisateur peut en grande partie être assuré que ses activités demeurent confidentielles ».

IV. Les dimensions économiques des données personnelles

Certains estiment que le droit est incapable de saisir le nouvel écosystème dans lequel les données se déploient et interagissent car le droit à la vie privée, tel qu'interprété par les tribunaux et consacré dans les lois de protection des renseignements personnels, ne correspondrait plus à une réalité sociale. Prenant avantage de ce qui apparaît comme une inadéquation entre le droit à la vie privée et les univers dématérialisés et fondant leur analyse sur une économisation des pratiques numériques, certains entendent faire des données personnelles une marchandise comme une autre. Les tenants de cette opinion ne sont pas forcément des néolibéraux obsédés par le marché comme horizon indépassable des sociétés humaines.

Réitérons d'abord le constat selon lequel les internautes ne sont pas complètement ignorants du droit à la vie privée. Mais, ils sont prêts à moduler celui-ci au regard des exigences de gestion de leur capital social. De même, la possibilité de bénéficier de services gratuits ne manque pas de jouer et d'atténuer certaines exigences au regard de la vie privée (application du principe « je sais bien, mais quand même ») : je sais que les opérateurs examinent ma navigation, enregistrent mes traces numériques, analysent mes courriels, revendent le tout à des marques, etc. mais même si je sais bien tout cela, « quand même, les services fournis par ces plateformes sont avantageux, surtout s'ils sont gratuits... »[42]. Cette connaissance des contextes numériques constituerait-elle alors un fondement logique pour exiger une rémunération pour l'utilisation de ses données personnelles ?

Voilà un débat qui resurgit, celui de déterminer la nature du droit à la vie privée : un droit de la personnalité qui relève également des libertés fondamentales ou un droit patrimonial qui peut être cessible ? Ce débat n'est pas sans lien avec l'émergence de la notion de *digital labor* qui peut être définie comme « la réduction de nos "liaisons numériques" à un moment du rapport de production, la subsomption du social sous le marchand dans le contexte de nos usages technologiques ». Ces liaisons numériques sont en fait « les activités numériques quotidiennes des usagers des plateformes sociales, d'objets connectés ou d'applications mobiles »[43]. Il s'agit donc des activités conduites par les internautes dans le cadre de leurs

---

42 Dominique Boullier, *Sociologie du numérique*, Paris, Armand Colin, 2016, p. 114.

43 Dominique Cardon et Antonio A. Casilli, *Qu'est-ce que le Digital Labor ?*, Paris, INA Éditions, 2015, p. 13.

navigations sur Internet et qui produisent au bénéfice des plateformes une valeur importante :

> (...) chaque post, chaque photo, chaque saisie et même chaque connexion à ces dispositifs [les plateformes] remplit les conditions évoquées dans la définition : produire de la valeur (appropriée par les propriétaires des grandes entreprises technologiques), encadrer la participation (par la mise en place d'obligations et contraintes contractuelles à la contribution et à la coopération contenues dans les conditions générales d'usage), mesurer (moyennant des indicateurs de popularité, réputation, statut, etc.)[44].

L'internaute contribue, en effet, à une création de valeur lorsqu'il participe à l'animation et à l'activité des différentes plateformes du web 2.0 (réseaux sociaux, blogues, partage de contenus, évaluation, posts, tweets, etc.), puisqu'il alimente par ses données (*like* ou *share* sur Facebook, un commentaire, une recommandation, un partage de photo, etc.) l'écosystème et le modèle d'affaires des entreprises. Il le fait gratuitement et ces dernières exploitent ces données et en obtiennent un important rendement. Ces données sont parfois nominatives, au sens où l'entendent les lois de protection des données personnelles, ou simplement le résultat d'une activité sur les réseaux, comme celle, par exemple, du système des reCAPTCHAS de Google qui « demande aux utilisateurs de "vérifier s'ils sont humains" en cherchant à déchiffrer des mots déformés ». Or, « sans le savoir, toute personne se prêtant à la tâche contribue de fait à la numérisation de textes du service propriétaire Google Books »[45]. La reconnaissance des numéros d'adresse civique pour Google Street View ou l'appariement d'images relève du même exercice gratuit et profitable pour les entreprises[46].

