CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

PROTECTION DE LA VIE PRIVÉE ET MÉDIAS SOCIAUX À L'ÈRE DES MÉGADONNÉES

Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le président

Pierre-Luc Dusseault, député

AVRIL 2013

41e LÉGISLATURE, PREMIÈRE SESSION

PROTECTION DE LA VIE PRIVÉE ET MÉDIAS SOCIAUX À L'ÈRE DES MÉGADONNÉES

Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le président

Pierre-Luc Dusseault, député

AVRIL 2013

41e LÉGISLATURE, PREMIÈRE SESSION

COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE

PRÉSIDENT

Pierre-Luc Dusseault

VICE-PRÉSIDENTS

Scott Andrews

Patricia Davidson

MEMBRES

Charlie Angus	Brad Butt	Dean Del Mastro
Charmaine Borg	Blaine Calkins	Earl Dreeshen
Alexandre Boulerice	John Carmichael	Colin Mayes

AUTRES DÉPUTÉS AYANT PARTICIPÉ

Mike Allen	Jinny Jogindera Sims	Joe Preston
Dean Allison	Daryl Kramp	James Rajotte
Kelly Block	Jean-François Larose	L'hon. Geoff Regan
Marjolaine Boutin-Sweet	Laurin Liu	Kennedy Stewart
Rod Bruinooge	L'hon. Lawrence Mac Aulay	Merv Tweed
Sean Casey	Joyce Murray	Chris Warkentin
L'hon. Denis Coderre	Tilly O'Neill-Gordon	
Richard M. Harris	François Pilon	

GREFFIER DU COMITÉ

Chad Mariage

BIBLIOTHÈQUE DU PARLEMENT

Service d'information et de recherche parlementaires

Miguel Bernal-Castillero

Dara Lithwick

Maxime-Olivier Thibodeau

LE COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE

a l'honneur de présenter son

CINQUIÈME RAPPORT

Conformément au mandat que lui confère l'article 108(3)h) du Règlement, le Comité a étudié la vie privée et les médias sociaux et a convenu de faire rapport de ce qui suit :

TABLE DES MATIÈRES

PROTECTION DE LA VIE PRIVÉE ET MÉDIAS SOCIAUX À L'ÈRE DES MÉGADONNÉES

ÉTUDE DU COMITÉ

Le 8 mai 2012, il a été convenu que le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes (le Comité) réalise une étude des efforts faits par les entreprises de médias sociaux et des mesures prises par elles pour protéger les renseignements personnels des Canadiens, et qu'il fasse rapport de ses conclusions à la Chambre des communes[1].

Le 29 mai 2012, le Comité a tenu sa première audience sur cette question. Jennifer Stoddart, commissaire à la protection de la vie privée du Canada, s'est présentée devant lui et a donné un bref aperçu du secteur des médias sociaux, de ses activités et de son influence sur la vie privée des Canadiens. Pour reprendre ses mots :

> Les médias sociaux font appel à des applications grâce auxquelles les individus, les organisations et les collectivités peuvent échanger de l'information et produire un contenu[2].

La commissaire Stoddart a ensuite exposé les quatre préoccupations de son Commissariat, à savoir la responsabilité, le consentement valable, la limitation de l'utilisation et la conservation des données. Ces quatre points ont formé une première trame pour l'étude du Comité sur ce vaste sujet.

Entre le 29 mai et le 11 décembre 2012, le Comité a consacré 15 séances à l'étude, il a entendu une trentaine de témoins représentant le gouvernement, le milieu universitaire, des groupes d'intérêt public et le secteur privé, et il a reçu plusieurs mémoires. Au début d'octobre, il a rencontré à Washington, D.C. des fonctionnaires et des spécialistes de la protection de la vie privée des États-Unis.

LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES

La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)[3] est le principal texte de loi qui régit la protection des renseignements personnels des individus dans leurs rapports avec les entreprises de médias sociaux et d'autres organisations du secteur privé. Cette loi définit les règles de base pour la gestion des renseignements personnels dans le secteur privé et elle vise à

---

1 Chambre des communes, Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI)], *Procès-verbal*, 1re session, 41e législature, réunion no 37, 8 mai 2012.

2 ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1145 (Jennifer Stoddart, commissaire à la protection de la vie privée).

3 *Loi sur la protection des renseignements personnels et les documents électroniques*, (LPRPDE), L.C. 2000, ch. 5.

assurer un équilibre entre le droit à la protection des renseignements personnels et le besoin qu'ont les organisations de recueillir, d'utiliser et de communiquer des renseignements personnels à des fins commerciales légitimes. La LPRPDE s'applique aux organisations qui mènent des activités commerciales au Canada, à l'exception de ceux qui sont régis par des provinces ayant adopté des dispositions législatives essentiellement similaires à celles de la loi fédérale[4]. La LPRPDE protège aussi les renseignements personnels sur les employés qui œuvrent dans des secteurs assujettis à la réglementation fédérale.

Depuis le 1er janvier 2004, la LPRPDE s'applique à la collecte, à l'utilisation et à la communication de renseignements personnels dans le cadre d'activités commerciales au Canada. Elle s'applique aussi aux renseignements personnels recueillis dans le cadre de transactions commerciales interprovinciales et internationales[5]. Les entreprises qui œuvrent dans le secteur des médias sociaux sont donc assujetties à la LPRPDE.

La LPRPDE est neutre sur le plan technologique et elle repose sur le *Code canadien de protection des renseignements personnels* de l'Association canadienne de normalisation[6]. Ce code, qui a été intégré à la *Loi*, est le fruit d'un travail de collaboration entre des représentants du gouvernement, des consommateurs et des groupes d'entreprises. Il énonce 10 principes de gestion de l'information équitable, par exemple, sauf quelques exceptions, les personnes au sujet desquelles des renseignements sont recueillis, utilisés ou communiqués doivent en être informées et y consentir. De plus, les fins pour lesquelles une organisation peut recueillir, utiliser ou communiquer des renseignements personnels se limitent à celles « qu'une personne raisonnable estimerait acceptables dans les circonstances[7] ». Les renseignements personnels peuvent être utilisés uniquement aux fins pour lesquelles ils ont été recueillis et, si une organisation compte s'en servir à une autre fin, il doit obtenir le consentement des intéressés. La LPRPDE maintient l'obligation des entreprises de faire preuve de transparence en ce qui concerne leurs politiques et pratiques de gestion des renseignements personnels. Elle confère aussi aux individus le droit de consulter les renseignements personnels qui les concernent et que les organisations peuvent détenir à leur sujet, et de demander que soit corrigé tout renseignement inexact ou incomplet[8].

---

4 Jusqu'ici, l'Alberta, la Colombie-Britannique et le Québec ont adopté des lois sur la protection des renseignements personnels qui sont essentiellement similaires à la loi fédérale. Le Nouveau-Brunswick, Terre-Neuve-et-Labrador et l'Ontario ont également adopté des lois essentiellement similaires qui touchent les dépositaires des renseignements sur la santé. Mais même dans ces provinces, la LPRPDE s'applique aux organisations du secteur privé qui sont assujettis à la compétence fédérale, ainsi qu'aux renseignements personnels dans les transactions interprovinciales et internationales.

5 Commissariat à la protection de la vie privée du Canada (CPVP), *La Loi sur la protection des renseignements personnels et les documents électroniques*, Fiches d'information.

