Vol. 33, n° 3

« Made in Canada » : Distinctions culturelles de la protection des renseignements personnels canadienne

Vincent Gautrais*

* Professeur titulaire à la Faculté de droit de l'Université de Montréal, directeur du Centre de recherche en droit public (CRDP) et titulaire de la Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique à la Faculté de droit de l'Université de Montréal. Je tiens à remercier chaleureusement Nicolas Aubin, avocat, assistant de recherche, CRDP, Chaire L.R. Wilson, candidat à la Maîtrise en droit des technologies, Université de Montréal, pour son aide précieuse dans la recherche bibliographique de cet article. Merci également à Justin Boileau, avocat, candidat au J.D., Université de Montréal, pour ses recherches sur certaines des questions traitées.

[Note : cet article a été soumis à une évaluation à double anonymat.]

RÉSUMÉ

La protection de la vie privée est assujettie à des valeurs, des institutions, des lois, qui sont intimement liées aux spécificités culturelles propres à chacune des juridictions. Or, face à la globalisation de ce domaine à la mode, des comparaisons fréquentes sont faites entre le droit européen et le droit canadien. Dans le cadre de cet article, nous essayerons de montrer que « comparaison n'est pas raison » et que si des inspirations sont assurément possibles entre les deux régimes juridiques, il importe de ne pas dénaturer le droit canadien tant au regard de ses principes substantiels qu'à celui des modalités d'application institutionnelle.

ABSTRACT

The protection of privacy is subject to values, institutions and laws that are intimately linked to the cultural specificities of each jurisdiction. However, given the globalization of this trendy field, comparisons are frequently made between European and Canadian law. In this article, we will try to show that "comparison do not provide all the answers" and that, while it is certainly possible to draw inspiration between the two legal systems, it is important not to distort Canadian law in terms of both its substantive principles and its institutional application.

INTRODUCTION

Globalisation. « L'Europe, l'Europe, l'Europe ! »[1] Cette entrevue très médiatisée du Général de Gaulle en décembre 1965 invitait son auditoire non pas à se détacher de la construction en formation qu'était la Communauté économique européenne, alors constituée de 6 États, mais à « prendre les choses comme elles sont ». Si cette référence, très hors contexte, très datée, constitue notre incipit de ce texte sur les spécificités canadiennes de la vie privée, c'est qu'en la matière, le droit européen, fort d'un règlement majeur adopté en 2016, le fameux Règlement général sur la protection des données[2] (ci-après « RGPD »), influence le monde au complet et le Canada en particulier. Certes, l'approche comparative est désormais une source indispensable de réflexion, le regard externe étant une source fructueuse d'autodéfinition, d'inspiration, surtout dans des domaines comme le numérique où l'on ne dispose que d'un recul encore bien à court terme. Certes, l'Europe constitue un partenaire économique et culturel indispensable qui fait que l'analyse de son cadre législatif est riche d'enseignement. Certes, encore, la vie privée a très tôt été identifiée comme une priorité européenne, priorité dont l'incidence vers l'extérieur a été matérialisée dès la Directive de 1995 obligeant les pays tiers ayant des données concernant des Européens à disposer d'un « niveau de protection adéquat »[3]. Cette globalisation des

1. INA POLITIQUE, « Charles de Gaulle "Cabri, l'Europe ! l'Europe !" », *YouTube*, 14 décembre 1965, en ligne : <https://www.youtube.com/watch?v=zufecNrhhLs> (consulté le 9 août 2021).
2. UE, *Règlement 2016/679 (UE) du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*, [2016] J.O. L 119/1 (ci-après « RGPD »).
3. CE, *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, 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*, [1995] J.O. L 281/31, art. 25 (ci-après « Directive 95/46/CE »). Le RGPD contient des dispositions équivalentes (voir art. 44 et s.).

cadres normatifs est donc bien présente, calquant la globalisation des données.

Différences culturelles. Cela dit, revenons à la courte vidéo du Général de Gaulle : « Il faut prendre les choses comme elles sont. » Et si « l'on ne fait pas de politique autrement que sur des réalités », il en est sans doute de même pour le droit. Conformément aux propos de Vittorio Villa, « les deux modèles généraux de connaissance » prônent une cohérence entre à la fois le contact avec la réalité et la mise en avant d'un préalable construit, subjectif[4]. Or, culturellement, la vie privée se conçoit différemment d'un continent à l'autre[5]. Bien entendu, il nous aurait fallu mesurer ces différences, sociologiquement, ethnologiquement, ce que, faute de temps, de compétences, nous ne ferons pas dans cet article[6]. En revanche, nous tenterons d'identifier dans le droit des distinctions majeures qui illustrent le fait que le modèle européen n'est pas, comme n'importe quel autre modèle d'ailleurs, transposable sans adaptation. Notons aussi sur ce point que cette volonté de dissociation d'avec les façons de faire européennes ne constitue aucunement un jugement de valeur laissant croire que le cadre canadien serait meilleur. Évidemment pas ! Sur plusieurs éléments que nous traiterons, c'est plutôt le contraire.

Européanisation à tout crin. Comme nous le disions plus tôt, en matière de vie privée, l'Europe a la cote. En premier lieu, le RGPD est le premier cadre général qui s'applique alors que la nouvelle réalité numérique exacerbe les risques d'atteintes aux droits des individus. Les deux projets de loi québécois[7] (ci-après « projet de loi

4. Vittorio VILLA, « La science juridique entre descriptivisme et constructivisme », dans Paul AMSELEK (dir.), *Théorie du droit et science*, Paris, P.U.F., 1994, p. 288.
5. *The Gazette* c. *Valiquette*, [1997] R.J.Q. 30, p. 10 : « En fait, la vie privée représente une "constellation de valeurs concordantes et opposées de droits solidaires et antagonistes, d'intérêts communs et contraires" évoluant avec le temps et variant d'un milieu culturel à un autre. »
6. Nous nous limiterons sur ce sujet largement sous-étudié à citer certaines références qui tentent de mesurer l'influence des différences culturelles tant sur la vie privée que sur l'encadrement de cette matière. John H. BENAMATI, Zafer OZDEMIR, et Jeff H. SMITH, « Information Privacy, Cultural Values, and Regulatory Preferences », (2021) 29-3 *Journal of Global Information Management* 34 ; Steven BELLMAN, Eric J. JOHNSON, Stephen J. KOBRIN, et Gerald L. LOHSE, « International Differences in Information Privacy Concerns: A Global Survey of Consumers », (2004) 20-5 *The Information Society* 313 ; Nik THOMPSON, Tanya MCGILL, Anna BUNN, et Rukshan ALEXANDER, « Cultural Factors and the Role of Privacy Concerns in Acceptance of Government Surveillance », (2020) 71-9 *Journal of the Association for Information Science and Technology* 1129.
7. *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, projet de loi nº 64 (étude détaillée – 2 septembre 2021), 1re sess., 42e légis. (Qc) (ci-après « projet de loi nº 64 »).

nº 64 ») et fédéral[8] (ci-après « projet de loi nº C-11 »), qui sont apparus respectivement en juin et novembre 2020, sont des réponses à cette tendance initiée de l'autre côté de l'Atlantique. Une réponse qui au Québec a pris la forme d'un avis de la Commission européenne en 2014, et donc avant le RGPD, où sur la base de la directive européenne de 1995, un regard circonspect a été donné sur le cadre législatif québécois[9], matérialisant un contrôle extraterritorial de l'Europe sur le Québec. Alors qu'en 2001, une analyse somme toute assez sommaire avait été rendue sur la nouvelle loi fédérale, en 2015, le temps n'était plus à la complaisance. L'analyse du « niveau de protection adéquat » impliquait une densité du contrôle et des mesures mises en place. En deuxième lieu, et de façon beaucoup plus paradoxale, le rapprochement avec le RGPD est exigé par l'industrie elle-même[10]. Celle-ci en effet est en quête d'une certaine uniformité, d'autant que plusieurs entreprises font le choix d'adopter les solutions européennes dans la mesure où celles-ci sont, à tort ou à raison, perçues comme les plus exigeantes du monde, et donc les plus susceptibles de s'appliquer partout. Enfin, en troisième lieu, l'analyse du RGPD se justifie du fait que les différents cadres, tant le cadre fédéral[11] que les cadres provinciaux[12], sont passablement dysfonctionnels. Que ce soit en ce

8. *Loi édictant la Loi sur la protection de la vie privée des consommateurs et la Loi sur le Tribunal de la protection des renseignements personnels et des données et apportant des modifications corrélatives et connexes à d'autres lois*, projet de loi nº C-11 (dépôt et 1re lecture – 17 novembre 2020), 2e sess., 43e légis. (Can.) (ci-après « projet de loi nº C-11 »).
9. GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES PHYSIQUES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL, *Avis 7/2014 sur la protection des données à caractère personnel au Québec*, 4 juin 2014, en ligne : <https://www.dataprotection.ro/servlet/ViewDocument?id=1290>.
10. Eloïse GRATTON, Elisa HENRY, François JOLI-CŒUR, Max JARVIE et Andy NAGY, *Préserver un équilibre délicat : renforcer la protection des renseignements personnels dans le secteur privé tout en favorisant l'innovation et en soutenant l'économie numérique du Québec*, mémoire présenté à la Commission des institutions de l'Assemblée nationale dans le cadre des consultations particulières et auditions publiques sur le projet de loi nº 64, 22 septembre 2020, en ligne :<http://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CI/mandats/Mandat-43315/memoires-deposes.html> ; Antoine AYLWIN, Karl DELWAIDE, Jennifer STODDART, Julie UZAN-NAULIN, Guillaume PELEGRIN, Aya BARBACH et William DENEAULT-ROUILLARD, *Moderniser, mais conserver un équilibre*, mémoire présenté à la Commission des institutions de l'Assemblée nationale dans le cadre des consultations particulières et auditions publiques sur le projet de loi nº 64, 23 septembre 2020, en ligne : <http://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CI/mandats/Mandat-43315/memoires-deposes.html>.
11. *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. C-5 (ci-après « loi PIPEDA »).
12. *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c. P-39.1 ; *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1.

qui a trait à l'application de la règle, dont les sanctions sont nulles ou insignifiantes, ou aux règles elles-mêmes, toutes adoptées dans des temps technologiquement très distincts, les lois canadiennes sont profondément désadaptées. Comme en Europe au début des années 2010, le Canada doit mettre à jour son cadre législatif.

PARTIE 1 – LES DISTINCTIONS SUBSTANTIELLES DE LA PRP

Plan. Sur le plan de la substance, la comparaison de la vie privée entre Europe et Amérique laisse entrevoir une différence de degré. À certains égards, et sans prétention d'exhaustivité, des distorsions apparaissent d'abord par le fait que les textes traitant de la protection des renseignements personnels (ci-après « PRP ») considèrent différemment l'équilibrage constitutionnel entre des valeurs concurrentes. Que ce soit sur le plan théorique ou sur le plan pratique, à tort ou à raison, une moindre fondamentalisation non pas de la vie privée, mais de la PRP, semble de mise au Canada. Ensuite, sur le plan opérationnel toujours, des différences sensibles peuvent également être constatées. À titre d'illustration, cela peut notamment se vérifier au regard de l'intégration de la notion de dommage qui est souvent considérée comme inhérente à la PRP, et non en Europe. Il en est de même quant à l'absence, au Canada, de la notion de traitement, omniprésente en Europe, alors qu'au Canada chaque opération d'utilisation des données dispose (collecte, communication, conservation, etc.) d'un régime propre.

1. Fondamentalisation de la PRP

Relativement à ce premier point, nous souhaitons envisager la différence Europe / Amérique, tant du point de vue théorique que du point de vue pratique. Des différences qui ne sont bien évidemment pas monolithiques, mais dont nous espérons néanmoins identifier les gros traits.

1.1 Bases théoriques incertaines de la PRP

1.1.1 Appréhension complexe de la PRP par rapport à elle-même

Nouvelle donne technologique. Lorsque vient le temps de considérer la vie privée, ce domaine fortement impacté par les

technologies[13], doit forcément donner lieu à une perpétuelle évolution, à une perpétuelle adaptation. Et la généralisation de l'usage des données nous oblige à considérer plus globalement la vie privée, plus largement que la seule PRP.

> La vie privée ne se limite pas, au plan historique, à protéger un lieu […]. À partir du lieu, elle tresse également une démarcation des pouvoirs.[14]

Le numérique est donc affaire de pouvoirs. Ces auteurs citent notamment les travaux de Shoshana Zuboff qui justement considère que la généralisation du « capitalisme de surveillance » est tout simplement une atteinte à nos principes démocratiques[15]. Des développements récents qui s'appuient sur les expérimentations généralisées de données massives, mais qui se trouvaient, il y a longtemps, déjà identifiés comme des risques susceptibles de mettre en péril des principes juridiques qui ont mis des décennies à se sédimenter.