Dominique Boullier avance que nous sommes en présence d'une économie de l'*attention* :

> La rareté de l'attention rend particulièrement précieux les moments où le client ou le public marque son intérêt aussi minime soit-il pour une offre. Kessous appelle cela des « dépôts d'attention ». Tout le système des traces numériques qui se met en place à partir des réseaux sociaux mais bien au-delà (un clic sur un lien dans Google est une

---

44 *Id.*

45 *Id.*, p. 21.

46 *Id.*

trace déjà exploitable) permet de collecter ces bribes d'attention pour les calculer (et les métriques deviennent essentielles, telles celles de la réputation), et pour orienter les stratégies de marketing[47].

Les algorithmes développés par les principaux acteurs d'Internet permettent d'agréger ces traces et ces signaux et d'en tirer une valeur. Leur puissance est accrue lorsque ces algorithmes sont apprenants. Des données massives sont ainsi accessibles et constituent un outil statistique, plutôt qu'intelligent[48], d'une grande utilité dans les stratégies commerciales. Dominique Cardon distingue les traces des signaux : les *signaux* sont des données qui « proposent des contenus explicites, informations ou expressions subjectives » (par exemple, « un statut sur Facebook ») alors que les *traces* seraient des « données implicites », « des enregistrements contextuels de comportements » (par exemple, « clics, géolocalisation, navigation, vitesse de lecture etc. »)[49]. Les algorithmes vraiment efficaces sont ceux capables de coupler « étroitement des signaux informationnels avec des traces de comportement ou, pour le dire autrement, qui se servent des traces pour trouver la meilleure relation entre les signaux »[50]. On peut se demander si ces traces et ces signaux constituent des données personnelles au sens juridique du terme. Avec Dominique Boullier, on peut affirmer « que toutes les traces d'activité les plus élémentaires peuvent devenir "personnelles" au sens où elles peuvent être associées, corrélées et modélisées pour revenir à des profils individuels (...) »[51]. Les principaux opérateurs d'Internet ont ainsi mis en place un régime efficace de prédation des données afin d'asseoir un modèle d'affaires capable de générer de formidables profits.

Cette réalité économique explique donc que certains préconisent une approche propriétaire des données. En effet, avancent-ils, si mes données

---

47 Dominique BOULLIER, *Sociologie du numérique*, Paris, Armand Colin, 2016, p. 186.

48 « Désormais, les machines cherchent beaucoup moins à modéliser le raisonnement qu'à ingurgiter des contextes à travers d'énormes masses de données. Les concepteurs ont abandonné l'ambition de faire des machines "intelligentes". Ils préfèrent les rendre "statistiques". », Dominique CARDON, *À quoi rêvent les algorithmes. Nos vies à l'heure des big data*, Parus, Seuil, 2015, p. 59.

49 *Id*., p. 62.

50 *Id*., p. 63. Lire aussi la typologie proposée par Dominique BOULLIER qui distingue les données personnelles fournies, observées, dérivées ou inférées : Dominique BOULLIER, *Sociologie du numérique*, Paris, Armand Colin, 2016, p. 279.

51 *Id*.

produisent de la valeur pour autrui, je devrais pouvoir en bénéficier également en exerçant un contrôle propriétaire sur les données que mes activités et ma personne génèrent. L'attribution d'un droit de propriété sur les données pourrait constituer une voie susceptible de contribuer à une meilleure protection de la vie privée que ne le font les lois actuelles. Ces dernières ne peinent-elles à couvrir tout le spectre des utilisations des données par les opérateurs ? Jaron Lanier[52], par exemple, est de cet avis lorsqu'il affirme que le droit de propriété peut seul garantir « une maîtrise des conditions d'appropriation des contenus que nous échangeons en ligne »[53]. Un système de microroyalties permettrait de faciliter la gestion de nos informations personnelles, d'en tirer des revenus et de rééquilibrer un régime numérique carrément féodal. Plusieurs régimes peuvent être proposés afin d'assurer un droit de propriété sur les données, on pense notamment à celui de la propriété intellectuelle, mais quel qu'il soit, une telle reconnaissance « pose a priori de redoutables problèmes de définition et de mise en œuvre sur un plan institutionnel »[54]. Une myriade de questions surgit : quelle serait l'étendue exacte de ce droit de propriété, relèverait-il de la simple possession, quelle en serait la nature, comment assurer l'information des titulaires, une négociation serait-elle possible ou déboucherait-elle inévitablement sur un contrat d'adhésion, comment évaluer les données, qui assurerait un cadastre des droits de propriété, quelles seraient les institutions à mettre en place pour assurer la délimitation, l'administration et la surveillance des droits octroyés et qui en assumerait les coûts, quel tribunal pourrait être compétent etc. ? Ce ne sont que quelques unes des questions que soulève une telle approche.