6 Norme nationale du Canada, *Code canadien de protection des renseignements personnels*, CAN/CSA-Q830-96.

7 LPRPDE, art. 4.

8 Pour plus de renseignements sur les principes, voir CPVP, *Se conformer à la* Loi sur la protection des renseignements personnels et les documents électroniques, Fiches d'information, et Nancy Holmes, *Les lois fédérales du Canada sur la protection de la vie privée*, publication n° PRB 07-44F, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, Ottawa, 25 septembre 2008.

PRÉOCCUPATIONS CONCERNANT LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES MÉDIAS SOCIAUX

Des témoins ont expliqué au Comité comment les médias sociaux avaient suscité un changement dans la façon qu'ont les individus et les organisations de percevoir et de protéger les renseignements personnels. Définis dans la LPRPDE comme étant des renseignements concernant un individu identifiable[9], les renseignements personnels sont devenus des données utiles et quantifiables — faciles à recueillir, traiter et utiliser pour des fins nouvelles, différentes et en constante évolution. C'est pour cette raison qu'on en est venus à se demander comment les médias sociaux traitent les renseignements personnels et quelles mesures ils prennent pour respecter les lois canadiennes concernant la protection de la vie privée.

A. Évolution des pratiques des individus et des entreprises de médias sociaux

> *Nous sommes à l'ère des mégadonnées, et les renseignements personnels sont devenus une monnaie d'échange utilisée librement au Canada et ailleurs dans le monde*[10].
>
> *- Jennifer Stoddart, commissaire à la protection de la vie privée du Canada*

Un premier aspect de la question de la vie privée et des médias sociaux est que les gens transmettent volontiers leurs renseignements personnels sur les sites des médias sociaux et ne comprennent peut-être pas pleinement l'utilisation qui en est faite ou les risques s'y rattachant[11]. Normand Landry, professeur à la TÉLUQ, a relevé six risques et pièges associés à la communication de renseignements personnels dans les médias sociaux, dont certains touchent en particulier les personnes mineures : la perte ou l'absence d'anonymat dans les médias sociaux et le dévoilement d'informations qui étaient jugées privées ou confidentielles; le vol d'identité; les dangers et les risques liés à l'emploi; les nombreuses atteintes à l'honneur et à la réputation; la cyberintimidation; la violence psychologique et sexuelle[12].

Selon les témoins, plusieurs facteurs qui dépassent le niveau de maîtrise ou de connaissances technologiques des utilisateurs expliquent la compréhension limitée qu'ils ont. Au nombre de ces facteurs, mentionnons les intérêts et le plan d'affaires des entreprises de médias sociaux[13], une notion désuète de ce qui constitue de l'information personnelle en droit canadien[14] et l'absence d'un cadre juridique clair qui procure aux

---

9 LPRPDE, art. 2.

10 ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1145 (Jennifer Stoddart, commissaire à la protection de la vie privée).

11 ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1225 (Janet Goulding, Industrie Canada).

12 ETHI, *Témoignages*, 1re session, 41e législature, 20 novembre 2012, 1550 (Normand Landry, TÉLUQ).

13 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1120 (Valerie Steeves, Université d'Ottawa).

14 ETHI, *Témoignages*, 1re session, 41e législature, 1er novembre 2012, 1640 (Colin Bennett, Université de Victoria).

utilisateurs des médias sociaux un ensemble de normes pour la protection des renseignements personnels[15].

Par exemple, les entreprises de médias sociaux recueillent des données produites par les utilisateurs et elles les utilisent ou les communiquent de différentes façons qui ne sont peut-être pas claires pour les utilisateurs. La commissaire Stoddart a signalé :

> En un tour de main, les entreprises de médias sociaux parviennent à réunir une quantité astronomique de renseignements personnels. En plus des préférences, des habitudes et des interactions sociales des utilisateurs, elles recueillent une foule de renseignements de base qui ne figurent pas dans le profil public, notamment l'historique des recherches, les achats effectués, les sites Web consultés et le contenu des messages privés. En recueillant ces milliards de points de données, les entreprises de médias sociaux peuvent analyser le comportement des utilisateurs au moyen d'algorithmes évolués dans le but de personnaliser leurs services et de trouver des façons de générer des revenus. Elles permettent aussi à d'autres, par exemple, des chercheurs, des employeurs, des administrateurs scolaires et des organismes d'application de la loi, d'en savoir plus sur les individus et leurs activités[16].

Teresa Scassa, professeure à l'Université d'Ottawa, ajoute que les entreprises de médias sociaux jouent un rôle central « dans la cueillette ou dans la facilitation de la cueillette de grandes quantités de renseignements à notre sujet dans le but de suivre nos activités en ligne, nos habitudes de consommation et même nos déplacements[17] ». Normand Landry, professeur à la TÉLUQ, fait la mise en garde suivante : « Le risque est qu'avec les nouvelles techniques de croisement des données, on peut, à partir d'un individu, retracer l'intégralité de sa vie privée en multipliant les enquêtes qui sont faites sur les sites de médias sociaux que cet utilisateur fréquente. Le danger est là et ce problème est croissant[18]. »

Colin McKay, gestionnaire responsable des politiques chez Google Canada, a dit au Comité que l'information utilisée par les entreprises de médias sociaux ne concerne pas nécessairement les gens; l'information est rendue anonyme et remaniée de façon qu'il ne soit plus possible de la relier à une personne. L'information anonymisée est utile aux entreprises comme Google, qui s'en servent pour créer de nouveaux produits et de nouveaux outils[19].

Plusieurs témoins ont attiré l'attention du Comité sur le fait que les changements dans la façon dont les entreprises de médias sociaux utilisent l'information sont ce qui alimente le monde numérique moderne. Les réseaux de médias sociaux contribuent à imbriquer davantage la vie sociale, politique, culturelle et économique des Canadiens;

---

15 ETHI, *Témoignages*, 1re session, 41e législature, 20 novembre 2012, 1540 (Normand Landry, TÉLUQ).

16 ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1145 (Jennifer Stoddart, commissaire à la protection de la vie privée).

17 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1100 (Teresa Scassa, Université d'Ottawa).

18 ETHI, *Témoignages*, 1re session, 41e législature, 20 novembre 2012, 1550 (Normand Landry, TÉLUQ).

19 ETHI, *Témoignages*, 1re session, 41e législature, 30 octobre 2012, 1625 (Colin McKay, Google Canada). Pour plus de renseignements sur Google, voir les témoignages concernant spécifiquement certaines entreprises privées, dans le présent rapport.

l'échange d'information facilite l'échange démocratique d'idées et la création de possibilités économiques pour les Canadiens et les entreprises canadiennes[20]. Warren Everson, vice-président principal, Politique, Chambre de commerce du Canada, a indiqué :

> Les médias sociaux connaissent à présent une expansion tout à fait dramatique. Grâce à ces derniers, des millions de dollars sont investis dans l'économie numérique du Canada, ce qui crée des milliers d'emplois au Canada. Ces emplois peuvent être de très bonne qualité et bien rémunérés[21].