> Today the enormous amounts of personal data available in computers threaten the individual in a way that renders obsolete much of the previous legal protection. The danger that the computer poses is to human autonomy. The more that is known about a person, the easier it is to control him. Insuring the liberty that nourishes democracy requires a structuring of societal use of information and even permitting some concealment of information.[16]

Double approche. À cette nouveauté en lien avec l'influence technologique, s'ajoute théoriquement, une perception de la vie privée qui décèle une grande variété de perspectives ; variété que nous ne

13. Ethan KATSH, *The Electronic Media and the Transformation of Law*, New York, Oxford University Press, 1989, p. 189 : « Privacy, like copyright and obscenity, had no direct legal ancestor in the preprint era ».
14. Karim BENYEKHLEF et Pierre-Luc DÉZIEL, *Le droit de la vie privée en droit québécois et canadien*, Montréal, Éditions Yvon Blais, 2018, p. 6. Les auteurs citent ensuite Georges DUBY, « Préface à l'histoire de la vie privée », dans Philippe ARIÈS et Georges DUBY (dir.), *Histoire de la vie privée*, tome 2, De l'Europe féodale à la Renaissance, Paris, Éditions du Seuil, 1999, p. 22 : « […] admettre que l'opposition entre vie privée et vie publique est moins affaire de lieu que de pouvoirs. »
15. Shoshana ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs, New York, 2020.
16. Paul SCHWARTZ, « The computer in German and American constitutional law: Towards an American right of informational self-determination », (1989) 37 *American Journal of Comparative Law* 675, 676.

pouvons qu'effleurer dans cet article[17]. Dans le cadre de notre comparaison, notre proposition de catégorisation peut se séparer en deux, et ce, en se basant sur le « centre de gravité » autour duquel les acteurs impliqués interviennent.

> One theoretical assumption formulated as a possible response to the questions above, and underlying this research project, is the existence of two prevalent and competing formulations of privacy: one rooted in control and the other in dignity.[18] (nos soulignements)

La première « grande famille » théorique est basée sur la capacité de contrôle de l'individu lui-même. Fondée sur des publications séminales et anciennes[19], l'influence de cette perspective individualiste fut profondément reprise tant par la jurisprudence canadienne[20] qu'américaine. Une approche qui mesure donc la capacité de l'individu à contrôler – ou à refuser de le faire – les données le concernant. Cette approche, habituellement jugée comme étant dominante[21], et selon nous, beaucoup plus présente en Amérique qu'en Europe[22], fait pourtant l'objet de critiques nombreuses. En effet, du fait de la complexité des rapports, les pratiques douteuses de consentement[23], il est souvent jugé illusoire que l'individu puisse réellement contrôler ses données[24]. La seconde catégorie de théories en matière de vie privée propose des visions plus collectives où, en fin de compte, l'important est de vérifier, d'évaluer, si un procédé technologique donné est en adéquation avec le contexte social dans lequel il est utilisé[25]. Que ce

17. K. BENYEKHLEF et P.-L. DÉZIEL, préc., note 14, p. 13 à 75 sur un chapitre s'intitulant « Les approches théoriques et historiques de la vie privée ».
18. Avner LEVIN et Patricia SANCHEZ ABRIL, « Two Notions of Privacy Online », (2009) 11-4 *Vanderbilt Journal of Entertainment & Technology Law* 1001, 1005. Voir aussi : James Q. WHITMAN, « The Two Western Cultures of Privacy: Dignity versus Liberty », (2004) 113:6 *Yale Law Journal* 1151, 1172.
19. Voir notamment Alan F. WESTIN, *Privacy and Freedom*, Atheneum, New York, 1967.
20. K. BENYEKHLEF et P.-L. DÉZIEL, préc., note 14, p. 30.
21. A. LEVIN et P. SANCHEZ ABRIL, préc., note 18, 1008.
22. La capacité de contrôle de l'individu sur ses propres données est omniprésente tant dans les lois applicables au Canada que dans les projets de lois présentés (projets de loi nº 64 et nº C-11).
23. Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, Éditions Thémis, 2010.
24. Vincent GAUTRAIS, « Proposition de Règlement général sur la protection des données : un regard d'ailleurs… », dans Nathalie MARTIAL-BRAZ (dir.), *La proposition de règlement européen relatif aux données à caractère personnel*, coll. « Trans Europe Experts », Paris, Société de législation comparée, 2014, p. 464-493.
25. Edward BLOUSTEIN, « Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser », (1964) 39 *N.Y.U. L. Rev.* 962, 971.

soit au regard d'une contextualisation sociale[26] ou d'un « examen de pondération » visant à identifier la justification sociale de l'utilisation des données[27], une appréciation externe aux seules parties s'impose.

Trois points. De ces deux grandes familles que nous entrevoyons, trois commentaires complémentaires peuvent être présentés. En premier lieu, cette dichotomie trahit peut-être une évolution dans le temps face à des technologies de plus en plus intrusives. En effet, un certain déterminisme technologique prévaut face à certains procédés plus enclins à autoriser un contrôle que d'autres. La « profondeur » d'analyse qui peut parfois être associée à certains outils, comme l'intelligence artificielle, est sans doute propice à une approche plus collective, des justifications sociales venant se greffer aux habituelles considérations touchant les individus et les organisations. En deuxième lieu, ces deux grandes familles de théories ne s'opposent pas. Car les théories du contrôle ne peuvent être envisagées que lorsque celui-ci correspond à une certaine réalité. Les situations factuelles d'utilisation des données présentent un large spectre de possibilités, allant de celles où certains individus « s'abandonnent » à laisser filer leurs données à d'autres où, au contraire, aucun contrôle n'est envisageable par ceux-ci[28]. En troisième lieu, cette ambivalence est très nord-américaine et se base principalement sur des perspectives anglo-saxonnes. Car dans une perspective européenne, l'approche collective, considérant l'utilisation des données de façon globale, situant la vie privée comme une des considérations parmi d'autres à envisager, va de soi[29].

Approche intermédiaire. Justement, parmi les éléments de comparaison, et sans effectuer une analyse historique des différences entre les cultures européennes et américaines, il est toujours apparu que des différences sensibles ont été constatées dès lors qu'il s'agit de savoir où le curseur entre des libertés fondamentales concurrentes doit être positionné[30]. Que ce soit pour des raisons historiques[31],

26. K. BENYEKHLEF et P.-L. DÉZIEL, préc., note 14, p. 44 : les auteurs traitent du livre de Helen NISSEMBAUM, *Privacy in Context: Technology Policy and the Integrity of Social Life*, Stanford University Press, Stanford, 2010.
27. *Ibid.*, p. 50 : les auteurs analysent les propos de Graham MAYEDA, « My Neighbour's Kid Just Bought a Drone… New Paradigms for Privacy Law in Canada », (2016) *National Journal of Constitutional Law* 59.
28. *Ibid*.
29. *Infra*, par. 1.1.2.
30. J.Q. WHITMAN, préc., note 18, 1172.
31. Paul M. SCHWARTZ et Karl-Nikolaus PEIFER, « Transatlantic Data Privacy Law », (2017) 106-1 *Georgetown Law Journal* 115, 123 ; McKay CUNNINGHAM, « Diminishing Sovereignty: How European Privacy Law Became International

culturelles, économiques, le Canada semble privilégier une approche « intermédiaire » entre le laisser-faire états-unien et l'interventionnisme européen[32].

Protection contre l'État. Également, et même si, en fonction des juridictions, il existe de multiples hypothèses où les entreprises privées sont assujetties à des obligations concernant la vie privée, l'approche états-unienne est associée à une prévalence d'une préoccupation du contrôle de l'État.

> Suspicion of the state has always stood at the foundation of American privacy thinking, and American scholarly writing and court doctrine continue to take it for granted that the state is the prime enemy of our privacy.
>
> [...]
>
> In particular, « privacy » begins with the Fourth Amendment: At its origin, the right to privacy is the right against unlawful searches and seizures. It is thus a right that inheres in us as free and sovereign political actors, masters in our own houses, which the state is ordinarily forbidden to invade. Over time, to the American mind, the early republican commitment to « privacy » has matured into a much more far-reaching right against state intrusion into our lives.[33] (nos soulignements)

Prévalence qui se retrouve également au Canada[34]. Même le Québec entend appliquer la Charte en général et la protection de la vie privée en particulier aux instances tant publiques que privées.

Norm », (2013) 11-2 *Santa Clara J. Int'l. L.* 421, 428-429 : « The historical origins undergirding this commitment to privacy derive in part from Nazi exploitation of European census records preceding and during World War II. Many contend that the extensive accumulation of personal data by the Nazi regime facilitated pre-war abuses of human rights. In 1984, data protection experts concluded that "one of the prime motives for the creation of data protection laws in continental Europe is the prevention of the recurrence of experiences in the 1930s and 1940s with Nazi and fascist regimes". » (nos soulignements)

32. Jennifer MCCLENNAN et Vadim SCHICK, « "O, Privacy" – Canada's Importance in the Development of the International Data Privacy Regime », (2007) 38-3 *Georgetown Journal Int'l Law* 674 : « Canada has traditionally occupied the middle ground between the strict regulation in Europe and the laissez-faire approach in the United States ».
33. J.Q. WHITMAN, préc., note 18., 1212.
34. Avner LEVIN et Mary Jo NICHOLSON, « Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground », (2005) 2-2 U *Ottawa Law & Tech. Journal* 357, 393 : « Canada has much in common with the US in terms of

1.1.2 PRP et autres libertés fondamentales

Europe : Vie privée comme droit fondamental. Une autre différence importante qu'il est possible d'identifier entre les textes de loi européens et canadiens sur la PRP est que les premiers envisagent généralement la protection des données au regard d'un « risque élevé pour les droits des personnes physiques »[35] alors que les seconds tendent à se limiter à la protection de la vie privée[36]. En effet, une vision plus globale semble mise de l'avant dans l'approche européenne. C'était le cas dans le cadre de la directive de 95[37] ; ça l'est encore au regard du RGPD.

> Afin de mieux garantir le respect du présent règlement lorsque les opérations de traitement sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement devrait assumer la responsabilité d'effectuer une analyse d'impact relative à la protection des données pour évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque.[38] (nos soulignements)

Clairement donc, la vie privée n'est pas envisagée isolément : le « présent règlement respecte tous les droits fondamentaux et observe les libertés et les principes reconnus par la Charte […] »[39].

Canada : double autonomie législative. Si bien évidemment, la vie privée dispose au Canada d'un ancrage important dans les chartes[40], les lois semblent disposer d'une double autonomie au regard des libertés fondamentales. En effet, un doute prévaut d'abord quant à l'approche quasi constitutionnelle dont la vie privée dispose. Plus exactement, à la différence de l'Europe, cette perspective n'est qu'insuffisamment relevée dans les lois sur la vie privée. Ainsi, il y a

---

history (we are both former colonies); its geography (we are both massive North American countries with rich natural resources); and political structure (we are both federal countries with powerful and difficult state and provincial sub-sets). In many ways Canada resembles the US more closely than the EU. Western Canada, in particular is partial to the American emphasis on personal liberty. » ; voir aussi *Hunter et autres* c. *Southam Inc.*, [1984] 2 R.C.S. 145.

35. Art. 35(7)c)-d) RGPD. On retrouvait déjà cette tendance dans la Directive 95/46/CE.
36. Voir, par exemple, la loi PIPEDA et les deux récents projets de loi. Nous y reviendrons.
37. Directive 95/46/CE, préc., note 3.
38. RGPD, Considérant 84. Voir aussi art. 35(7)c)-d) RGPD.
39. RGPD, Considérant 4.
40. K. BENYEKHLEF et P.-L. DÉZIEL, préc., note 14.

sans doute lieu de renforcer la prise en compte d'intérêts collectifs, au-delà donc de la relation entre l'individu et l'organisation. Ensuite, et la vie privée ne peut pas, et peut-être même ne peut plus, être prise isolément. L'utilisation des données, notamment avec les outils numériques désormais disponibles, doit également prendre en compte d'autres droits fondamentaux, au-delà de la seule vie privée.

Intérêts collectifs. En premier lieu donc, un doute subsiste en droit canadien quant à la composante constitutionnelle des lois dédiées à la protection des renseignements personnels. Si l'on prend l'exemple de la loi PIPEDA tout comme d'ailleurs le projet de loi nº C-11, ces textes visent de façon assez technique à offrir une réponse proportionnée entre d'un côté les intérêts des individus et de l'autre ceux des organisations. Cette approche a d'ailleurs été critiquée par le Commissariat à la protection de la vie privée relativement à l'article 12(2)(e) du projet de loi nº C-11[41] :

> L'alinéa e) est aussi trop restreint en ce qui concerne la vie privée, car il ne décrit pas celle-ci comme un droit fondamental ou quasi constitutionnel.[42]

Cette position se retrouve également défendue par une partie de la doctrine qui considère que ce manquement est à la fois contraire à certains textes internationaux[43] et surtout mal connecté avec les besoins de protection.