Au-delà de ces questions d'application se pose celle, encore plus préoccupante, des effets et des conséquences d'une telle approche propriétaire pour des données qui relève, dans la réalité juridique, des droits de

---

52 Jaron LANIER, *Who owns the Future ?*, New York, Simon & Schuster, 2014. Voir également le projet de recherche universitaire VALDO qui se propose de réfléchir à la « nécessité d'offrir à l'individu la possibilité de prendre part à la valorisation de ses données personnelles » : projet VALDO, valorisation et monétisation des données personnelles à l'ère du Big Data. En ligne : http://www.cerdi.u-psud.fr/partenariats/projet/valdo-valorisation-et-monetisation-des-donnees-personnelles-a-lere-du-big-data (consulté le 1er septembre 2016).

53 Dominique CARDON et Antonio A. CASILLI, *Qu'est-ce que le Digital Labor ?*, Paris, INA Éditions, 2015, p. 37-38.

54 Fabrice ROCHELANDET, *Économie des données personnelles et de la vie privée*, Paris, La Découverte, 2010, p. 100.

la personnalité et de la personne. La patrimonialisation des données personnelles soulève un problème éthique de même nature que celui lié à la commercialisation des parties du corps humain (sperme, sang, embryons etc.). On ne peut, d'une part, dénoncer un usage marchand des données personnelles et, d'autre part, participer et légitimer un usage ravalant les données personnelles au rang de marchandise. Ce serait, pour employer les termes d'Antonio Casilli, « privatiser la privacy »[55] et contribuer à une économisation déjà bien entamée des activités numériques que l'on dénonce par ailleurs. Le Conseil national du numérique en France a rejeté cette approche dans son rapport de 2014. Il précise ainsi qu'il convient d'exclure une telle option :

- parce qu'elle renvoie à l'individu la responsabilité de gérer et protéger ses données, renforce l'individualisme et nie le rapport de force entre consommateurs et entreprises ;
- parce qu'elle ne pourrait que générer des revenus anecdotiques pour les usagers et susciter à l'inverse un marché de la gestion protectrice des données numériques ;
- parce qu'elle déboucherait à un renforcement des inégalités entre citoyens en capacité de gérer, protéger et monétiser leurs données et ceux, qui par manque de littératie, de temps, d'argent ou autre, abandonneraient ces fonctions au marché[56].

L'approche propriétaire s'inscrit clairement dans une perspective néolibérale qui présume que l'individu serait le mieux placé pour décider du sort de ses données. Cette approche fait donc reposer sur l'individu le lourd fardeau de gérer des données personnelles dans un contexte de déséquilibre patent des acteurs en présence. Ce rapport de forces inégales est rappelé à juste titre par le Conseil national du numérique de France.

---

55 Dominique CARDON et Antonio A. CASILLI, *Qu'est-ce que le Digital Labor ?*, Paris, INA Éditions, 2015, p. 38.

56 CONSEIL NATIONAL DU NUMÉRIQUE, *Neutralité des plateformes. Réunir les conditions d'un environnement numérique ouvert et soutenable*, Ministère de l'économie, du redressement productif et du numérique, mai 2014, en ligne : http://cnnumerique.fr/wp-content/uploads/2014/06/CNNum_Rapport_Neutralite_des_plateformes.pdf (consulté le 1er septembre 2016). Sur ce thème, on peut aussi lire l'article de Valérie PEUGEOT, « Données personnelles : sortir des injonctions contradictoires », en ligne : http://vecam.org/archives/article1289.html (consulté le 1er septembre 2016).