B. Équilibre entre innovation et réglementation

> *Les Canadiens ne devraient pas avoir à choisir entre leur droit à la vie privée et leur droit de participer à ce nouvel environnement interactif*[22].
>
> *- Tamir Israel, Clinique d'intérêt public et politique d'Internet du Canada*

De nombreux témoins ont parlé de la nécessité d'établir un équilibre entre, d'une part, le désir des entreprises de médias sociaux d'innover et de mettre à l'essai de nouveaux produits et services et, d'autre part, le juste niveau de protection des renseignements personnels des Canadiens.

Certes, des témoins représentant le milieu universitaire et le secteur privé ont laissé entendre qu'il fallait adopter des politiques stimulant le développement du commerce électronique et des médias sociaux au Canada, afin d'« apposer un sceau résolument canadien[23] » et de faire du « Canada […] une destination qui permet la croissance et la prospérité des entreprises[24] ». D'autres témoins, qui représentaient principalement des organismes de règlementation, des universités et des groupes d'intérêt public, soutenaient qu'il ne faisait aucun doute que « le gouvernement et les organismes de réglementation ont un rôle à jouer pour établir des paramètres sur ce qui est acceptable et pour s'assurer que ceux-ci tiennent compte des valeurs chères aux Canadiens sur le plan de la protection des renseignements personnels et de la sécurité[25] ». D'autres témoins représentant surtout des associations de l'industrie et des entreprises privées reconnaissaient le besoin de protéger les renseignements personnels, mais privilégiaient la formule de l'autoréglementation. David Elder, de l'Association canadienne du marketing (ACM), a mentionné que « [l]es entreprises légitimes ont en effet tout intérêt à anticiper les besoins des consommateurs à l'égard de la protection des renseignements personnels et

---

20 ETHI, Mémoire présenté par la Freedom of Information and Privacy Association de la Colombie-Britannique, *Médias sociaux, données volumineuses et respect de la vie privée : Protéger les droits des citoyens à l'ère de l'interconnectivité*, 1re session, 41e législature, 13 décembre 2012, p. 8.

21 ETHI, *Témoignages*, 1re session, 41e législature, 5 juin 2012, 1100 (Warren Everson, Chambre de commerce du Canada).

22 ETHI, *Témoignages*, 1re session, 41e législature, 19 juin 2012, 1110 (Tamir Israel, CIPPIC).

23 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1110 (Michael Geist, Université d'Ottawa).

24 ETHI, *Témoignages*, 1re session, 41e législature, 20 novembre 2012, 1535 (Karna Gupta, Association canadienne de la technologie de l'information (ACTI)).

25 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1150 (Michael Geist, Université d'Ottawa).

à résoudre toute situation problématique, indépendamment des exigences ou des sanctions juridiques[26] ».

Cette préférence pour une approche fondée sur l'autoréglementation, par opposition à des obligations imposées par la loi, a été exprimée par plusieurs témoins qui considèrent qu'il est plus facile de l'adapter aux conditions qui évoluent rapidement. Vincent Gautrais, professeur à l'Université de Montréal, a indiqué :

> C'est la raison pour laquelle cette notion d'imputabilité ne devrait pas être introduite par une loi, mais plutôt par des normes de pratique informelles, des codes de conduite. Avec une approche plus négociée, il n'y aurait pas de loi imposant des choses dans un délai généralement assez court et on favoriserait le dialogue pour élaborer des normes de pratique[27].

À titre d'exemple de secteur autoréglementé, il y a celui que représente l'ACM, qui a expliqué au Comité qu'elle avait publié à l'intention de ses membres des lignes directrices sur la façon de fournir aux consommateurs des explications claires et faciles à comprendre.

> [L]es lignes directrices exigent que les agents de marketing utilisant la publicité en ligne fondée sur les intérêts s'assurent qu'eux-mêmes et les canaux publicitaires et les éditeurs de sites Web qu'ils utilisent pour afficher ces annonces en leur nom offrent des informations claires pour expliquer comment sont recueillis et utilisés les renseignements envoyés lors de la navigation, et qu'ils offrent une façon simple d'attirer l'attention des consommateurs vers cette information[28].

Pour sa part, la commissaire à la protection de la vie privée s'est dite préoccupée par le fait que les entreprises de médias sociaux font apparemment fi des mesures législatives du Canada en matière de protection des renseignements personnels, un problème qui s'accentue à mesure que les entreprises se développent et qu'elles deviennent moins enclines à faire preuve d'une transparence complète envers les autorités de réglementation[29].

> Selon moi, l'émergence de géants Internet menace l'équilibre recherché par l'esprit et la lettre de la LPRPDE. Le quasi-monopole exercé par ces multinationales a rendu inefficace, selon moi, l'approche toute en douceur de la LPRPDE, qui repose sur des recommandations non contraignantes et sur une menace de ternir la réputation. Nous avons vu des organisations ignorer nos recommandations jusqu'à ce que la Cour soit saisie de l'affaire, et nous avons vu de grandes entreprises, au nom d'une consultation avec le Commissariat, s'engager à mettre en place des mesures répondant à nos préoccupations pour ensuite ignorer nos conseils. Par ailleurs, compte tenu des vastes quantités de renseignements personnels détenus par les organisations sur des

---

26 ETHI, *Témoignages*, 1re session, 41e législature, 16 octobre 2012, 1545 (David Elder, ACM).

27 ETHI, *Témoignages*, 1re session, 41e législature, 12 juin 2012, 1230 (Vincent Gautrais, Université de Montréal).

28 ETHI, *Témoignages*, 1re session, 41e législature, 16 octobre 2012, 1545 (David Elder, ACM).

29 ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1145 et 1155 (Jennifer Stoddart, commissaire à la protection de la vie privée). Elizabeth Denham, commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, partageait également ce point de vue : ETHI, *Témoignages*, 1re session, 41e législature, 7 juin 2012, 1135.

> plateformes de plus en plus complexes, le risque lié à des atteintes importantes et à des utilisations inattendues, non souhaitées, voire envahissantes, de ces renseignements exige la mise en place de mesures de sécurité et de conséquences financières adaptées qui ne sont pas actuellement prévues par la LPRPDE[30].

Selon les témoins, les entreprises de médias sociaux n'ont pas encore établi de normes d'autoréglementation. Les témoins s'accordaient cependant à dire que les médias sociaux formaient un secteur nouveau, évoluant rapidement, un secteur confronté aux limites de la vie privée et se devant de garantir la vie privée pour susciter la confiance des consommateurs. Alan Chapell, qui est conseiller juridique externe et responsable de la protection de la vie privée chez BlueKai inc., une entreprise de gestion de données, a fait observer :

> [L]es entreprises de médias sociaux contribuent à une culture de la protection de la vie privée en évolution […]
>
> Tant d'un point de vue législatif que réglementaire, il est difficile de définir l'équilibre qu'il faut trouver entre étouffer l'innovation et protéger la vie privée des consommateurs[31].