> […] and it falls far short of the statements quoted from Convention 108+ and the GDPR. In the PIPEDA context, the argument has been that « human rights » are not within exclusive federal jurisdiction, so talking about human rights in PIPEDA just makes the issue of its constitutionality more fraught. Whether

41. Projet de loi nº C-11, préc., note 8, art. 12(e) : « (2) Pour établir le caractère acceptable des fins, il est tenu compte des éléments suivants : […] e) la proportionnalité entre l'atteinte à la vie privée de l'individu et les avantages pour l'organisation, au regard des moyens, techniques ou autres, mis en place par l'organisation afin d'atténuer les effets de l'atteinte pour l'individu ».
42. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE AU CANADA, *Mémoire du Commissariat à la protection de la vie privée du Canada sur le projet de loi C-11, la Loi de 2020 sur la mise en œuvre sur la Charte du numérique*, 11 mai 2021, en ligne : <https://priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/memoires-presentes-dans-le-cadre-de-consultations/sub_ethi_c11_2105>.
43. Ignacio COFONE, « Propositions stratégiques aux fins de la réforme de la LPRPDE élaborées en réponse au rapport sur l'intelligence artificielle », *Commissariat à la protection de la vie privée du Canada*, novembre 2020, en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-ai/pol-ai_202011/#fn169-rf>.

> this argument holds water or not (it doesn't), the same excuse does not exist for the federal *Privacy Act*.[44]

Notons que cette reconnaissance expresse qui pourrait – devrait – être faite dans les lois portant sur la PRP n'aurait pas forcément pour effet ni d'assurer une protection plus grande ou équivalente à celle de l'Europe ni d'empêcher l'intégration des spécificités canadiennes ; simplement, cela permet d'avoir une approche plus globale, plus intégrée des valeurs complémentaires qui prévalent dans notre système démocratique[45].

Au-delà de la seule vie privée. Justement, en second lieu, et ce point est très relié au précédent, des hésitations sont également perceptibles quant à la mise en perspective de la vie privée au regard des autres libertés fondamentales.

> Les avantages qu'obtient l'organisation ne devraient pas seulement être appréciés par rapport à l'atteinte à la vie privée dans un sens limité et technique, mais aussi par rapport aux droits et aux intérêts fondamentaux, tels que l'autonomie, la dignité ou les droits à l'égalité de l'individu qui sont touchés par la collecte, l'utilisation ou la communication.[46]

Comme nous l'avons vu, le projet de loi nº C-11 refuse une telle perspective. De son côté, le projet de loi nº 64 semble lui aussi se limiter aux seuls aspects de vie privée, ne considérant que ce point en particulier[47].

---

44. Teresa SCASSA, « It's not you, it's me? Why does the federal government have a hard time committing to the human right to privacy? », 18 novembre 2020, en ligne : <www.teresascassa.ca>. Voir aussi Teresa SCASSA, « A Human Rights-Based Approach to Data Protection in Canada », dans Elisabeth DUBOIS et Florian MARTIN-BARITEAU (dir.), *Citizenship in a Connected Canada: A Research and Policy Agenda*, Presses de l'Université d'Ottawa, Ontario, 2020, p. 185.
45. *Ibid.* : « Recognizing privacy as a human right does not mean that data protection will not require some balancing. However, it does mean that in a data driven economy and society we keep fundamental human values strongly in focus. We're not going to get data protection right if we cannot admit these connections and clearly state that data protection is about the protection of fundamental human rights and freedoms ».
46. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE AU CANADA, *Mémoire du Commissariat à la protection de la vie privée du Canada sur le projet de loi C-11, la Loi de 2020 sur la mise en œuvre sur la Charte du numérique*, préc., note 42.
47. Comme on peut notamment le constater à l'article 153 du projet de loi nº 64, modifiant l'actuel article 93 de la *Loi sur la protection des renseignements personnels* dans le secteur privé, la loi référant aux « articles 35 à 40 du Code civil »

Exemple de l'intelligence artificielle. À bien des égards, la globalité européenne se comprend bien, notamment dans le domaine du numérique. Ainsi, si l'on prend l'exemple de l'intelligence artificielle, il est difficile de considérer cette matière du seul regard de la vie privée. Il est par exemple hasardeux que sur ces questions on ne traite pas des conséquences de ces outils sur la discrimination et plus généralement sur les justifications sociales de ceux-ci. Ainsi, les mesures de diligence visant à mesurer l'impact que vont avoir les décisions automatisées[48] doivent, bien entendu, intégrer les risques d'atteinte à la vie privée, mais également d'autres conséquences néfastes sur les individus (comme la discrimination, les pertes de chances) voire sur la société dans son ensemble (justification sociale)[49]. Comme mentionné précédemment, les changements récents dans le domaine du numérique imposent un regard plus global, plus politique, plus en phase avec les valeurs qui fondent notre démocratie.

> […] Dans le contexte des sociétés avancées, le droit à la vie privée devient politique au sens où il constitue un obstacle à une surveillance sans cesse accrue et attentatoire à l'esprit démocratique par la puissance publique comme par les opérateurs économiques.[50]

1.2 Illustrations de la mise en opposition des libertés fondamentales

Trois illustrations. De façon plus concrète, il nous semble important d'identifier maintenant des situations où, face à une similarité factuelle, la réponse juridique, fortement influencée par une donne culturelle distincte, se distingue d'un continent à l'autre. Trois exemples sont ici proposés : les sites d'évaluation, le droit à l'oubli et le cas particulier de la publicité judiciaire. Dans ces trois cas, le

---

c'est-à-dire des dispositions qui ne concernent que le seul domaine de la protection de la vie privée.

48. Pour reprendre une expression que l'on retrouve tant dans le projet de loi nº 64 (art. 20, 102, 150), le RGPD (notamment art. 21 et 22) que le projet de loi nº C-11 (art. 2, 62(2), 63(3)).
49. Dans le cadre d'un projet académique sous l'égide de l'OBVIA, j'ai participé à la rédaction de règles de pratique qui viendraient objectiver les manières de faire des instances publiques souhaitant utiliser des outils d'intelligence artificielle. Parmi les principes proposés, l'un d'entre eux est justement la justification sociale du procédé afin de valider au préalable que les gains obtenus soient supérieurs aux risques de dommages. Reprenant à certains égards le test de l'arrêt *Oakes* (*R.* c. *Oakes*, [1986] 1 R.C.S. 103), il est important d'un point de vue social d'évaluer la pertinence de l'outil.
50. K. BENYEKHLEF et P.-L. DÉZIEL, préc., note 14, p. 10.

difficile équilibre entre des libertés fondamentales concurrentes est distinctement opéré.

1.2.1 PRP et sites d'évaluation

Note2B. Il y a de cela une douzaine d'années, tout un débat a eu lieu relativement à la capacité d'un site français de noter les professeurs[51]. Le site en question, *Note2Be*, autorisait n'importe qui à associer un nom, un prénom, un établissement à une note allant de 0 à 20. En France, que ce soit au niveau des directives gouvernementales, des décisions de la Commission nationale de l'informatique et des libertés (ci-après « CNIL »)[52], du Tribunal de grande instance (ci-après « TGI »)[53] ou de la Cour d'appel[54], ou encore des représentants syndicaux du monde de l'éducation, une rare unanimité condamnait l'utilisation de ces renseignements personnels. Ce qui peut surprendre dans une perspective canadienne c'est que c'est la raison d'être de ce site qui a été remise en cause. Dans la mesure où toutes les instances de contrôle consultées réclamaient un consentement préalable à l'utilisation des données, un tel site ne peut fonctionner ; exister. Et si tant est que ce soit un indice sur la différence culturelle, la doctrine semblait elle aussi unanime sur le peu de pertinence de telles plateformes[55].

RateMD. Récemment, un cas similaire s'est présenté devant le Commissariat à la protection de la vie privée du Canada[56]. Une dentiste de Colombie-Britannique se plaignait du fait que ses données soient utilisées sans son consentement et que des commentaires soient associés à son nom, une situation qui se présente bien au-delà des professions de la santé[57]. Même si le Commissariat s'est plaint des carences de la loi actuelle, en l'occurrence la loi PIPEDA, à la différence de l'Europe, il ne remet pas en cause la raison d'être du site

51. Vincent GAUTRAIS, « "Give me five?" Traitement jurisprudentiel du commerce électronique », (2009) 21 *C.P.I.* 389, en ligne : <https://www.lescpi.ca/s/1136>.
52. *Ibid*.
53. TGI Paris, réf., 3 mars 2008, *SNES FSU et al.* c. *Sté Note2be.com*, nº 08/51650.
54. Cour d'appel de Paris 14e chambre, section A, Arrêt du 25 juin 2008, *Note2be.com* c. *SNES FSU et autres*.
55. V. GAUTRAIS, préc., note 51, p. 401.
56. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE AU CANADA, « Un site d'évaluation des professionnels de la santé cesse de facturer le retrait des avis, une "zone interdite" de la LPRPDE », Conclusions en vertu de la LPRPDE 2020-002, 30 juin 2020, en ligne : <https://priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2020/lprpde-2020-002/>.
57. Notamment au regard des nombreux sites « d'évaluation » des professeurs.

ou du type de site lui-même. Ainsi, une balance des intérêts en cause est effectuée, tant du professionnel de santé que du patient[58]. Si le premier a des droits en lien avec sa vie privée, les patients disposent d'un droit à être informés et ces sites participent à cet exercice. Également, les informations générales, génériques, utilisées sur ce genre de sites (nom, prénom, profession, adresse, etc.), bien qu'elles soient considérées comme des renseignements personnels, bénéficient d'un régime d'exception faisant en sorte qu'un consentement préalable à leur utilisation n'est pas requis[59]. Encore une fois, n'eût été de ce traitement dérogatoire, c'est la raison d'être du site qui serait remise en cause. Enfin, le Commissariat considère que la fin, l'objectif, la raison d'être du site est acceptable[60], conformément au critère qui a été interprété de l'article 5(3)[61]. En fait, le principal enjeu de cette affaire, qui a donné lieu à une correction, est que la plateforme exigeait le paiement d'une somme d'argent pour corriger ou effacer des propos jugés faux, personnels ou diffamants. Or, il apparaît clairement que l'utilisation des renseignements personnels dans le but de réclamer une somme d'argent est une pratique inacceptable[62]. Une différence sensible apparaît donc dans la manière de traiter cette situation identique, l'enjeu n'étant pas ici en lien avec la raison d'être du site, mais bien en lien avec les modalités d'application.

58. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE AU CANADA, Conclusions en vertu de la LPRPDE 2020-002, préc., note 56, par. 57.
59. *Ibid.* : voir notamment le par. 39 : « Néanmoins, le Commissariat est d'avis que les coordonnées d'affaires de la plaignante qui figurent dans le site Web de RateMDs sont accessibles au public au sens du *Règlement précisant les renseignements personnels auxquels le public a accès* (le Règlement). Par conséquent, RateMDs n'a pas à obtenir le consentement de la plaignante pour recueillir, utiliser et communiquer ses coordonnées d'affaires conformément aux alinéas 7(1)d), 7(2) c.1) et 7(3)h.1) de la Loi. »
60. *Ibid.*, par. 75 : « De l'avis du Commissariat, sous réserve de la préoccupation mentionnée ci-dessous, une personne raisonnable ne considérerait généralement pas que la collecte, l'utilisation et la communication de renseignements liés à des avis et à des classements relatifs à des professionnels de la santé par RateMDs comme une fin inappropriée dans les circonstances. Conformément à l'analyse de la question du consentement présentée ci-dessus, les intérêts des patients qui publient sur le site Web et en particulier l'intérêt public des patients éventuels qui pourraient bénéficier de ces avis et classements dans le choix d'un professionnel de la santé laissent entendre que les objectifs de RateMDs sont généralement appropriés. »
61. *A.T.* c. *Globe24h.com*, 2017 CF 114, par. 74.
62. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE AU CANADA, *Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5(3)*, mai 2018.

1.2.2 PRP et oubli

Origines. Les différences culturelles peuvent aussi se matérialiser dans l'illustration d'une jurisprudence bien connue en Europe, où un citoyen espagnol a obtenu gain de cause en demandant à une plateforme de déréférencer une information relative à une faillite passée[63]. Cette jurisprudence a été ensuite en grande partie reprise dans le RGPD[64], l'oubli se matérialisant soit par l'effacement ou la désindexation dans les moteurs de recherche.