Le danger de consacrer ainsi un capitalisme cognitif[57], qui assoit déjà la domination de quelques grands opérateurs d'Internet, est d'établir un troisième régime d'*enclosure* après celui des terres communes dans l'Angleterre des XVI^e^ et XVII^e^ siècle et son parachèvement avec le *Black Act* du XVIII^e^ siècle[58] et celui de la propriété intellectuelle entamé à la fin du XIX^e^ siècle[59]. Une marchandisation et une *propriétarisation* des données engendreraient sans aucun doute une course effrénée vers une appropriation de toutes les ressources cognitives primaires (les données) et secondaires (l'information). Notre époque est encore propice à une réification et une appropriation de composantes de la vie sociale qui avaient toujours échappé à une détermination de valeur[60]. La reconnaissance d'un droit de propriété sur les données remettrait radicalement en cause le droit à la vie privée. Si les composantes informationnelles de ce droit, qui en constituent en fait un fondement premier dans nos sociétés contemporaines, peuvent ainsi être aliénées ou autrement démembrées, c'est alors l'intan-

---

57 Yann MOULIER-BOUTANG, *Le capitalisme cognitif : la nouvelle grande transformation*, Paris, Éditions Amsterdam, 2007 et Michael A. PETERS et Ergin BULUT (dir.), *Cognitive Capitalism, Education and Digital Labor*, New York, Peter Lang Publishing, 2011. Dans cet ouvrage, Peters et Bulut définissent ainsi le capitalisme cognitif à la p. xxv de leur introduction : « "Cognitive capitalism" is a general term that has become significant in the discourse analyzing a new form of capitalism sometimes called the third phase of capitalism, after the earlier phases of mercantile and industrial capitalism, where the accumulation process is centered on immaterial or digital labor processes and production of symbolic goods and experiences. It is a term that focuses on the socio-economic changes ushered in with the Internet as platform and new Web 2.0 technologies that have impacted the mode of production and the nature of labor. The core of cognitive capitalism is centered on digital labor processes that produce digital products cheaply utilizing new information and communications technologies that are protected through intellectual property rights regimes, which are increasingly subjected to interventions and negotiations of the nation states around the world. »

58 E.P. THOMPSON, *Whigs & Hunters. The Origin of the Black Act*, Londres (rééd.), Breviary Stuff Publications, 2013 (première publication en 1975).

59 Sur cette seconde enclosure, lire James BOYLE, « The Second Enclosure Movement and the Construction of the Public Domain », (2003) 66 *Law and Contemporary Problems* 33. Aussi en ligne : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=470983 (consulté le 1^er^ septembre 2016).

60 « Commodification presumes the existence of property rights over processes, things, and social relations, that a price can be put on them, and that they can be traded subject to legal contract », David HARVEY, *A Brief History of Neoliberalism*, Oxford, Oxford University Press, 2005, p. 165.

gibilité d'un droit fondamental qui est compromise. La marchandisation l'emporterait sur la dignité humaine et toute atteinte à la vie privée serait immédiatement monnayable sans égard aux considérations d'ordre public ou collectives qui rappellent que la société est également partie prenante des libertés individuelles, puisqu'elle en est le creuset et le garant. À cet égard, d'aucuns considèrent que les données générées par les activités des internautes constitueraient des biens communs, donc ni privés, ni publics et, par conséquent, « inappropriables ». La théorie des biens communs ne nie pas le droit de propriété, mais elle rappelle notamment que celui-ci est « le fruit d'un processus historique et non, comme le suppose une pensée économiste néoclassique, un « droit naturel immuable »[61]. En ces temps d'appropriation du vivant, de la nature et de l'immatériel aux fins de créer des rentes, il apparaît primordial de réactiver la théorie des communs afin d'assurer une juste répartition des ressources et éviter un accaparement nuisible à la paix sociale. Au sujet des données collectées dans le cyberespace, Valérie Peugeot écrit :

> 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 (...) 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.

---

61 Béatrice PARANCE et Jacques DE SAINT-VICTOR, « Commons, biens communs, communs : une révolution juridique nécessaire », dans Béatrice PARANCE et Jacques DE SAINT-VICTOR (dir.), *Repenser les biens communs*, Paris, CNRS Éditions, 2014, p. 9, à la page 20.

Les deux peuvent non seulement cohabiter mais également se compléter[62].

Cette perspective, bien que plus humaniste, illustre en tout état de cause la complexion économique croissante des données personnelles et l'importance accordée au phénomène des données massives (*big data*) qui constituerait le pétrole du XXI^e^ siècle. On peut légitimement se demander quel poids pourront bien avoir les considérations juridiques du droit à la vie privée au regard de ce phénomène. Tout le contexte d'échange, de transfert et de partage des données sur Internet, tout ce chassé-croisé de données mêlés à des services, des expressions de soi, ne peut manquer de relativiser le droit à la vie privée, voire de le rendre anecdotique au regard des enjeux colossaux du capitalisme cognitif.