Le Comité a également appris que, même si les Canadiens utilisent activement les médias sociaux, ils ne représentent qu'une partie des intérêts commerciaux des grandes entreprises de médias sociaux. Par conséquent, bon nombre des politiques de ces entreprises concernant la vie privée sont rédigées selon des modèles législatifs différents de la LPRPDE, qui mettent l'accent non pas sur les renseignements personnels, mais sur les informations personnellement identifiables[32]. Selon John Lawford, du Centre pour la défense de l'intérêt public (CDIP) :

> [L]es grands réseaux sociaux définissent les « renseignements personnels » d'une façon qui prête à confusion, et aucune des définitions ne correspond à celle prévue dans la *Loi sur la protection des renseignements personnels et les documents électroniques* [LPRPDE] […]
>
> Cette non-définition de renseignements personnels est importante, car les utilisateurs qui lisent une politique en la matière ne sont pas en mesure de comprendre véritablement leurs droits en vertu de la [LPRPDE] afin de déposer une plainte, d'exiger le respect de la *Loi* ou même de contacter la société[33].

Le CDIP a présenté au Comité un tableau (annexe A du présent rapport) qui compare la définition de « renseignement personnel » donnée dans la LPRPDE et les définitions qui se trouvent dans les conditions et politiques de confidentialité de plusieurs médias sociaux[34]. Ce tableau met en lumière les différences fondamentales qui existent

---

30 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1615 (Jennifer Stoddart, commissaire à la protection de la vie privée).

31 *Ibid.*, 1655 (Alan Chapell, BlueKai). Pour plus de renseignements sur Bluekai, le lecteur pourra se reporter aux témoignages concernant spécifiquement certaines entreprises privées, dans le présent rapport.

32 ETHI, *Témoignages*, 1re session, 41e législature, 18 octobre 2012, 1620 (John Lawford, CDIP).

33 *Ibid.*, 1535.

34 ETHI, Document présenté par le Centre pour la défense de l'intérêt public, *Comparaison des définitions dans les conditions et politiques de confidentialité des médias sociaux*, 18 octobre 2012.

entre ce que prévoit la loi canadienne et ce que font les entreprises de médias sociaux. Dans son témoignage, M. Lawford a laissé entendre qu'il faudrait que les organisations, dans leurs contrats d'utilisation, définissent les « renseignements personnels » en des termes compatibles avec la définition qu'en donne la LPRPDE[35].

Dans le mémoire qu'il a présenté au Comité au sujet de cette étude, Christopher Parsons, candidat au doctorat à l'Université Victoria et collaborateur à un projet visant à déterminer comment les entreprises de réseautage social se conforment aux aspects des lois canadiennes sur la protection des renseignements personnels, a mentionné au Comité que les lois américaines sont des « lois prééminentes » auxquelles les réseaux sociaux acceptent de se conformer et que certaines grandes entreprises de réseautage social hésitent à appliquer des lois canadiennes (ou européennes) sur la protection des données parce que ces lois « pourraient entraver ou empêcher l'utilisation de pratiques auxquelles elles recourent actuellement à des fins lucratives[36] ».

Ayant pris connaissance de ces témoignages, le Comité est préoccupé du fait que les grandes entreprises de médias sociaux préfèrent être régies par d'autres lois que celles du Canada bien qu'elles y exercent des activités. Les raisons à cela sont peut-être de nature économique, linguistique ou commerciale, mais il importe que les Canadiens qui utilisent les services de ces entreprises soient protégés par leurs propres lois et valeurs. Cela vaut tout particulièrement pour la façon dont les « renseignements personnels » sont maintenant définis au Canada, tant sur le plan juridique que dans la pratique.

C. Changements touchant la collecte, l'utilisation et la communication de l'information

> *Les lois sur la protection des renseignements personnels s'appuient toujours sur des renseignements personnels. En réalité, je crois qu'on perd la notion de ce concept, de ce qu'est un renseignement personnel. On reconnaît que c'est le nom, l'adresse, et d'autres renseignements qu'on peut donner à quelqu'un. Mais de plus en plus, un renseignement personnel, c'est un renseignement qui porte sur toutes nos activités, sur tout ce qu'on fait sur Internet et même dans d'autres contextes[37].*
>
> *- Teresa Scassa, professeure à l'Université d'Ottawa*

Des témoins ont laissé entendre que ces dernières années, avec la création des réseaux de médias sociaux, les renseignements personnels sont recueillis, utilisés et communiqués de façons différentes. Alors que jadis ces renseignements étaient recueillis pour des transactions, ils représentent maintenant un bien de valeur en soi. De l'avis de M[me] Scassa, le fait que les renseignements personnels soient maintenant considérés comme des données utiles ayant valeur de transaction

---

35 ETHI, *Témoignages*, 1re session, 41e législature, 18 octobre 2012, 1550 (John Lawford, CDIP).

36 ETHI, Mémoire présenté par Christopher Parsons, « Réseautage social et droit canadien en matière de protection des renseignements personnels — Compétence, conservation et divulgation », 1re session, 41e législature, 23 décembre 2012, p. 3. [traduction]

37 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1210 (Teresa Scassa, Université d'Ottawa).

> […] risque d'éviscérer le modèle de consentement sur lequel la loi est fondée. Ce nouveau paradigme mérite une attention particulière et pourrait nécessiter des normes et des approches juridiques différentes.
>
> […]
>
> Ces renseignements sont utilisés pour établir notre profil, afin de définir nos habitudes de consommation, de déterminer si nous nous qualifions pour des assurances ou d'autres services, ou d'exercer une discrimination fondée sur le prix lors de la livraison de marchandises ou de services. Nous devenons des personnes concernées dans tous les sens du terme. Il existe peu de transactions ou d'activités qui ne laissent pas de traces sous forme de données[38].

Outre la transformation des renseignements personnels en données, les nouvelles technologies facilitent la manipulation de l'information et son utilisation dans des contextes différents de ceux dans lesquels elle a été présentée de même que sur des supports différents. Par conséquent, les entreprises peuvent plus facilement recueillir, utiliser et communiquer des renseignements personnels, et les gens n'ont plus la haute main sur les renseignements qui les concernent et doivent maintenant se montrer prudents quand vient le temps de communiquer des renseignements. Adam Kardash, directeur général d'Access Privacy au bureau d'avocats Heenan Blaikie, a fait observer qu'« en tant qu'individus, nous avons tous la responsabilité de faire attention à la manière dont nous utilisons nos renseignements personnels dans des contextes publics[39] ».

Dans cette optique, des témoins ont souligné que l'utilisation de renseignements personnels comme données facilite l'agrégation de données et crée des occasions de monétiser les renseignements personnels des utilisateurs. Tamir Israel, de la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC), a indiqué : « Toutes ces données sont recueillies, analysées et transformées en un schéma élaboré de classification socioéconomique[40] ». Selon Ian Kerr, professeur à l'Université d'Ottawa, le résultat est que :

> [C]es entreprises de réseaux sociaux et de renseignements et d'autres courtiers en information collaboreront avec qui ils veulent pour établir des ententes lucratives, dont l'objectif est d'établir des liens entre ces éléments d'information afin de créer certains types de profils sur nous leur permettant de nous classer dans des catégories à des fins qui nous avantagent, etc.[41]

Au dire de certains témoins, cela signifie que les services de médias sociaux ne sont pas gratuits; il s'agit plutôt d'un moyen de commercialiser l'accès aux utilisateurs et aux renseignements qui les concernent. Comme l'a fait remarquer Jason Zushman, du

---

38 *Ibid.*, 1105.

39 ETHI, *Témoignages*, 1re session, 41e législature, 19 juin 2012, 1130 (Adam Kardash, Heenan Blaikie).

40 *Ibid.*, 1110 (Tamir Israel, CIPPIC).