Inspirations législatives canadiennes. La mise de l'avant de ce nouveau droit subjectif a sans aucun doute eu une influence sur les projets de loi fédéral et provincial[65]. Car si le droit à l'oubli pouvait donner lieu à certaines formes de reconnaissance, au cas par cas, par la jurisprudence[66], il est difficile de croire qu'un droit équivalent à celui disponible en Europe existe au Canada[67]. Relativement au projet de loi nº C-11, l'article 55(1) est venu mettre en place une procédure assez circonscrite[68]. Côté provincial, le nouvel article 28.1 de la *Loi*

63. CJUE, G*oogle Spain SL et Google Inc.* c. *Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, Affaire C-131/12, 13 mai 2014, arrêt de la Cour (Grande chambre), ECLI:EU:C:2014:317.
64. Art. 17 RGPD.
65. Même si le Commissariat fédéral s'en défend. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE AU CANADA, *Projet de position du Commissariat sur la réputation en ligne*, 26 janvier 2018, en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-sur-la-reputation-en-ligne/pos_or_201801/> : « Dans l'ensemble, le pouvoir de demander le déréférencement de résultats de recherche ou l'effacement de renseignements à la source est, dans certaines situations, similaire au "droit à l'effacement ('droit à l'oubli')" prévu par le *Règlement général sur la protection des données* (RGPD) de l'Union européenne. Toutefois, le rapport ne constitue pas l'adoption au Canada d'un cadre européen. Il s'agit plutôt d'une interprétation des lois canadiennes actuelles et des recours qu'elles prévoient concernant la réputation en ligne. » (nos soulignements)
66. On peut notamment citer une toute récente décision de la Cour fédérale en juillet 2021 qui reconnaît un tel droit. Michael GEIST, « Episode 95: Mark Phillips on the Federal Court of Canada's Right to be Forgotten Ruling », *Michael Geist*, 19 juillet 2021, en ligne : <https://www.michaelgeist.ca/podcast/episode-95-mark-phillips-on-the-federal-courts-decision-on-the-right-to-be-forgotten/>.
67. *CL* c. *BCF Avocats d'affaires*, 2016 QCCAI 114, par. 60-61, la commission indique qu'« il n'est pas certain que ce droit [le droit à l'oubli], reconnu en Europe, trouve application au Québec. »
68. Projet de loi nº C-11, préc., note 8, art. 55(1) : « L'organisation qui reçoit d'un individu une demande écrite visant à ce qu'elle procède au retrait des renseignements personnels qu'elle a recueillis auprès de lui, procède, dès que possible, à leur retrait si, à la fois : a) le retrait n'entraîne pas le retrait des renseignements personnels d'un autre individu dont ce renseignement ne peut être retranché ; b) aucune exigence de la présente loi ou du droit fédéral ou provincial ni aucune restriction contractuelle raisonnable ne l'en empêche ».

sur la protection des renseignements personnels dans le secteur privé (ci-après « Loi sur le privé »), proposé par le projet de loi nº 64, se rapproche davantage du modèle européen[69], et ce, même si l'ambition de reconnaître un droit à l'oubli est moins marquée qu'en Europe[70]. Mais au-delà de ces questionnements, cette prérogative offerte aux individus présente deux types de problématiques.

Différences substantielles. En premier lieu, il apparaît clairement que substantiellement, il n'y a pas « une » position canadienne, mais bien plusieurs. Ces aménagements sur le droit à l'oubli proposés dans les deux projets de loi précités s'intègrent justement dans un contexte jurisprudentiel qui n'est pas univoque. Si le RGPD a pu aisément insérer un principe reconnu par la jurisprudence, et donc présentant des liens « culturels » avec la situation européenne, la situation n'est pas équivalente au Canada. À titre d'exemple, la Cour suprême a présenté une vision retenue quant à la possibilité d'obliger *Google* à retirer des liens hypertextes[71] et plus généralement à densifier les obligations de ceux qui réfèrent à des liens correspondant à du contenu mis en ligne par autrui[72]. Sans prétention d'exhaustivité, une ambivalence prévaut entre ceux qui militent pour un nouveau droit aux individus[73] et d'autres au contraire qui considèrent que le droit

69. Projet de loi nº 64, préc., note 7, art. 113 : « […] **28.1** La personne concernée par un renseignement personnel peut exiger d'une personne qui exploite une entreprise qu'elle cesse la diffusion de ce renseignement ou que soit désindexé tout hyperlien rattaché à son nom permettant d'accéder à ce renseignement par un moyen technologique, lorsque la diffusion de ce renseignement contrevient à la loi ou à une ordonnance judiciaire. Elle peut faire de même, ou encore exiger que l'hyperlien permettant d'accéder à ce renseignement soit réindexé, lorsque les conditions suivantes sont réunies : 1º la diffusion de ce renseignement lui cause un préjudice grave relatif au droit au respect de sa réputation ou de sa vie privée ; 2º ce préjudice est manifestement supérieur à l'intérêt du public de connaître ce renseignement ou à l'intérêt de toute personne de s'exprimer librement ; 3º la cessation de la diffusion, la réindexation ou la désindexation demandée n'excède pas ce qui est nécessaire pour éviter la perpétuation du préjudice. […] ».
70. OPTION CONSOMMATEURS, *Projet de loi nº 64 – Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, commentaires d'Option Consommateurs présentés à la Commission des institutions, 29 septembre 2020, p. 12 : « Option consommateurs accueille favorablement l'instauration d'une forme de "droit à l'oubli" à l'article 28.1 de la *Loi sur le privé*. Nous estimons que ce droit, plus restreint qu'en Europe, propose un équilibre judicieux entre, d'une part, la liberté d'accès à l'information et la liberté d'expression, et, d'autre part, le droit à la vie privée et à la réputation. »
71. *Google Inc.* c. *Equustek Solutions Inc*., 2017 CSC 34.
72. *Crooke* c. *Newton*, 2011 CSC 47.
73. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Projet de position du Commissariat sur la réputation en ligne*, préc., note 65 ; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Mémoire du*

général est susceptible de gérer les cas de retrait ou de désindexation des pages en cause[74].

Difficultés applicatives. En second lieu, et peut-être surtout, la mise en place de ces mesures nous laisse perplexe quant à la façon dont ces dispositions, si adoptées, vont être interprétées. Ainsi, on peut s'interroger sur l'issue qui serait rendue à une situation conforme à la récente jurisprudence européenne où des personnes accusées de meurtres sont parvenues à effacer des références journalistiques faisant référence à ces faits passés[75]. Outre une interprétation sans doute plus ferme de la liberté d'expression[76], plusieurs craignent soit la censure[77] soit une diligence excessive de la part des plateformes à retirer des contenus qui risquent d'être problématiques :

> As many commentators have pointed out, these corporations have an incentive to err on the side of removal to reduce costs and/or to avoid legal liability and the hefty fines to which they are exposed in case of non-compliance.[78]

Un malaise est donc identifiable lorsqu'à la suite de l'initiative d'un individu, une décision est mise en avant par la plateforme elle-

---

Commissariat à la protection de la vie privée du Canada sur le projet de loi C-11, la Loi de 2020 sur la mise en œuvre sur la Charte du numérique, préc., note 42.

74. Pierre TRUDEL, « Moteurs de recherche, déréférencement, oubli et vie privée en droit québécois », (2016) 21 *Lex electronica* 89, en ligne : <https://www.lex-electronica.org/s/1535> ; BARREAU DU QUÉBEC, *Mémoire du Barreau du Québec : Projet de loi nº 64 – Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, mémoire présenté à la Commission des institutions de l'Assemblée nationale dans le cadre des consultations particulières et auditions publiques sur le projet de loi nº 64, septembre 2020, en ligne : <http://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CI/mandats/Mandat-43315/memoires-deposes.html> ; E. GRATTON *et al.*, préc., note 10.
75. CEDH, *M.L. et W.W.* c. *Allemagne*, nº 60798/10 et 65599/10, 28 juin 2018, en ligne : <http://hudoc.echr.coe.int/fre?i=002-11988>, citée dans Pierre TRUDEL, « Effacer le passé : un droit ? », 17 juillet 2018, *Le Devoir*, en ligne : <https://www.ledevoir.com/opinion/chroniques/532531/effacer-le-passe-un-droit>.
76. À titre d'exemple, il est possible de penser que relativement à une affaire comparable, les juges considéreraient que la diffusion de tels propos serait couverte par le critère de « l'intérêt du public de connaître ce renseignement » que l'on trouve à l'article 113 (correspondant à l'article 28.1) du projet de loi nº 64.
77. P. TRUDEL, préc., note 74.
78. Eloïse GRATTON et Jules POLONETSKY, « Privacy above all other Fundamental Rights? Challenges with the Implementation of a Right to be Forgotten in Canada », août 2016, p. 17, en ligne : <https://fpf.org/wp-content/uploads/2016/04/PolonetskyGratton_RTBFpaper_FINAL.pdf>. Les auteurs citent notamment McKay CUNNINGHAM, « Free Expression, Privacy and Diminishing Sovereignty in the Information Age: The Internationalization of Censorship », (2016) 69 *Arkansas Law Review* 71.

même, l'État n'intervenant, éventuellement, que pour remettre en cause cette décision[79].

1.2.3 PRP et publicité des jugements

Nouvel équilibre. Autre illustration de ces différences culturelles, il nous plaît de référer à la publicité des jugements qui là encore témoigne d'un équilibre profondément distinct entre des principes fondamentaux mis en opposition. Car en matière de publicité judiciaire, la balance s'opère bien entendu entre vie privée des individus et publicité des débats judiciaires ; balance certes renouvelée dans un contexte numérique qui exacerbe la mise en opposition[80]. Le numérique vient, en effet, renforcer le caractère public des décisions, celles-ci qui se trouvaient autrefois disponibles dans des bibliothèques de droit étant désormais accessibles au vu et au su de tous : sur Internet[81]. Cela dit, ce changement de contexte ne doit pas forcément remettre en cause des principes bien établis sur chaque continent. Des principes qui, frontalement, s'opposent.

France. Du côté du droit français, une disposition du Code de l'organisation judiciaire a récemment été modifiée afin de préciser la donne. Ainsi, si le principe de la mise en ligne des décisions judiciaires est mis en avant, un travail de caviardage s'impose sur un nombre substantiel d'informations : les noms, prénoms et autres données concernant les parties, celles concernant les tiers qui permettraient d'identifier les parties prenantes, l'identification des magistrats et greffiers dont l'utilisation des données est tout simplement interdite[82]. De façon similaire, l'anonymisation des données à caractère personnel est requise dans le Code des relations entre le public et l'administration[83]. Notons que dans une approche européenne, la publicité des

79. E. GRATTON *et al.*, préc., note 10, p. 13 : « […] il apparaît déconcertant d'exiger des entreprises privées qu'elles mettent en balance les droits et libertés fondamentaux et déterminent ce qui est dans l'intérêt public, et ce, avec peu de contrôle des autorités gouvernementales ou des tribunaux de droit commun, et sans garanties ou mesures de sécurité procédurales. »
80. Teresa SCASSA, « Personal information in tribunal decisions: still seeking a balance with the open courts principle », 20 août 2018, en ligne : <www.teresascassa.ca>.
81. MINISTÈRE DE LA JUSTICE DE LA RÉPUBLIQUE FRANÇAISE, *L'Open Data des décisions de justice*, novembre 2017, en ligne : <http://www.justice.gouv.fr/publication/open_data_rapport.pdf> (ci-après « Rapport Cadiet, *L'Open Data des décisions de justice* »).
82. Code de l'organisation judiciaire, article L. 111-13, modifié par la *Loi n° 2019-22 du 23 mars 2019*, art. 33.
83. Code des relations entre le public et l'administration, art. L. 321-1 à L. 326.1.

débats judiciaires n'est pas mise de côté ; simplement, il est souvent considéré que le retrait de certaines informations, notamment personnelles, ne pose pas d'atteinte à ce principe[84].