Conclusion

L'émergence d'Internet grand public en 1995, couplée à une numérisation croissante des sociétés contemporaines, constitue un phénomène qui remet en cause l'économie générale du droit à la vie privée. D'un droit essentiellement porté sur la défense d'une intimité bourgeoise pétrie de bonnes manières, il se transforme en un droit manifestement politique fondant l'autonomie de l'individu au regard de pouvoirs trop curieux incarnés par les dérives de la NSA illustrées par l'affaire Snowden et un capitalisme cognitif porté par les opérateurs géants d'Internet. Que pèse le droit à la vie privée, forgé dans les modestes offices de la jurisprudence et de la doctrine, devant ces formidables pouvoirs ? La sécurité et le commerce exercent une invraisemblable pression sur celui-ci, le sommant de se modeler aux exigences sécuritaires et à l'air des temps marchands. La nature globale du terrain de jeu sur lequel il se déploie contribue à rendre encore plus difficile son exercice et son respect. La mondialisation a beau faciliter les flux économiques et financiers, elle ne montre pas le même empressement à faciliter une réelle circulation des droits fondamentaux qui pourraient accompagner et soumettre ces flux au droit. Un droit global se met certes en place, mais il sert d'abord à encadrer les échanges économiques[63]. Les juristes ont le devoir d'apparier les droits fondamen-

---

62 Valérie PEUGEOT, « Données personnelles : sortir des injonctions contradictoires », en ligne : http://vecam.org/archives/article1289.html (consulté le 1er septembre 2016).

63 Sur ce thème, lire entre autres : Karim BENYEKHLEF, « Une introduction au droit global », dans Karim BENYEKHLEF (dir.), *Vers un droit global ?*, Montréal, Éditions Thémis, 2016, p. 1.

taux, de première et de seconde génération, aux flux économiques afin d'assurer une globalisation prenant en compte la dignité humaine et les droits collectifs. La réponse à ces mutations des objets du droit à la vie privée doit également emprunter la voie politique d'une discussion démocratique. Or, avec Dominique Boullier, on doit déplorer « l'absence d'espace de discussion démocratique » relatif aux choix des internautes quant aux contours espérés et attendus du droit à la vie privée dans un contexte technologique. Cette absence est hélas une « constante de tous ces systèmes techniques alors même qu'ils conditionnent toute l'activité politique et citoyenne »[64].

Par ailleurs, les agences de protection des données personnelles ne sont plus aussi démunies qu'elles pouvaient l'être au début des années 2000. En effet, on a noté plus haut la centralisation croissante d'Internet par le jeu croisé d'entreprises majeures comme Facebook, Google, Apple et Amazon. Cette centralisation relativise en bonne partie les arguments entendus dès l'émergence du World Wide Web selon lesquels, les caractéristiques d'Internet étant l'ubiquité, la décentralisation, l'absence de centre et de contrôle, la déterritorialisation, voire l'extraterritorialité, il apparaissait impossible pour le souverain d'y étendre sa règle. En d'autres mots, le souverain ne pouvait prétendre exercer sa loi sur un phénomène ou un acteur délocalisé et ubiquitaire. On entendait également souvent le commentaire selon lequel le souverain devait s'abstenir de toute intervention puisqu'Internet était en plein développement et qu'il fallait éviter d'inhiber l'innovation et la détermination des stratégies industrielles des acteurs, bref de leurs modèles d'affaires. Ce n'est plus vrai aujourd'hui. Ces acteurs ont un solide modèle d'affaires et sont essentiellement des régies publicitaires qui récoltent des données personnelles et les vendent ou les utilisent pour des publicités ciblées.