41 ETHI, *Témoignages*, 1re session, 41e législature, 12 juin 2012, 1235 (Ian Kerr, Université d'Ottawa).

Merchant Law Group, « l'archivage et le suivi des informations qui sont fournies par les utilisateurs est ce qui donne un avantage financier aux entreprises[42] ».

Colin McKay a reconnu également que l'« énorme quantité d'information qui ne se compose pas de données de l'utilisateur » est « extrêmement précieuse » pour Google en raison des différentes utilisations possibles de ces données, notamment pour promouvoir des pratiques de navigation plus sûres[43]. Pour sa part, Alan Chapell, de BlueKai, a expliqué que l'utilisation de renseignements personnels pour de la publicité ciblée « finance une bonne partie du contenu [en ligne] que les consommateurs consultent gratuitement[44] ». Robert Sherman, directeur, Protection des renseignements personnels et politiques publiques de Facebook, abondait dans ce sens : selon lui, le modèle de gestion de l'entreprise de média social consiste « à offrir l'utilisation de Facebook gratuitement à quiconque veut s'en servir. En échange, nous faisons de la publicité sur Facebook[45] ».

À l'appui de cette pratique, Brendan Wycks, de l'ARIM, une association sans but lucratif qui représente l'industrie de recherche et d'intelligence marketing, a indiqué au Comité : « [L]es praticiens légitimes de la recherche par les médias sociaux s'efforcent toujours de respecter les règles des sites sociaux que nous surveillons, de respecter les vœux de ceux qui diffusent des renseignements personnels en ligne et d'anonymiser les renseignements personnels contenus dans les données que nous recueillons; de plus, nous n'essayons jamais de vendre quoi que ce soit ou de faire de la sollicitation sous quelque forme que ce soit[46] ».

Or, plusieurs témoins, dont Ian Kerr et Teresa Scassa, ont dénoncé le profilage résultant de l'agrégation de données, c'est-à-dire le fait de placer les utilisateurs, avec exactitude ou non, dans des « catégories sociales […] sur la base du traitement de l'information[47] ». M[me] Scassa a indiqué à ce propos :

> On nous dit que le profilage est une bonne chose, car cela signifie que nous ne serons pas bombardés d'annonces publicitaires faisant la promotion de produits ou de services qui nous laissent indifférents. Pourtant, l'autre côté de la médaille, c'est que le profilage peut être utilisé pour déterminer que des personnes ne sont pas admissibles à des rabais ou à des prix promotionnels, qu'elles ne se qualifient pas pour du crédit ou des assurances, ou qu'il est sans intérêt de les viser par le marketing d'un type particulier de produits et de services. Le profilage peut exclure certaines personnes et en privilégier d'autres, et c'est ce qui va se produire[48].

---

42 ETHI, *Témoignages*, 1re session, 41e législature, 16 octobre 2012, 1645 (Jason Zushman, Merchant Law Group).

43 ETHI, *Témoignages*, 1re session, 41e législature, 30 octobre 2012, 1555 (Colin McKay, Google Canada).

44 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1550 (Alan Chapell, BlueKai).

45 ETHI, *Témoignages*, 1re session, 41e législature, 27 novembre 2012, 1550 (Robert Sherman, Facebook). Pour plus de renseignements sur Facebook, voir les témoignages concernant spécifiquement certaines entreprises privées, dans le présent rapport.

46 ETHI, *Témoignages*, 1re session, 41e législature, 5 juin 2012, 1115 (Brendan Wycks, ARIM).

47 ETHI, *Témoignages*, 1re session, 41e législature, 12 juin 2012, 1235 (Ian Kerr, Université d'Ottawa).

48 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1105 (Teresa Scassa, Université d'Ottawa).

La commissaire Stoddart a ajouté pour sa part :

> Le fait que cette pratique déterminera l'information ou les publicités qui vous seront présentées et parfois, le classement dans les moteurs de recherche — mais je n'en suis pas certaine — signifie que l'expérience et l'étendue des connaissances que l'on a sur Internet seront limitées. Elles dépendront d'un profil qui peut être juste, erroné ou approximatif que des algorithmes vous attribuent[49].

Dans son témoignage, la commissaire Stoddart a attiré l'attention du Comité sur un récent article de Jeffrey Rosen, professeur à l'Université George Washington, qui explique les effets du profilage sur les consommateurs[50]. Dans cet article, M. Rosen explique comment les entreprises telles Google, Facebook et BlueKai recueillent des données sur les interactions sur le Web (participation à des réseaux sociaux, recherches dans Internet et magasinage en ligne) pour créer des profils de consommateur. Ces profils servent ensuite à classer les gens dans des catégories selon leurs intérêts et leur pouvoir d'achat, et ils sont ensuite vendus à des annonceurs en ligne à l'occasion d'enchères en temps réel. Les gens ne sont plus des consommateurs, mais un produit vendu à des annonceurs à différents prix. Le danger est que ces « profils qui nous définissent pour toujours peuvent également servir à des fins de classification et d'exclusion […] Contrairement à une situation de marché où les gens marchandent avec des vendeurs sur un même pied, il est difficile d'échapper à votre profil de consommateurs dans le nouveau monde de la discrimination par les prix, et vous ne saurez jamais si les entreprises offrent en tout premier lieu des rabais à des consommateurs d'un rang supérieur[51] ».

Se fondant sur des recherches qu'il a effectuées, M. Normand Landry a relevé quatre dimensions qui se rattachent au droit à la vie privée et neuf critères applicables à la protection des renseignements personnels. Ces dimensions sont : le droit à l'anonymat, l'absence de surveillance, la préservation d'un espace d'intimité et l'accès à une saine gestion des renseignements personnels. Selon M. Landry, l'individu doit être en mesure de « contrôler les accès, la diffusion, le partage et l'exactitude des renseignements personnels qui sont collectés sur son compte[52] ». Pour ce qui est des critères applicables à la protection des renseignements personnels, M. Landry soutient que toute personne au sujet de laquelle des renseignements personnels sont recueillis devrait pouvoir :

> [Ê]tre correctement informée que l'on procède à une collecte, y souscrire bien volontairement et être en mesure d'identifier les acteurs procédant à cette collecte de renseignements. De plus, elle devrait pouvoir connaître les manières de collecter ces renseignements, identifier la nature de ces renseignements et connaître les usages qui vont en être faits. Une telle personne devrait également pouvoir identifier les acteurs qui peuvent avoir accès à ces renseignements et les règles qui encadrent leur confidentialité ainsi qu'évaluer si ces renseignements sont correctement protégés. Enfin, elle devrait

---

49 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1655 (Jennifer Stoddart, commissaire à la protection de la vie privée).

50 *Ibid.*

51 Jeffrey Rosen, « Who Do Online Advertisers Think You Are? », *The New York Times*, 30 novembre 2012. [traduction]

52 ETHI, *Témoignages*, 1re session, 41e législature, 20 novembre 2012, 1540 (Normand Landry, TÉLUQ).

> pouvoir accéder aux renseignements collectés ainsi que rectifier, corriger ou retirer des renseignements personnels qui ont été accumulés ailleurs[53].