Canada. Dans une perspective canadienne, l'ouverture des tribunaux est un principe grandement consacré[85], prenant appui sur la liberté d'expression et la liberté de la presse[86]. Ceci a d'ailleurs été confirmé récemment par la Cour suprême :

> Le test des limites discrétionnaires à la publicité des débats judiciaires vise à maintenir la présomption tout en offrant suffisamment de souplesse aux tribunaux pour leur permettre de protéger d'autres intérêts publics lorsqu'ils entrent en jeu. Pour obtenir gain de cause, la personne qui demande au tribunal d'exercer son pouvoir discrétionnaire de façon à limiter la présomption de publicité doit établir ce qui suit : 1) la publicité des débats judiciaires pose un risque sérieux pour un intérêt public important ; 2) l'ordonnance sollicitée est nécessaire pour écarter ce risque sérieux pour l'intérêt mis en évidence, car d'autres mesures raisonnables ne permettront pas d'écarter ce risque ; et 3) du point de vue de la proportionnalité, les avantages de l'ordonnance l'emportent sur ses effets négatifs.[87]

Disposant de bases historiques issues de la *Magna Carta*[88], sa raison d'être est principalement axée sur la transparence et l'imputabilité des tribunaux :

> The very legitimacy of the legal system depends on « public acceptance of process and outcome » and the open court system promotes this acceptance by ensuring the accountability of the justice system. Canadian courts regularly state that the open court principle builds public confidence in the integrity of

84. Voir, par exemple, Anne DEBET, « Contribution de M^me^ Anne Debet », dans Rapport CADIET, *L'Open Data des décisions de justice*, préc., note 81, p. 181 : « Dans un autre arrêt du 6 octobre 2009 (*C. C.* c. *Espagne*, Requête n^o^ 1425/06), la CEDH ne décèle pas l'existence d'un "aspect primordial de l'intérêt public" (§33) qui justifiait "la publication de l'identité d'une personne en toutes lettres en rapport avec son état de santé dans un jugement" ».
85. Par exemple *Société Radio-Canada* c. *Nouveau-Brunswick (Procureur général)*, [1996] 3 R.C.S. 480.
86. *Edmonton Journal* c. *Alberta (Procureur général)*, [1989] 2 R.C.S. 1326.
87. *Sherman (Succession)* c. *Donovan*, 2021 CSC 25.
88. Jane BAILEY et Jacquelyn BURKELL, « Revisiting the Open Court Principle in an Era of Online Publication: Questioning Presumptive Public Access to Parties' and Witnesses' Personal Information », (2016) 48-1 *Ottawa L. Rev.* 150.

> the judicial system by allowing members of the public to hold judges to account.
>
> [...]
>
> The open court principle, therefore, can clearly be understood to be a means of assuring the public accountability of the court system and its key actors, particularly judges. Open courts, however, also put parties and witnesses on public view in ways that can compromise their privacy and dignity, without necessarily contributing to the underlying purposes of public transparency, accountability, and access to justice.[89] (nos soulignements)

Si une prévalence de l'ouverture prévaut sur la vie privée, bien évidemment, des exceptions demeurent. En effet, cette présomption d'ouverture ne vaut pas dans certains domaines plus sensibles, comme le droit de la famille et les crimes à caractère sexuel. Aussi, il est toujours possible de faire une demande spécifique pour renverser la présomption[90]. Quelques cas spécifiques contraires prévalent également[91].

Désindexation partielle. Mais, de façon volontaire, il est également possible de limiter la fonction recherche d'une plateforme en intégrant une ligne de code « html », et ce, faisant en sorte que les moteurs de recherche n'accèdent pas au contenu en question. C'est par exemple ce qui s'effectue sur le site www.canlii.ca[92], l'opération étant évidemment d'une simplicité sans commune mesure avec les exercices d'anonymisation qui doivent s'opérer sur les sites équivalents européens[93].

---

89. *Ibid.*, 152 et 153.
90. *Ibid.*, 155 : « There are a variety of statute-based limitations on the open court principle in Canada. Some operate automatically in certain kinds of cases, while the applicability of others is determined on a case-by-case basis. [...] A party seeking an exception to the default of openness bears the burden of demonstrating that limiting openness is necessary in order to protect a countervailing interest of sufficient public importance. »
91. Il est possible de constater que le projet de loi nº C-11 prévoit que les décisions rendues par le tribunal de la protection des renseignements personnels et des données ne sont rendues avec les noms des parties que si celles-ci y consentent. Voir sous l'article 35 du projet de loi, l'article 18(2).
92. Voir notamment l'affaire *A.T.* c. *Globe24h.com*, 2017 CF 114.
93. Rapport Cadiet, *L'Open Data des décisions de justice*, préc., note 81.

2. Opérationnalisation de la PRP

Les trois illustrations que nous venons de présenter dans cet office d'équilibrage de libertés fondamentales concurrentes ont tenté de montrer encore une fois, d'une part, que le « curseur » ne se positionne pas au même endroit entre Europe et Amérique, et d'autre part, que d'une manière générale, la « vision large de la vie privée »[94] européenne ne trouve pas systématiquement application en Amérique. Mais il y a plus. Cette différence de perspective prend également appui sur la manière même d'opérationnaliser le renseignement personnel. À plusieurs égards, une tolérance semble de mise en Amérique quant à la façon d'utiliser les données. Sans exhaustivité aucune, cette distinction peut se vérifier pour les trois raisons suivantes.

2.1 Valorisation des données

De l'immobilisation à la circulation. D'abord, il est un changement majeur, directement impacté par les technologies, qui fait en sorte que les premiers temps de la PRP optèrent pour une protection basée sur l'immobilisation des données. Ainsi, pour protéger le dossier patient, il importait qu'il demeure conservé dans l'officine du médecin. Mais de plus en plus, afin que les données « parlent », il est nécessaire de les faire circuler[95]. Fort de cet objectif, il fallait nécessairement trouver un autre fondement que l'immobilisation sur laquelle baser la protection. La valorisation des données implique forcément la circulation de ces dernières[96]. Toujours sur le même exemple, pas de télémédecine sans circulation de données.

Légitimité à géométrie variable. Cela dit, même si une ouverture vers une utilisation des données s'envisage, l'application diffère. Nous l'avons vu notamment dans le cas des sites d'évaluation ; ce qui était légitime dans un cas ne l'était pas dans l'autre. Il en est de même dans une enquête rendue par le Commissariat à la protection de la vie privée relative à Facebook, en 2009, où la gratuité

94. P. TRUDEL, préc., note 75.
95. Pierre TRUDEL, *Améliorer la protection de la vie privée dans l'administration électronique : pistes afin d'ajuster le droit aux réalités de l'État en réseau*, réalisé pour le ministère des Relations avec les citoyens et de l'immigration du Québec, Montréal, mars 2003.
96. V. GAUTRAIS et P. TRUDEL, préc., note 23, p. 12.

de la plateforme permet de justifier la valorisation des données pour des fins publicitaires[97].

Ouverture à la valorisation. De façon encore plus éclairante, la valorisation est présente dans les textes de loi. Cela se traduit de façon particulièrement explicite dans le projet de loi nº C-11 où, au-delà du titre même qui entend « faciliter et [...] promouvoir le commerce électronique », la valorisation des données est inhérente au texte. Ainsi, l'article concernant l'objet du projet de loi est explicite à cet égard, considérant que :

> […] une part importante de l'activité économique repose sur l'analyse, la circulation et l'échange de renseignements personnels.[98]

Alors que l'objet de la loi PIPEDA prenait acte de la circulation accrue[99], ses avantages commerciaux sont désormais identifiés. Il en est de même dans la loi californienne où la vente des données est une des hypothèses principales de l'application de la loi. Cette perspective est évidemment mise en opposition avec les intérêts des individus, des consommateurs[100], mais également de justifications sociales plus collectives qui devraient être considérées[101].

2.2 Inhérence de la notion de dommages

Notion inhérente. Une autre différence qui se matérialise dans la définition même de renseignement personnel tient à la notion de dommage qui, dans une perspective nord-américaine, est

---

97. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par le CIPPIC contre Facebook », Rapport de conclusions en vertu de la LPRPDE nº 2009-008, 16 juillet 2009, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2009/lprpde-2009-008/>, voir notamment les paragraphes 132 et 134 : « Devant la "gratuité" du service de réseautage social qu'offre Facebook, je trouve raisonnable qu'on oblige les utilisateurs à consentir à la publicité Facebook comme condition de service ».
98. Projet de loi nº C-11, préc., note 8, art. 5.
99. Loi PIPEDA, préc., note 11, art. 3.
100. De façon étonnante, tant le projet de loi nº C-11 que la *Loi californienne* traitent désormais du consommateur. Plus exactement, dans le projet de loi nº C-11, alors que les dispositions continuent d'utiliser les renseignements personnels de l'individu, tous les titres réfèrent à la notion de consommateur, laissant présager une marchandisation qui tranche avec les habitudes.
101. *Supra*, par. 1.

plus souvent mise en avant. Qu'il soit subjectif ou objectif[102], il est souvent requis pour que le cadre législatif associé à la PRP s'applique. Ainsi, la PRP ne pourra être invoquée que dans les hypothèses où un dommage est susceptible de peser sur l'individu[103], les lois sur la PRP ne devant se déployer que si le risque est suffisamment grand pour justifier une action, un contrôle[104]. Selon la vision européenne, si la notion de dommage est présente, notamment dans le RGPD, on ne le trouve que de façon générale dans les considérants dudit texte et aussi dans le cadre très particulier de l'article 82 relatif aux compensations financières.

Bris de sécurité. En ce qui à trait à cette comparaison, et toujours au sujet des différences d'intensité quant à l'application des règles, il est intéressant de constater que dans le cas très particulier des obligations de sécurité, une moindre obligation pèse sur les organisations. Et si le Canada a clairement introduit cette règle afin de calquer l'exigence européenne[105], les modalités applicatives semblent plus légères que celles prévalant dans le RGPD[106].

2.3 Traitement versus opérations

Besoin de précision. En fait, et pour compléter cette comparaison substantielle, la définition de renseignement personnel est intimement liée à celle de traitement qui est de surcroît interprétée avec une grande largesse. Toujours dans cette optique de protection optimale, les textes européens ont en effet valorisé cette notion qui correspond à toutes les étapes du cycle de vie du document[107]. Une notion de traitement qui est en revanche absente des lois canadiennes

102. Ryan CALO, « The Boundaries of Privacy Harm », (2011) 86-3 *Indiana Law Journal* 1131.
103. Éloïse GRATTON, *Understanding Personal Information: Managing Privacy Risks*, LexisNexis, Markham, 2013, p. 208-217.
104. INFORMATION COMMISSIONER'S OFFICE, *Data Protection Strategy, Consultation Draft*, U.K., juin 2007, p. 5 : « Being a strategic regulator means that, in so far as we have a choice, we have to be selective with our interventions. We will therefore apply our limited resources in ways that deliver the maximum return in terms of a sustained reduction in data protection risk. That is the risk of harm through improper use of personal information. There are priorities we have to set. We need to focus most attention on situations where there is a real likelihood of serious harm ».
105. Loi PIPEDA, préc., note 11, art. 10(1) et s.
106. Art. 33 RGPD.
107. Cette notion de « cycle de vie » est employée à l'occasion dans les lois relatives à la preuve et à la gestion documentaire. On peut notamment citer, au Québec, la *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1.

et québécoises qui préfèrent identifier avec plus de finesse l'opération en cause de façon isolée telle que la conservation, la communication, la collecte, etc.[108]. Or, chacune de ces étapes ne présente pas les mêmes risques ; d'une manière générale, et à titre d'exemple, les opérations de divulgation sont susceptibles d'être passablement plus attentatoires que celles de communication interne[109]. Ceci est d'autant plus vrai dans une optique de circulation accrue des données en général et donc des données personnelles en particulier[110].

Exemple. Présentons l'illustration suivante[111] : un ministère québécois proposa à la population un service d'identification électronique sécurisée. Pour des fins de sécurité, l'administré devait saisir une ligne correspondant à une information contenue dans sa déclaration d'impôt, information ensuite vérifiée par les services gouvernementaux. Il faut noter qu'à la suite de la vérification, l'information en cause était détruite et ne trouvait plus trace dans le système. Paradoxalement, le consentement qui avait été initié – non sans difficulté afin d'expliciter au citoyen cette opération complexe à laquelle il consentait – était la seule information qui était conservée. Aussi, selon nous, une telle opération ne doit pas être interprétée comme une communication et donc, il n'y a pas lieu d'appliquer les règles associées à la PRP. En revanche, du fait de la définition englobante de la notion de traitement, il est difficile de croire que l'on puisse extraire l'application des règles de PRP. Notons que dans une hypothèse comme celle-ci, la finalité de l'opération est simple : le service au citoyen. Or, le consentement qui s'est traduit au mieux dans les faits comme un irritant, au pire comme une source d'angoisse, est le seul pis-aller pour contrer l'utilisation de données personnelles dont il est clairement possible d'affirmer que le traitement ne présente aucun risque pour l'individu.