Google, Facebook et les autres ont aujourd'hui une présence physique dans la plupart des pays occidentaux. Ainsi, l'appropriation quasi littérale du web par ces géants a pour effet de centraliser Internet et de le rendre ainsi beaucoup plus perméable à une régulation et alors à une surveillance et un contrôle. La loi nationale peut jouer à nouveau son rôle et trouver application sans que les arguments a-nationaux (délocalisation, ubiquité etc.) et conjoncturels (émergence d'Internet, fragilité de l'écosystème et de ses acteurs) ne puissent à nouveau être avancés pour justifier une inaction. Il devient maintenant plus facile d'exercer une pression juridique

64 Dominique BOULLIER, *Sociologie du numérique*, Paris, Armand Colin, 2016, p. 263.

induite par la loi, puisque les principaux protagonistes sont peu nombreux, ont pignon sur rue et leur modèle d'affaires est clairement établi : collecter des données personnelles afin de les utiliser à des fins lucratives. Les agences de protection des données personnelles ont donc la capacité d'agir afin d'assurer le respect des législations nationales et elles devraient en effet être moins timides aujourd'hui. En fait, les décisions récentes de la Cour de justice de l'Union européenne illustrent un *activisme* plus marqué. La Cour n'a-t-elle pas démontré, en 2015, dans l'affaire Maximilian Schrems une plus grande sûreté que l'agence irlandaise de protection des données[65] ? On se souviendra qu'abonné à Facebook depuis 2008, Schrems a déposé en 2013 une plainte devant l'agence irlandaise de protection des données invoquant l'absence de protection réelle des données conservées sur son territoire à l'encontre de la surveillance de l'État au regard des révélations de l'affaire Snowden. Schrems contestait plus particulièrement le *Safe Harbor*, accord permettant le transfert de données personnelles concernant des citoyens européens de l'Union européenne vers les États-Unis. L'agence irlandaise a rejeté sa plainte, la qualifiant même de futile et vexatoire. Elle n'a pas fait preuve d'un grand courage, sans doute craintive des conséquences économiques de sa décision et pleine de respect et de déférence devant les autorités de surveillance américaines. La Cour de justice de l'Union européenne a rescindé le *Safe Harbor*. L'arrêt de la Cour relatif au déréférencement, en 2014, est une autre illustration de son activisme en matière de protection de la vie privée informationnelle[66].

Ces décisions de la CJUE illustrent sa volonté de prendre le droit de la protection des données personnelles au sérieux et de garantir, dans la mesure de son action, une protection réelle et non simplement rhétorique de ce droit. La voie judiciaire peut constituer une manière d'assurer une plus grande égalité des parties en présence, même s'il faut bien reconnaître les limites de celle-ci (coûts, délais etc.).

Au Canada, la Cour suprême devra imprimer une nette évolution au droit de la protection de la vie privée informationnelle dans un contexte

---

65 *Maximilian Schrems* c. *Data Protection Commissioner*, Affaire C-362/14, 6 octobre 2015, en ligne : http://curia.europa.eu/juris/liste.jsf ?num=C-362/14 (consulté le 1er septembre 2016).

66 *Google Spain* c. *Agencia espanola de proteccion de datos*, Affaire C-131/12, 13 mai 2014, en ligne : http://curia.europa.eu/juris/document/document.jsf?docid=152065 (consulté le 1er septembre 2016).

non pénal. Les récentes décisions de la Cour, citées plus haut, attestent d'une meilleure compréhension des incidences des technologies de l'information et de la communication sur l'écologie du droit à la vie privée. On serait aussi bien inspiré de s'éloigner du modèle dual habituel d'équilibration dans l'analyse juridique de la vie privée : vie privée c. vie publique. Sans renier complètement cette dichotomie, il y aurait lieu de prendre appui sur les analyses sociologiques des pratiques des internautes afin d'actualiser un droit à la vie privée en prise avec celles-ci. Il serait également important de prendre en compte les dimensions économiques du droit à la vie privée afin de mieux armer les citoyens contre la prédation de leurs données personnelles par les grands opérateurs d'Internet. À cet égard, le secteur privé n'est pas moins menaçant pour la vie privée que l'État. L'affaire Snowden a d'ailleurs confirmé les collaborations des entreprises avec les agences de renseignement. Les dénégations subséquentes et les professions de foi ne doivent pas nous leurrer. Au-delà de cette collaboration avérée, la prédation du secteur privé demande également une attention et le développement d'une réflexion juridique qui soit en mesure d'assurer une protection des droits des individus et, plus généralement, une meilleure symétrie des droits et des intérêts. Les valeurs et les représentations de la vie privée sont encore bien vivantes, même si le droit à la vie privée doit s'adapter à un contexte de circulation radicale et effrénée de l'information. Ce contexte induit une accélération du temps qui brouille les repères habituels d'un droit dont l'élaboration formelle remonte à la fin du XIX^{e} siècle, dans une époque où on laissait du temps au temps.