L'importance du contrôle individuel n'était pas l'unique sujet de préoccupation des universitaires et des groupes d'intérêt public. Robert Sherman, de Facebook, a indiqué : « On est à l'aise pour échanger des renseignements en ligne que lorsqu'on contrôle qui verra l'information et qu'on a confiance en ceux qui la reçoivent[54] ».

D. Responsabilité et transparence

> *La cueillette ne se produit plus sous nos yeux; elle se produit en arrière-plan[55].*
>
> *- Valerie Steeves, professeure à l'Université d'Ottawa*

La responsabilité est le premier des 10 principes de gestion équitable de l'information que prévoit la LPRPDE. Suivant ce principe, il incombe à l'organisation de « désigner une ou des personnes qui devront s'assurer du respect des principes[56] ». Il s'agit du tout premier principe « parce que c'est celui en vertu duquel les organisations doivent appliquer les autres principes relatifs à l'équité dans le traitement des renseignements dont l'objectif est d'assurer la gestion appropriée et la protection des renseignements personnels des particuliers[57] ». La LPRPDE énonce également le principe de la transparence comme suit : « Une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne[58] ».

Selon la commissaire à la protection de la vie privée, la responsabilité englobe les obligations des entreprises que prévoit la loi :

> En gros, il faudrait que les entreprises décrivent toutes les mesures qu'elles prennent pour respecter la loi en matière de protection de la vie privée. Par exemple, la compagnie peut avoir un chef de la protection de la vie privée, donner de la formation à son personnel, supprimer les données après le délai requis, investir dans la protection des données personnelles, montrer qu'elle applique la procédure appropriée pour répondre aux demandes présentées en vertu de la loi, etc.[59]

Des témoins ont mentionné que le modèle de responsabilité actuel que prévoit la LPRPDE a bonne presse sur la scène internationale, notamment parce qu'il est neutre sur le plan technologique et pour l'industrie, et aussi parce qu'il promeut l'autoréglementation

---

53 *Ibid.*,

54 ETHI, *Témoignages*, 1re session, 41e législature, 27 novembre 2012, 1530 (Robert Sherman, Facebook).

55 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1120 (Valerie Steeves, Université d'Ottawa).

56 LPRPDE, annexe 1, art. 4.1.

57 ETHI, Document présenté par le Commissariat à la protection de la vie privée du Canada, par les Commissariats à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique, *Un programme de gestion de la protection de la vie privée : la clé de la responsabilité*, p. 3.

58 LPRPDE, annexe 1, art. 4.8.

59 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1650 (Jennifer Stoddart, commissaire à la protection de la vie privée).

par les associations industrielles. Adam Kardash de Heenan Blaikie a mentionné que la LPRPDE « permet […] de bien régler les problèmes en matière de protection de la vie privée susceptibles de surgir dans le monde virtuel ou, encore, dans le contexte technologique[60] ».

Le Commissariat à la protection de la vie privée du Canada (CPVP) et les commissariats à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique ont soumis ensemble au Comité un mémoire élaboré à l'intention des organisations visées par leurs lois respectives en matière de protection des renseignements personnels dans le secteur privé. Ce document fournit une ligne directrice sur la notion d'organisation responsable et définit les attentes des commissariats quant à un programme de gestion de la protection de la vie privée[61].

David Elder, représentant de l'ACM, a indiqué que le Code de déontologie et normes de pratique de l'Association est un modèle qui montre de quelle façon l'autoréglementation peut promouvoir la responsabilité à l'intérieur d'un secteur[62]. Il a ajouté que le Code, qui reflète les 10 principes énoncés dans la LPRPDE, « vise à permettre aux consommateurs de garder mainmise sur leurs renseignements personnels, ainsi qu'à favoriser la transparence du processus de collecte et d'utilisation des données des clients par les spécialistes du marketing[63] ».

Plusieurs témoins ont cependant signalé que des problèmes de responsabilité surgissent quand il y a un manque de transparence de la part des entreprises et dans des circonstances où le modèle d'autoréglementation ne fonctionne pas[64]. La commissaire à la protection de la vie privée a fait observer que cela vaut en particulier dans le monde des médias sociaux qui « est en constante évolution. On voit pointer à tout moment de nouvelles entités pressées de lancer sur le marché un service inédit. La protection de la vie privée ne semble pas être une priorité à leurs yeux[65] ».

Jusqu'ici, les entreprises de médias sociaux n'ont pas établi de normes relatives à la responsabilité ou à la transparence, d'où la remarque de M. Kerr qu'« il faut améliorer la transparence, non seulement pour la collecte de renseignements personnels, mais aussi la façon dont ils sont utilisés et à qui ils sont divulgués. Cela doit s'appliquer à tous les aspects des transactions des médias sociaux[66] ».

---

60 ETHI, *Témoignages*, 1re session, 41e législature, 19 juin 2012, 1120 (Adam Kardash, Heenan Blaikie).

61 ETHI, Document soumis par le Commissariat à la protection de la vie privée du Canada et les Commissariats à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique, « Un programme de gestion de la protection de la vie privée : la clé de la responsabilité ».

62 Le *Code de déontologie et normes de pratique* de l'ACM est disponible à l'adresse : http://online.the-cma.org/french/?WCE=C=47|K=225885.

63 ETHI, *Témoignages*, 1re session, 41e législature, 16 octobre 2012, 1540 (David Elder, ACM).

64 Voir, par exemple, ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1225 (Michael Geist, Université d'Ottawa).

65 ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1145 (Jennifer Stoddart, commissaire à la protection de la vie privée).

66 ETHI, *Témoignages*, 1re session, 41e législature, 12 juin 2012, 1205 (Ian Kerr, Université d'Ottawa).

De l'avis de la commissaire à la protection de la vie privée, « l'autoréglementation, c'est bien », mais « il faut une loi pour l'appuyer[67] ». M. Kerr est également en faveur de l'établissement de normes minimales par voie législative :

> [l]l ne s'agit pas seulement de modifier légèrement les politiques sur la protection de la vie privée ou d'adopter des dispositions relatives aux avis plus claires. Il s'agit d'adopter des mesures législatives sur ce que j'appellerais des normes minimales obligatoires pour la transparence en matière de protection de la vie privée, ce qui requiert leur intégration dans les technologies et les techniques sociales. Nous ne vendons pas des voitures sans indicateur de vitesse, compteur kilométrique, jauge à essence ou indicateur de pression. De même, nos médias sociaux devraient comprendre des mécanismes de rétroaction qui nous permettraient d'y voir de plus près et qui nous avertiraient lorsque nous ne serions plus en sécurité[68].

Les témoignages présentés au Comité montrent à quel point les entreprises de médias sociaux doivent se montrer plus responsables et faire preuve d'une plus grande transparence. Les pratiques actuelles ne permettent pas de croire que les principes énoncés dans la LPRPDE sont pleinement appliqués.

Recommandation 1

Le Comité recommande que la commissaire à la protection de la vie privée du Canada établisse des lignes directrices à l'intention des entreprises de médias sociaux et de gestion de données pour les aider à développer des pratiques qui respectent entièrement la LPRPDE, particulièrement la responsabilité et la transparence.

67 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1715 (Jennifer Stoddart, commissaire à la protection de la vie privée).