PARTIE 2. LES DISTINCTIONS INSTITUTIONNELLES DE LA PRP

Rôles de l'État. Mais au-delà de ces différences substantielles existant entre les modèles américains et européens, il est un second groupe de distinctions qu'il est possible d'identifier : que ce soit dans le

108. *Loi fédérale sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. C-5 ; *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 12.
109. É. GRATTON, préc., note 103, p. 219-418.
110. V. GAUTRAIS et P. TRUDEL, préc., note 23, p. 19-21.
111. *Ibid*. Cette illustration est tirée d'un cas pratique que nous avons traité dans cet ouvrage.

droit actuel ou dans les projets de loi déposés récemment, on constate des velléités institutionnelles beaucoup plus fortes en Europe que dans les juridictions nord-américaines. Qu'il s'agisse de son implication, de ses fonctions, des différences culturelles apparaissent. Cette affirmation tient lieu de ce qui est et non de ce qui devrait être. À bien des égards, nous croyons que les modèles canadiens peinent d'un désengagement de l'État, tant au point de vue de ses fonctions, sa structure, son financement. Également, une réflexion s'impose sur la généralisation de formes alternatives de normativité afin de mesurer la diligence des organisations à protéger les données tout comme l'identification du droit applicable.

3. Implications distinctes de l'État

3.1 Fonctions institutionnelles distinctes

Bien évidemment, dans un domaine du droit qui détient un haut niveau d'ordre public, il est dans la nature des choses d'exercer un contrôle par le biais de sanctions dissuasives incitant les acteurs à mettre en place une diligence organisationnelle. Ceci étant dit, il importe d'aller au-delà de la « peur du gendarme ». À bien des égards, un rôle d'accompagnement est sans doute de mise.

3.1.1 Rôle classique de sanction

Canada : lois sans dent. Face à un domaine largement associé à l'ordre public, il est dans la normalité des choses d'avoir une loi qui sanctionne et qui est en mesure de jouer un rôle de dissuasion. Or, au Canada, la situation actuelle est particulièrement gênante. Si les lois provinciales, comme c'est le cas au Québec, sont susceptibles de sanctions, sources de bien peu de contraintes financières[112], la loi fédérale est impressionnante de par son incapacité. En effet, les enquêtes du Commissariat ne sont pas associées à une sanction financière, d'autant que certaines sont anonymes et donc insusceptibles d'opérer une quelconque atteinte à la réputation. Cette situation unique est problématique. Et preuve du manque de maturité juridique de la matière, les pratiques ont plus évolué avec des dénonciations journalistiques que par des décisions faisant état des manquements des organisations. C'est donc la raison pour laquelle le Commissariat est parvenu à infléchir les pratiques des entreprises

112. *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 12, art. 91.

davantage par des efforts de communication que par une approche strictement judiciaire[113].

Changements en vue. Face à cette incongruité, un appel généralisé à un redressement institutionnel[114] a été demandé. Au-delà du renforcement du caractère juridictionnel, avec la création du Tribunal de la protection des renseignements personnels et des données[115], le projet de loi nº C-11 manifeste aussi sa volonté de changement en termes de sanction. En effet, le projet de loi fédéral nº C-11[116], tout comme le projet de loi provincial nº 64[117], effectue presque un copier-coller du RGDP, reprenant dans l'ensemble le très sensationnel « 4 % » du chiffre d'affaires de l'entreprise fautive que l'on retrouve dans ce texte[118].

Bien mais… Conformément aux propos précédents, cette tendance s'imposait. Cela dit, on peut douter que cette solution soit la panacée et qu'un organisme de contrôle tel que la Commission d'accès à l'information (ci-après la « CAI »), disposant d'un budget annuel global de 7 à 8 millions, puisse parvenir à imposer une telle sanction à une multinationale. Le Québec n'est pas l'Europe, et ses 400 millions d'individus. Comme l'affirmait Montesquieu, chaque juridiction se doit d'intégrer des cadres de gouvernance adaptés à ses particularismes. Également, on peut se demander si cette menace est un effet de manche ou entend être appliquée souvent à des entreprises contrevenantes. On peut notamment se poser la question lorsque, dans le projet de loi nº C-11, l'article 94(6), sous un intitulé « But de la pénalité », il est spécifiquement mentionné que :

> (6) L'infliction de la pénalité vise non pas à punir mais à favoriser le respect de la présente loi.

---

113. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par le CIPPIC contre Facebook*, préc., note 97.
114. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Consultation sur les propositions du Commissariat visant à assurer une réglementation adéquate de l'intelligence artificielle*, 13 mars 2020, en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-ai/pos_ai_202001/> ; voir la proposition 11 : « Donner au Commissariat le pouvoir d'émettre des ordonnances exécutoires et d'imposer des sanctions financières aux organisations qui ne se conforment pas à la loi. »
115. Projet de loi nº C-11, préc., note 8, Partie 2, art. 35 et s.
116. Projet de loi nº C-11, préc., note 8, art. 125.
117. Projet de loi nº 64, préc., note 7, art. 151.
118. Art. 83 RGPD.

Réactivité moindre. Mais ce renforcement institutionnel de l'État, en l'occurrence de sa fonction juridictionnelle, ne passe pas que par cette seule action sur la sanction. Actuellement, l'agilité des organismes de contrôle présente au Canada une moindre réactivité qu'en Europe, sans doute du fait de ressources moindres. On peut prendre pour exemple l'hypothèse en 2020, au début de la pandémie, où des chercheurs de l'Université de Montréal tentèrent de développer une application pour tracer les risques de communication du virus : la solution COVI. Basé sur le consentement, chaque individu devant télécharger l'application, la confiance dans l'outil devant être sans faille. Or, en l'absence d'une réaction franche et rapide d'une autorité indépendante, les débats publics générèrent du doute et de la circonspection. Une suspicion qui amena par la suite la non-recommandation du Gouvernement[119]. Ce que montra, selon nous, cet épisode c'est la carence réglementaire à réagir dans l'urgence. Comparativement, en France, en l'espace de moins d'un mois, trois avis avaient été rendus par la CNIL[120]. Simplement, dans ce pays, la structure même de l'autorité de contrôle dispose d'une procédure de référé. L'urgence est prévue ; ce qui n'est pas le cas chez nous.

3.1.2 Rôles alternatifs

Revisiter le rôle juridictionnel. Au-delà de la sanction, il est d'autres fonctions qui sont clairement énumérées dans le RGPD ; près d'une vingtaine même[121]. Parmi ces fonctions, plusieurs sont associées à un rôle de « guide », deuxième grande fonction du droit avec la sanction[122], mais que nous verrons ultérieurement dans le paragraphe sur les normes[123]. Relativement à la fonction juridictionnelle, et surtout dans une perspective canadienne, il est aussi possible

119. Relativement à cette affaire, voir Vincent GAUTRAIS, « COVI : dommage ! », 5 juin 2020, en ligne : <https://www.gautrais.com/blogue/2020/06/05/covi-pourquoi-pas/>.
120. Si l'on prend le fil des événements de la CNIL relativement à l'application équivalente en France (StopCovid), cette instance a émis un premier avis principiel le 26 avril (en ligne : <https://www.cnil.fr/fr/publication-de-lavis-de-la-cnil-sur-le-projet-dapplication-mobile-stopcovid>), un deuxième avis sur le décret le 8 mai 2020 (en ligne : <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000041869923/>), et une délibération le 25 mai (en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2020-056-25-mai-2020-avis-projet-decret-application-stopcovid.pdf>).
121. Art. 57 RGPD.
122. Clare DALTON, « An Essay in the Deconstruction of Contract Doctrine », (1985) 94 *Yale Law Journal* 997.
123. *Infra*, par. 4.

de trouver quelques inflexions qui modernisent quelque peu le rôle des magistrats.

Rôle de persuasion. Mais revenons sur le rôle de persuasion associé à la pénalité dans le projet de loi nº C-11. Cette disposition précitée est étonnante ! Étonnante, dans la mesure où la peine est forcément associée à une sanction, surtout quand on l'associe à une pénalité d'un certain pourcentage (4 ou 5 %) du chiffre d'affaires mondial. Mais d'un autre côté, cette formule correspond tant à la tradition de négociation[124] dont le Commissaire à la protection de la vie privée use, du moins dans un premier temps, qu'à son statut « unique » qui est d'abord et avant tout un agent du Parlement[125].

Rôle d'accompagnement. Toujours dans son office juridictionnel, l'organe de contrôle est de plus en plus amené à évaluer la diligence employée par une organisation pour la protection des données. Ainsi, notamment dans le projet de loi nº 64, nous avons pu constater une extension intéressante de ce qui s'intitule communément des ententes de partage ou de communication[126]. Alors que l'on en trouve quelques traces tant en droit provincial[127] qu'en droit fédéral[128], l'idée de cette formule est qu'une organisation développe une documentation interne et que celle-ci est communiquée à l'organisme de contrôle qui pourra, à la suite d'un éventuel échange, déclarer ladite documentation conforme ou pas. Cette solution a été prévue dans le projet de loi nº 64[129] et aurait assurément pu être

124. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Comment le Commissariat protège le droit des personnes à la vie privée et en fait la promotion », en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/mm/> : « Le commissaire tient à régler les plaintes par le biais de la négociation et de discussions persuasives ».

125. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Qui nous sommes », en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/qui-nous-sommes/> : « Le commissaire à la protection de la vie privée du Canada est indépendant du gouvernement et relève directement du Parlement ».

126. V. GAUTRAIS et P. TRUDEL, préc., note 23, p. 213.

127. *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, (art. 64 – **collecte** et art. 66, 67, 67.1, 67.2, 68 et 68.1 – **communication**) ; *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, art. 45.

128. Sans avoir été appliquée, cette solution avait été préconisée dans un rapport déposé à la Chambre des communes. CHAMBRE DES COMMUNES, *Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique*, décembre 2016, p. 12, en ligne : <https://www.noscommunes.ca/Content/Committee/421/ETHI/Reports/RP8587799/ethirp04/ethirp04-f.pdf>.

129. Quatre propositions sont offertes dans le projet de loi nº 64 : art. 67.2.3 *Loi sur le secteur public en matière de recherche* ; art. 70.1 *Loi sur le secteur public en*

étendue à d'autres hypothèses[130]. En effet, en instituant un tel contrôle *a posteriori*, cette formule semble rapide[131], simple, efficace, et surtout permet très souvent d'être une alternative au consentement qui, du fait de son caractère fictif, est facilement critiquable quant à sa capacité de protection. Sous réserve, bien évidemment, comme déjà dit, d'une capacité de réaction de l'organisme de contrôle à traiter de telles documentations. À titre d'illustration, si l'on prend des hypothèses prévues dans le projet de loi nº 64, il nous semble plus judicieux que des opérations telles que le profilage[132] ou les décisions automatisées[133] soient assujetties à de telles ententes de communications plutôt que basées sur le seul consentement des individus. En effet, en raison de la complexité inhérente de ces opérations, il sera pour le moins hasardeux de croire que celui-ci sera en mesure de lire ou comprendre la documentation forcément technique que cela implique.

3.2 Structure administrative distincte

3.2.1 Éléments de distinction

RGPD. Le RGPD constitue la référence maîtresse qui est venue densifier les obligations en matière de vie privée. Sur le plan institutionnel, il est deux actions sur lesquelles ce texte est intervenu. En premier lieu, et sans ajouter d'autres instances[134], ce texte développe les obligations et missions que les autorités de contrôle doivent suivre[135]. À cet égard, nous ne voyons pas de distinctions majeures d'avec ce qui se passe tant auprès du Commissariat fédéral[136] que la CAI au Québec[137]. En revanche, en second lieu, nous observons

matière d'information communiquée à l'extérieur ; art. 17 *Loi sur le secteur privé en matière d'information communiquée à l'extérieur* ; art. 21 *Loi sur le secteur privé en matière de recherche*.

130. Vincent GAUTRAIS, « Auditions publiques sur le projet de loi 64 », 23 septembre 2020, en ligne : <https://www.gautrais.com/blogue/2020/09/23/auditions-publiques-sur-le-projet-de-loi-64/>.
131. Selon le projet de loi nº 64, l'entente est effective 30 jours après sa réception à la CAI : art. 23 *in fine* : « L'entente est transmise à la Commission et entre en vigueur 30 jours après sa réception par celle-ci. »
132. Projet de loi nº 64, préc., note 7, art. 18 (art. 65.0.1 et 65.0.2 *Loi sur l'accès*) et 99 (art. 8.1, 8.2 et 8.3 *Loi sur le secteur privé*).
133. Projet de loi nº 64, préc., note 7, art. 20 (art. 65.2 *Loi sur l'accès*) et 102 (art. 12.1 *Loi sur le secteur privé*).
134. Si ce n'est, au plan européen, le Comité européen de la protection des données (art. 68 et s. RGPD) qui s'assure de l'application du Règlement et joue un rôle de conseil (art. 70).
135. Art. 51-59 RGPD.
136. Loi PIPEDA, préc., note 11, art. 12 et s.
137. *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1, art. 103 et s.

des différences importantes quant à l'élaboration, la validation[138], l'identification et la certification[139] de normes informelles[140]. Car alors que les autorités européennes participent à chacune de ces étapes de production normative, il n'y a pas d'équivalent au Canada. Plus exactement, seulement certaines d'entre elles. Ainsi, au Québec, si la CAI peut produire des documents internes (guides, politiques)[141], elle n'est pas amenée à valider ou autrement certifier des documents publics[142].