68 ETHI, *Témoignages*, 1re session, 41e législature, 12 juin 2012, 1205 (Ian Kerr, Université d'Ottawa).

E. Obtenir le consentement dans les contrats et les ententes avec les médias sociaux

> *Les entreprises de médias sociaux doivent expliquer clairement à quelles fins elles recueillent, utilisent et divulguent des renseignements personnels et préciser quels tiers — par exemple, les développeurs d'applications — y ont accès. Et elles doivent obtenir un consentement sans équivoque des utilisateurs*[69].
>
> *- Jennifer Stoddart, commissaire à la protection de la vie privée du Canada*

Une représentante d'Industrie Canada a expliqué au Comité que la législation canadienne en matière de protection de la vie privée est fondée « sur le principe du consentement, qu'il soit explicite ou implicite, de recueillir, d'utiliser et de communiquer des renseignements personnels[70] ». En fait, le principe 3 de la LPRPDE précise que « [t]oute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir[71] ». Ce principe oblige également les organisations « à faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés » de même qu'à adapter la forme du consentement à « la sensibilité des renseignements[72] » demandés.

Des témoins ont signalé que les formulaires de consentement ne sont pas placés ou rédigés de manière accessible aux consommateurs. Ceux-ci ne lisent peut-être pas les accords et ne savent donc pas à quoi ils consentent. Selon Vincent Gautrais,

> [u]n usager moyen des médias sociaux devrait passer 20 heures par mois pour lire les politiques concernant la vie privée qui s'appliquent à Google et à tous les sites qu'il visite. C'est infaisable. Dire que la protection passe par l'information et par le consentement est un leurre[73].

Plusieurs témoins ont fait allusion au problème du langage obscur ou inaccessible dans les formulaires de consentement, lesquels sont peu utiles et créent des attentes irréalistes à l'égard des utilisateurs. Michael Geist, professeur à l'Université d'Ottawa, a affirmé :

> Même s'ils étaient mieux rédigés, il n'est pas réaliste de croire que les gens s'arrêteront chaque fois pour lire une politique de confidentialité avant de s'inscrire dans un site Web, vu le nombre de sites qu'une personne peut visiter et avec lesquels elle peut réagir et vu la tendance vers les environnements mobiles et sans fil[74].

---

69 ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1150 (Jennifer Stoddart, commissaire à la protection de la vie privée).

70 *Ibid.*, 1220 (Janet Goulding, Industrie Canada).

71 LPRPDE, annexe 1, art. 4.3.

72 LPRPDE, annexe 1, art. 4.3.2 et 4.3.4.

73 ETHI, *Témoignages*, 1re session, 41e législature, 12 juin 2012, 1230 (Vincent Gautrais, Université de Montréal).

74 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1140 (Michael Geist, Université d'Ottawa).

M[me] Scassa a ajouté à ce propos que les formulaires de consentement sont rédigés de telle sorte qu'ils portent sur des points qui dépassent les mesures de protection prévues dans les lois sur la protection de la vie privée[75]. À l'heure actuelle, ces formulaires, également appelés contrats de licence de l'utilisateur final, sont des contrats de consommation ou conventions d'adhésion. Les utilisateurs devraient donc bénéficier des mesures de protection et des garanties que prévoient les lois sur la concurrence et la protection des consommateurs. Ces mesures de protection favoriseraient, par exemple, l'éthique publicitaire et comprendraient d'autres mesures visant à protéger les faibles ainsi que les personnes ne pouvant prendre soin d'elles-mêmes.

M. Landry a fait remarquer que le langage utilisé dans ces accords ayant force obligatoire « fait en sorte qu'il est très difficile pour les utilisateurs de savoir précisément dans quelle mesure et en fonction de quels paramètres leurs renseignements personnels sont protégés[76] ». Pierrot Péladeau, chercheur et consultant, a signalé qu'en règle générale, les textes des contrats « ne sont pas des moyens appropriés pour expliquer les processus[77] » de collecte, d'utilisation et de communication de renseignements personnels. Ces préoccupations montrent bien que le consentement donné n'est pas forcément valable ou informé.

Colin McKay, de Google Canada, a admis que les entreprises sont au fait du problème des conventions longues et complexes. Il a fait observer que Google s'affaire à déterminer quelles seraient les modalités qui aideraient les utilisateurs à prendre les décisions appropriées au sujet de leurs données. C'est ainsi, a-t-il dit, que Google a récemment dévoilé des changements apportés à sa politique de confidentialité, prenant ce qui était un document « très long et complexe » pour le décomposer en « plusieurs éléments très simples pour que les utilisateurs comprennent vraiment comment nous demandons de l'information et à quelle fin nous l'utilisons[78] ». M. McKay a ajouté : « Nous sommes très précis au sujet des renseignements que nous recueillons auprès des utilisateurs et des raisons pour lesquelles nous le faisons[79] ».

Robert Sherman, représentant de Facebook, a indiqué au Comité que l'entreprise a récemment modifié sa « politique d'utilisation des données » — auparavant appelée politique de protection de la vie privée — parce qu'elle reconnaît qu'« il est parfois difficile de comprendre comment l'information est utilisée lorsque les politiques de respect de la vie privée sont longues et complexes » et qu'elle souhaite également « fournir des renseignements précis et concrets sur les pratiques de gestion des données[80] ». M. Sherman a ajouté que la nouvelle politique est rédigée en « langage clair » de façon qu'« elle soit à la fois facile à comprendre et exhaustive » et qu'elle comprend un « guide

---

75 *Ibid.*, 1105 (Teresa Scassa, Université d'Ottawa).

76 ETHI, *Témoignages*, 1re session, 41e législature, 20 novembre 2012, 1545 (Normand Landry, TÉLUQ).

77 ETHI, *Témoignages*, 1re session, 41e législature, 16 octobre 2012, 1530 (Pierrot Péladeau, chercheur et consultant en évaluation sociale de systèmes d'information).

78 ETHI, *Témoignages*, 1re session, 41e législature, 30 octobre 2012, 1600 (Colin McKay, Google Canada).

79 *Ibid*., 1625.

80 ETHI, *Témoignages*, 1re session, 41e législature 27 novembre 2012, 1530 (Robert Sherman, Facebook).

simple de la protection de la vie privée sur Facebook[81] ». Et si Facebook ne permet pas aux utilisateurs d'accepter seulement certaines parties de la politique et pas d'autres, c'est qu'il serait inefficient de « négocier différentes versions de Facebook pour les différents utilisateurs[82] ».

Plusieurs témoins, dont Ian Kerr, professeur à l'Université d'Ottawa, et John Lawford, du CDIP, ont également mis en garde contre l'utilisation de formulaires types qui placent les utilisateurs dans une situation vulnérable. M. Kerr a dit au Comité que :

> La plus grande menace à la vie privée, c'est le contrat type. Dans le cadre des dispositions actuelles sur la vie privée, presque toutes les mesures de protection prévues peuvent être contournées facilement par n'importe quel fournisseur de biens et de services au moyen d'un contrat type. En exigeant de l'utilisateur qu'il clique sur « j'accepte les conditions », les entreprises peuvent utiliser le droit contractuel pour esquiver leurs obligations en matière de protection de la vie privée. Bref, c'est fondé sur une mauvaise conception de la question du consentement[83].