Proposition de règlement sur l'intelligence artificielle. Une autre illustration des différences structurelles entre Europe et Amérique peut s'appuyer sur la récente proposition de règlement européen sur l'intelligence artificielle[143]. Ce texte intéressant montre certaines limites de transposition à un pays comme le Canada, et ce, au-delà de la question de savoir si un domaine aussi émergent, aussi neuf, est susceptible d'être d'ores et déjà encadré par une loi. Ainsi, si des différences de fond, de fonctions[144] apparaissent, la rupture la plus évidente avec une perspective canadienne est le très haut degré d'institutionnalisation que la proposition de règlement exige. En effet, ledit texte prévoit la mise en place de plusieurs instances tant européennes que nationales afin de contrôler les activités d'intelligence artificielle. Dès lors, chaque État membre doit minimalement mettre en place des autorités de surveillance, par exemple des autorités notifiantes (*notifying authorities*)[145], des organismes notifiés

138. Art. 40(5) RGPD. Cette disposition réfère à l'article 55 où l'autorité de contrôle dispose de ce pouvoir.
139. Art. 43 RGPD.
140. *Infra*, par. 4.
141. On peut notamment mentionner COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Guide d'accompagnement : Réaliser une évaluation des facteurs relatifs à la vie privée*, mars 2021, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_Guide_EFVP_FR.pdf>.
142. Autrement que dans le cadre de document interne à une entreprise. À titre d'exemple, la CAI est habilitée à prendre des ordonnances relatives à des banques de données biométriques (*Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, art. 45).
143. *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, 2021/0106 (COD), 21 avril 2021, en ligne : <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX %3A52021PC0206>.
144. Forcément, dans un contexte européen, une volonté fort légitime d'harmonisation est requise (voir par exemple l'article 1). Cette quête est beaucoup moins présente dans la structure fédérale qui est la nôtre.
145. Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, 2021/0106 (COD), 21 avril 2021, art. 30, en ligne : <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX %3A52021PC0206>.

(*notifying bodies*)[146], et ce, en plus des instances existantes dans certains domaines d'activité[147]. Au plan européen, nous constatons la mise en place d'un comité européen de l'intelligence artificielle[148].

EIDAS. Si besoin était, le dernier exemple européen que nous souhaitons prendre, même s'il est un peu plus distant du monde des données, concerne les questions d'identité numérique. Là encore, l'Europe a très tôt fait preuve d'initiative législative en adoptant un règlement sur la question[149]. Si des travaux sous l'égide des Nations Unies se sont inspirés de ce texte pour tenter d'élaborer un projet de loi modèle proposé par la CNUDCI[150], une distance fut prise avec le processus de validation préalable à la suite des agréments autorisant la mise en place de solutions *ex ante*[151]. En effet, à la suite des accréditations effectuées par des instances habilitées, des présomptions de preuve ont ainsi été rendues possibles[152]. Les débats à ce sujet ont montré le malaise généralisé de la part de nombreuses délégations, notamment américaines, à la mise en place de telles structures administratives aussi lourdes.

Distinctions nord-américaines. Comme ces trois exemples le montrent, si les cadres administratifs semblent denses en Europe, ils sont moindrement établis en Amérique du Nord. Cela se vérifie d'abord en ce qui a trait à l'importance des autorités de contrôle, comme déjà mentionné plus tôt quant à leurs fonctions et comme nous le verrons rapidement dans le paragraphe traitant sur le financement[153]. Cela vaut également pour le lien plus faible qui prévaut entre

146. *Ibid.*, art. 33.
147. On peut notamment voir dans les développements qui accompagnent la proposition que ces instances devront collaborer avec des organismes qui existent dans certains secteurs comme le domaine financier.
148. Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, 2021/0106 (COD), 21 avril 2021, art. 56 et s., en ligne : <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX %3A52021PC0206>.
149. *Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE*, disponible en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX :32014R0910&from=FR>.
150. UNCITRAL, *Projet de dispositions relatives à l'utilisation et à la reconnaissance internationale de la gestion de l'identité et des services de confiance*, 26 janvier 2021, Doc. N.U. A/CN.9/WG.IV/WP.167, en ligne : <https://undocs.org/fr/A/CN.9/WG.IV/WP.167>.
151. *Infra*, par. 4.1.
152. *Ibid.*, art. 23.
153. *Infra*, par. 3.3.

les organismes reconnus et les normes informelles applicables[154]. À ce sujet, on peut citer le Comité d'harmonisation de la *Loi concernant le cadre juridique des technologies de l'information*[155] qui depuis 20 ans n'a jamais effectué le rôle qui lui était normalement dédié, à savoir, élaborer des normes.

3.2.2 Besoin de réinstitutionnalisation

Qui ? Mais au-delà des différences institutionnelles, il importe de revenir quelque peu sur les propos tenus plus tôt selon lesquels au-delà du droit, la centralisation de l'usage des données nous incite à adopter une vision politique de la question[156] : des rapports de force s'instaurent et la mainmise de l'industrie demande à être contre-carrée. Au tout début d'Internet, David Post avait d'ailleurs exprimé l'idée que la question du « qui » contrôle était sans doute la plus importante. Or, aujourd'hui, si l'on reprend l'exemple de l'intelligence artificielle, cette réflexion autour du « qui », 25 ans après l'article de David Post, est tout aussi pertinente. Deux autrices, Julia Powles et Helen Nissembaum, écrivent même qu'en matière d'intelligence artificielle, cette question est d'autant plus importante que celle des biais qui viennent naturellement à l'esprit quand vient le temps d'évaluer les possibles travers de ces nouvelles technologies. Au-delà donc de ces problématiques, il importe de s'interroger tant sur la pertinence de telles saisies de données par des entreprises privées qui les gèrent en vase clos que sur les moyens de contrôler leur usage :

> We are well overdue for a radical reappraisal over who controls the vast troves of data currently locked down by technology incumbents. Our governors and communities should act decisively to disincentivize and devalue data hoarding with creative policies, including carefully defined bans, levies, mandated data sharing, and community benefit policies, all backed up by the brass knuckles of the law.[157]

De l'institutionnalisation à la structuration. Cela dit, il est difficile de prôner un réengagement de l'État quand celui-ci ne souhaite pas réinvestir le rôle qu'il a déjà rempli, sans concurrence.

---

154. *Infra*, par. 4.
155. RLRQ, c. C-1.1, art. 63 et s.
156. *Supra*, par. 1.1.2.
157. Julia POWLES et Helen NISSEMBAUM, « The Seductive Diversion of "Solving" Bias in Artificial Intelligence », 7 décembre 2018, *OneZero*, en ligne : <https://onezero.medium.com/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53>.

Ce contrôle des activités marchandes pourrait donc être aussi le fruit d'un dialogue plus communautaire, dès lors que des garanties de légitimité, d'effectivité, sont satisfaites[158]. Au-delà des bienfaits d'un processus participatif des acteurs à l'élaboration des règles, des voies sont ouvertes pour des degrés divers de coopération entre des acteurs privés et publics[159].

3.2.3 Besoins de fédération des disciplines

Empiétements imposés par le numérique. Rapidement, le dernier point que nous souhaitons soulever concerne la fragmentation des organismes de contrôle en fonction des éléments à contrôler. Que ce soit du fait du partage de compétences prévu dans les lois constitutionnelles où simplement à cause de la répétition de pratiques qui prévalaient dans le monde analogique, on constate une multiplication des instances susceptibles d'agir pour un même fait. Ainsi, une plateforme comportant un niveau minimal d'utilisation de données serait susceptible d'être assujettie par un grand nombre de lois et autant d'organismes de contrôle. Actuellement, au Canada, plusieurs affaires en lien avec de la publicité comportementale ont été traitées par le *Bureau de la concurrence*[160], notamment à cause du fait que cette instance dispose de pouvoirs d'investigation et de sanction passablement plus élevés que les organismes de contrôle en matière de vie privée. Pourtant, et même si la *Loi sur la concurrence* a été en l'occurrence la loi sur laquelle la condamnation s'est basée[161], l'affaire disposait peut-être d'un lien plus naturel avec le droit de la vie privée. Relativement à ce débat, deux commentaires nous semblent pouvoir être donnés. D'abord, avec des pouvoirs de sanction plus forts, on peut imaginer que le Commissariat à la protection de la vie privée aurait pu avoir son mot à dire. Ensuite, et au regard du modèle européen,

158. Vincent GAUTRAIS, *Le contrat électronique international*, Bruxelles, Bruylant, 2002, p. 325.

159. Yves POULLET, « Vues de Bruxelles. Modes alternatifs de régulation et libertés dans la société du numérique », dans Céline CASTETS-RENARD, Valère NDIOR et Lukas RASS-MASSON (dir.), *Enjeux internationaux des activités numériques*, Bruxelles, Larcier, 2021, p. 102.

160. *Telus Communications Company*, CT 2015-15, 30 décembre 2015, en ligne : <https://decisions.ct-tc.gc.ca/ct-tc/cd/en/item/462517/index.do> ; *Rogers Communications Inc.*, CT 2015-02, 16 mars 2015 en ligne : <https://decisions.ct-tc.gc.ca/ct-tc/cd/en/item/462530/index.do>.

161. *Loi sur la concurrence*, L.R.C. (1985), ch. C-34, art. 74.01(1) : « Est susceptible d'examen le comportement de quiconque donne au public, de quelque manière que ce soit, aux fins de promouvoir directement ou indirectement soit la fourniture ou l'usage d'un produit, soit des intérêts commerciaux quelconques : a) ou bien des indications fausses ou trompeuses sur un point important. »

on peut se questionner sur les risques de voir se multiplier les instances de contrôle, les instances « traditionnelles » (consommation, concurrence, vie privée, etc.) se superposant aux nouvelles instances (identité, intelligence artificielle, etc.), et ce, en fonction de domaines d'application dont le numérique cause un chevauchement de plus en plus fréquent. Un chevauchement dont nous avons déjà soulevé l'occurrence précédemment en matière de protection des libertés fondamentales[162].

3.3 Financement de la PRP

Comment ? Une véritable réflexion s'impose aussi sur la tendance au désengagement de l'État qui bien entendu est un sujet sensible dans de nombreux domaines, mais particulièrement dans celui de la protection des renseignements personnels. Ainsi, il est étonnant de constater que les organismes de contrôle, s'ils ont pris de l'importance en termes de ressources humaines, cette hausse n'a aucune mesure avec l'importance que la vie privée a prise avec le numérique. L'affaire de Cambridge Analytica a notamment montré que, si l'organisme de contrôle britannique (ICO)[163] a eu un rôle déterminant dans cette affaire, c'est grâce à un nombre de personnes dédiées beaucoup plus important que dans d'autres juridictions, et notamment au Canada, tant au fédéral[164] qu'au Québec[165], mais aussi en comparaison avec d'autres juridictions pourtant considérées comme très « pro-vie privée »[166]. Arrêtons de croire que la protection des renseignements personnels ne coûte pas d'argent. Il va forcément en coûter pour le gestionnaire des données, conformément au principe de responsabilisation ; il va forcément en coûter également pour l'État qui va devoir s'assurer de l'application des règles en la matière. Plus exactement, il importe d'envisager les modalités de financement susceptibles de s'appliquer, allant d'un support financier exclusif de

162. *Supra*, par. 1.1.2.
163. Le rapport annuel de l'ICO fait état du fait que 722 postes permanents sont dédiés à cette organisation (en ligne : <https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf>).
164. Si nous n'avons pas été capables de trouver des chiffres précis, la CPVP compte, à notre connaissance, une cinquantaine de personnes à temps plein.
165. Selon le rapport annuel de la CAI, 58 personnes sont associées à la CAI au 31 mars 2019 (voir : <https://www.cai.gouv.qc.ca/documents/CAI_RAG_2018-2019.pdf>).
166. La France, par exemple, qui a une population globalement identique à la Grande-Bretagne a, quant à elle, un organisme de contrôle en matière de vie privée (la CNIL) qui ne réunit « que » 225 personnes. Pour en savoir plus, voir : <https://www.cnil.fr/fr/statut-et-organisation-de-la-cnil>.

l'État à des solutions alternatives, davantage axées sur des modèles d'affaires très variés[167].

4. Rapport distinct aux normes informelles

Horizontalité. Dans un ouvrage en forme de discussion, le sociologue Guy Rocher, qui a grandement travaillé sur les normes informelles[168], a déclaré qu'en Amérique du Nord :

> […] la démocratie est plus horizontale que la démocratie républicaine.[169]

Selon nous, cette affirmation représente bien une divergence de vue et selon laquelle la reconnaissance des normes informelles s'opère différemment d'un continent à l'autre. En effet, alors que dans le système européen, la faveur est pour que des organismes dédiés, que ce soit les autorités de contrôle elles-mêmes ou d'autres qu'elles ont identifiées, effectuent la reconnaissance des normes applicables, une plus grande souplesse prévaut généralement en Amérique du Nord. Dans le premier cas, la place de l'État est indispensable ; dans l'autre, souvent à cause du repli de celui-ci, il est comblé par des normes de l'industrie. Et subséquemment, par les juges sur lesquels repose l'ouvrage de reconnaître la qualité des normes concernées.

4.1 Différences quant à la place de l'État

Co-régulation vs Autorégulation. Le débat est vieux comme le Web. Et bien évidemment, il n'est pas propre aux domaines technologiques[170]. Simplement, on aperçoit dans un grand nombre de

---

167. Il est notamment intéressant de regarder comment l'ICO britannique fonctionne. En effet, cette organisation indépendante fonctionne à 85 % avec des fonds provenant d'une « taxe » (Data Protection Fee). Cette somme obligatoire est prévue dans la loi et oscille entre 40 et 2 900 livres selon la taille de l'institution. Pour en savoir plus, voir : <https://ico.org.uk/for-organisations/data-protection-fee/faqs-data-protection-fee-payment-and-online-registration/>.
168. Guy ROCHER, « Pour une sociologie des ordres juridiques », (1988) 29 *Cahiers de droit* 91 ; Andrée LAJOIE, Roderick MACDONALD, Richard JANDA et Guy ROCHER, *Théories et émergence du droit : pluralisme, surdétermination et effectivité*, Montréal/Bruxelles, Thémis/Bruylant, 1998 ; Guy ROCHER, « Les phénomènes d'internormativité : faits et obstacles », dans Jean-Guy BELLEY (dir.), *Le droit soluble. Contributions québécoises à l'étude de l'internormativité*, coll. « Droit et société », Paris, Librairie générale de droit et de jurisprudence, 1996, p. 25-42.
169. François ROCHER, *Guy Rocher : entretiens*, Montréal, Boréal, 2010, p. 114.
170. Pour une référence récente, Yves POULLET, préc., note 159, p. 91.

domaines, principalement à saveur technique, la mise en place d'un « mille-feuille » normatif où, en plus de règles formelles, législatives et réglementaires, s'en ajoutent nécessairement d'autres qui viennent objectiver les obligations à satisfaire. Ainsi, le domaine de la PRP, comme d'autres, est amené à développer des normes informelles qui donnent lieu à l'élaboration de normes individuelles. Les premières correspondent à des standards, codes de conduite, lignes directrices, provenant d'une institution donnée. Les secondes sont constituées de documents internes, politiques, procédures, audits, que l'organisation va elle-même mettre en place pour montrer sa diligence. Or, à ces deux paliers normatifs, la quête de légitimité peut être largement accentuée lorsque l'État décide d'intervenir, directement ou indirectement, en participant à l'identification des normes. En Europe, le phénomène est usuel et se retrouve par exemple clairement dans le RGPD – ce qu'Yves Poullet appelle la « corégulation descendante »[171] – lorsque les autorités de contrôle sont habilitées à reconnaître des organismes capables d'agréer des codes de conduite[172]. Équivalent que l'on ne retrouve pas, au meilleur de notre connaissance, au Québec ou au Canada. Ce qui est d'autant plus problématique que l'État n'a pas vraiment comblé ce « vide » par des décrets ou autres règlements applicatifs. Au plus, à l'occasion, l'autorité de contrôle va elle-même élaborer quelques directives généralement assez génériques et non applicables en l'état par les organisations[173]. En revanche, il existe quelques hypothèses encore rares où les normativités individuelles peuvent être *a posteriori* évaluées par les autorités compétentes[174].

Lourdeur vs Carences normatives. Entre les deux modèles, les grands traits sont faciles à tracer, et ce, même s'ils ne s'opposent pas forcément. D'un côté, celui de la corégulation, nous sommes face à un système administratif lourd, couteux[175], qui autorise une moindre souplesse aux acteurs privés. De l'autre, celui de l'autorégulation, des doutes existent tant sur la qualité des normes utilisées[176] que sur la suffisance des mesures suivies pour les respecter. Notons

171. *Ibid.*, p. 97.
172. Art. 57(q) RGPD. Les autorités de contrôle auront seulement à déterminer les critères selon lesquels les agréments peuvent se faire (voir art. 57(p)).
173. Voir par exemple COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Guide d'accompagnement : Réaliser une évaluation des facteurs relatifs à la vie privée*, préc., note 141.
174. *Supra*, voir nos propos sur les ententes de partage, par. 3.1.2.
175. Il est vrai qu'en Europe, les coûts peuvent être soutenus du fait d'une population conséquente et d'un haut niveau d'intégration sociale et économique.
176. Vincent GAUTRAIS, « Quête d'une meilleure garantie normative : les algorithmes sous contrôle », dans Catherine THIBIERGE (dir.), *La garantie normative : exploration d'une notion fonction*, Mare & Martin, avril 2021.

également qu'au-delà de la solution documentaire qui est généralement employée, et qui peut donner lieu à l'un ou l'autre des modèles, s'ajoutent parfois des solutions plus technologiques qui peuvent être préconisées afin de mesurer par exemple l'existence de biais discriminatoires dans une application. Par des empreintes technologiques, logicielles, la mesure permet d'identifier l'état de la situation à un moment « t »[177]. Or, dans un tel cas, ce « Polaroïd » demandera forcément à être analysé par une tierce partie, l'auto-analyse n'étant en l'occurrence pas d'une aide réelle.

Ex post vs Ex ante. Face à cette dualité transparaît une évidence généralement consacrée : une crédibilité plus grande est donnée à la solution qui est validée par un tiers indépendant. Aussi, des présomptions peuvent être associées à des solutions ainsi certifiées[178] (*ex ante*) alors que dans la solution autoréglementée, forcément, la reconnaissance finale passe ultérieurement (*ex post*) par l'appréciation d'un juge. Cela dit, au regard d'une jurisprudence assez famélique, l'adoubement judiciaire n'est pas souvent convaincant, l'analyse étant souvent technique et se concrétisant par le biais de témoignages, experts ou non[179]. En l'absence de reconnaissance expresse comme cela se fait en Europe, l'arrimage entre normes formelles et informelles est délicat. Et conformément aux règles de preuve, faute de présomption, la diligence employée doit être prouvée par la personne qui l'invoque[180]. Ceci nous ramène à la difficile question des usages commerciaux et de leur reconnaissance[181].

177. Joshua A. KROLL, Joanna HUEY, Solon BAROCAS, Edward W. FELTEN, Joel R. REIDENBERG, David G. ROBINSON et Harlan YU, « Accountable Algorithms », (2017) 165 *University of Pennsylvania Law Review* 633, 662 à 674, et ce, sous l'intitulé « Technical Tools for Procedural Regularity ».
178. Art. 42 et s. RGPD.
179. Pour faire état du dialogue entre normes juridiques et normes techniques dans la jurisprudence, voir Vincent GAUTRAIS, « Normativité et droit du technique », dans Stéphane ROUSSEAU (dir.), *Juriste sans frontières, Mélanges Ejan Mackaay*, Montréal, Éditions Thémis, 2015, p. 311.
180. Art. 2803 C.c.Q.
181. V. GAUTRAIS, préc., note 158, p. 220 ; Vincent GAUTRAIS, *Neutralité technologique : Rédaction et interprétation des lois face aux changements technologiques*, Montréal, Éditions Thémis, 2012.

4.2 Différences quant à la reconnaissance distincte des normes informelles

4.2.1 Différences quant à la reconnaissance des normes informelles

Agrément. Là encore, les modes de reconnaissance des normes informelles nous sont proposés par l'exemple européen où un encadrement institutionnellement fort est organisé. D'ores et déjà, on peut dire qu'aucun équivalent n'existe au Canada. C'est d'abord le cas des processus d'agrément des codes de conduite[182].

Certification et label. C'est ensuite le cas de procédures très développées qui vont certifier le traitement des données[183]. Au-delà de la lourdeur associée à une telle structure, la « privatisation » de la reconnaissance est associée à des doutes tant sur sa pertinence que sur sa capacité à faire le tri entre le bon grain et l'ivraie[184]. Notons qu'il y a une vingtaine d'années, le commerce électronique naissant avait tenté de développer de tels outils pour différencier les sites marchands, et ce, alors que les États refusaient de s'investir au-delà de l'encouragement du secteur privé à le faire. L'expérience a fait long feu, et ce, après un engouement qui avait vu plusieurs centaines de labels être initiées. Mais après quelques mois ou années, aucun projet ne perdura du fait de la convergence de plusieurs handicaps : le caractère volontaire, les coûts, le refus des États de s'engager à soutenir une certification spécifique ou à y investir[185]. Autant de circonstances qui prévalent encore aujourd'hui.

4.2.2 Différences quant à la reconnaissance des normes individuelles

Silence. Dans la hiérarchie normative associée à la PRP, nous sommes rendus à l'étape ultime, à savoir, ce que nous nous plaisons à qualifier de normativité individuelle[186] c'est-à-dire la documentation

182. Art. 57(q) RGPD.
183. Art. 42 et 43 RGPD.
184. Olivia TAMBOU, « L'introduction de la certification dans le règlement général de la protection des données personnelles : quelle valeur ajoutée », (2016) 125 *Revue Lamy droit de l'immatériel* 51.
185. Vincent GAUTRAIS, « Labellisation des sites sur Internet et protection du consommateur : vision comparée », (2001) *Jurisclasseur Consommation et concurrence* 4-6.
186. Vincent GAUTRAIS, « Preuve et développement durable : objectivation du droit par la normativité individuelle », dans Vincent GAUTRAIS et Mustapha

interne qui concrètement explicitera les tenants et aboutissants illustrant la diligence employée. Paradoxalement, le RGPD, si prolixe à encadrer, ne prévoit pas de modalités d'objectivation de la documentation, au-delà bien entendu de la nécessité d'en disposer, comme le RGPD en témoigne[187].

Ententes de partage. Tout aussi paradoxalement, c'est peut-être là, du moins au Québec, que certaines voies institutionnelles sont proposées. Sans revenir sur nos précédents propos sur les ententes de partage[188], quelques voies existent déjà et d'autres sont susceptibles d'être adoptées par le projet de loi nº 64. Également, certaines pistes apparaissent par exemple quant à la manière dont une analyse d'impact relative à la vie privée doit être rédigée[189].

CONCLUSION

En conclusion, comme souvent, nous sommes sujets à une certaine ambivalence. D'un côté, la comparaison entre l'Europe et l'Amérique, relativement à la façon d'appliquer le droit au domaine de la vie privée, nous amène à dire que « comparaison n'est pas raison ». Aussi et plutôt qu'européaniser le droit canadien face à la situation canadienne, il est important de faire coller le droit à la réalité, surtout dans un contexte où il est possible de croire que la mondialisation à tout crin est peut-être en voie de saturation, de suffocation. À certains égards, il est davantage possible de croire qu'il soit nécessaire, dans certains cas, de balkaniser la protection de la vie privée, notamment face à des approches irréconciliables qui s'exercent actuellement dans certaines parties du monde (comme la Chine).

D'un autre côté, il n'en demeure pas moins que la comparaison constitue une approche méthodologique particulièrement utile dans ce domaine « neuf », sans recul, de surcroît profondément remanié par le numérique. À titre d'exemple, la constitutionnalisation de ces questions aurait intérêt à être mieux identifiée dans les futures lois canadiennes[190], tout comme cela se fait en Europe. Sur ce point, et

---

MEKKI (dir.), *Preuve et développement durable*, Montréal, Éditions Thémis, 2016, p. 43-74.

187. RGPD, art. 30 (Registre des activités de traitement), 32 (Sécurité du traitement) et 35 (Analyse d'impact relative à la protection des données).
188. *Supra*, par. 3.1.2.
189. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Guide d'accompagnement : Réaliser une évaluation des facteurs relatifs à la vie privée*, préc., note 141.
190. *Supra*, par. 1.1.2.

comme nous avons commencé, nous pouvons mentionner une référence gaullienne, plus exactement de Malraux, qui relativement à la culture dont nous avons vanté la prise en considération déclarait qu'elle « ne s'hérite pas, elle se conquiert ».