M. Lawford, quant à lui, a ajouté que :

> Les politiques de protection des renseignements personnels des réseaux sociaux exigent une adhésion totale. C'est l'utilisateur qui assume le risque en ce qui concerne les renseignements personnels. Et pourtant, les réseaux sociaux misent sur le consentement des utilisateurs pour justifier leurs pratiques et indiquent que l'utilisation d'un site constitue un consentement à leur politique de protection des renseignements personnels[84].

Des témoins ont également signalé que les fournisseurs de services pouvaient modifier les contrats de manière unilatérale, d'où la nécessité d'exiger le consentement constant et informé des utilisateurs. À cet égard, Jason Zushman a affirmé :

> [I]l est primordial d'obtenir le consentement éclairé de l'utilisateur. Cela signifie que lorsque l'utilisateur consent aux conditions d'utilisation des services, il doit aussi consentir à toutes les étapes du processus. On doit également lui redemander son consentement chaque fois que les services ou leurs conditions d'utilisation sont modifiés. Le fournisseur de services ne peut pas se contenter de demander aux utilisateurs de consentir une seule fois aux conditions d'utilisation qu'il pourrait modifier de façon unilatérale par la suite[85].

Outre les modifications apportées aux politiques relatives aux renseignements personnels ou aux données, des témoins ont signalé les problèmes que posent, pour le modèle de consentement actuel, les changements apportés au contexte dans lequel les

---

81 *Ibid*.

82 *Ibid*., 1625.

83 ETHI, *Témoignages*, 1re session, 41e législature, 12 juin 2012, 1210 (Ian Kerr, Université d'Ottawa).

84 ETHI, *Témoignages*, 1re session, 41e législature, 18 octobre 2012, 1535 (John Lawford, CDIP).

85 ETHI, *Témoignages*, 1re session, 41e législature, 16 octobre 2012, 1550 (Jason Zushman, Merchant Law Group).

renseignements sont recueillis et de ce qu'Avner Levin, professeur à l'University Ryerson, appelle la « confidentialité en réseau[86] ».

Les changements contextuels renvoient à l'utilisation ou à la collecte de renseignements dans un certain contexte et à l'utilisation ultérieure qui en est faite dans un autre contexte par suite d'une innovation technologique ou de l'utilisation des renseignements par une tierce partie. La confidentialité en réseau soulève la question des attentes des utilisateurs en matière de protection des renseignements personnels et des défis reliés aux médias sociaux et à l'élargissement de la portée et de l'utilisation de ces renseignements. Selon Avner Levin,

> […] il y a une idée qui est très liée à la protection de la vie privée dans la société, et c'est celle de la confidentialité en réseau […] Il faut comprendre que lorsque les gens communiquent ou affichent des renseignements, ils ne pensent pas au nombre de personnes qui peuvent y avoir accès; ils se concentrent vraiment sur les personnes qui y ont accès dans l'immédiat[87].

Dans les deux cas, M^me^ Scassa a fait observer que les utilisateurs peuvent difficilement déterminer « quels renseignements sont recueillis, et comment et à qui ils sont communiqués[88] ». Or, compte tenu de la protection que prévoit actuellement la LPRPDE, la commissaire à la protection de la vie privée a dit : « Il est important de bien renseigner les utilisateurs en leur expliquant sans tarder les nouvelles fonctionnalités et en leur demandant de consentir de manière informée aux utilisations nouvelles des renseignements personnels[89]. »

Le Comité a reçu plusieurs recommandations visant à donner suite aux préoccupations au sujet du consentement. Par exemple, Alan Chapell, de BlueKai, estime que les entreprises devraient fournir « une plus grande granularité dans les déclarations de confidentialité parce qu'elle serait dans les contrats de licence d'utilisateur[90] » et Michael Geist est d'avis qu'il serait possible d'obtenir un consentement informé en « nous assurant que les choix personnels en matière de consentement sont respectés et que les organisations qui recueillent l'information dévoilent les renseignements de façon adéquate[91] ».

Il a également été recommandé d'exiger des entreprises qu'elles informent les utilisateurs de tout changement qui touche l'utilisation, la collecte ou la communication des renseignements personnels ou des données qui les concernent, et qu'elles en obtiennent le consentement lorsque de nouvelles conditions seront établies. La commissaire à la protection de la vie privée a indiqué :

---

86 ETHI, *Témoignages*, 1re session, 41e législature, 12 juin 2012, 1215 (Avner Levin, Université Ryerson).

87 *Ibid.*

88 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1100 (Teresa Scassa, Université d'Ottawa).

89 ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1150 (Jennifer Stoddart, commissaire à la protection de la vie privée).

90 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1550 (Alan Chapell, BlueKai inc).

91 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1110 (Michael Geist, Université d'Ottawa).

> Je crois que les entreprises devraient signaler à leurs abonnés, ou à leur clientèle, que les conditions ont changé, car le consentement que le consommateur a donné lors de son adhésion ne portait pas sur les nouvelles conditions. Il faudrait que la compagnie signale au moins que les règles du jeu ont changé pour que le consommateur ait alors le choix entre continuer et terminer son abonnement[92].

De plus, des témoins ont proposé que les entreprises fassent montre d'une plus grande transparence à l'égard de la communication des renseignements sur les utilisateurs au sein des organisations et à des tierces parties. À ce propos, Jason Zushman a dit au Comité :

> L'utilisateur doit également savoir dans quelle mesure l'information est communiquée non seulement au sein de l'organisation, mais aussi au public et à des tierces parties, qui pourraient utiliser l'information à des fins qui n'étaient pas nécessairement prévues au contrat initial que l'utilisateur a conclu avec le fournisseur de services de médias sociaux[93].

Enfin, la commissaire à l'information et à la protection de la vie privée de l'Ontario, Ann Cavoukian, a affirmé : « Il est possible de limiter la collecte de renseignements personnels en définissant avec précision et très étroitement ce qui est autorisé[94]. »

Les témoignages présentés au Comité font ressortir les difficultés auxquelles se heurtent les Canadiens au moment de donner leur consentement dans les contrats et ententes avec les médias sociaux. Pour bien appliquer les lois canadiennes en matière de protection de la vie privée et protéger les intérêts des citoyens à cet égard, il est impératif que le consentement donné soit valable et adapté aux circonstances, conformément aux principes énoncés dans la LPRPDE. Le Comité prend acte que, pour ce faire, le langage utilisé pour s'adresser aux individus doit être clair et accessible.

Recommandation 2

Le Comité recommande que la commissaire à la protection de la vie privée du Canada établisse des lignes directrices à l'intention des entreprises de médias sociaux et de gestion de données pour les aider à développer des politiques, des accords et des contrats rédigés d'une façon claire et accessible qui facilite un consentement valable et constant.

---

92 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1630 (Jennifer Stoddart, commissaire à la protection de la vie privée).

93 ETHI, *Témoignages*, 1re session, 41e législature, 16 octobre 2012, 1550 (Jason Zushman, Merchant Law Group).

94 ETHI, *Témoignages*, 1re session, 41e législature, 7 juin 2012, 1225 (Ann Cavoukian, commissaire à l'information et à la protection de la vie privée de l'Ontario).

F. Conservation et suppression des renseignements personnels

> *Le droit de se faire oublier est un aspect fondamental de la protection de la vie privée. Nos lois permettent donc aux organisations de conserver les renseignements seulement dans la mesure où elles en ont encore besoin à des fins commerciales. Ensuite, elles doivent les supprimer*[95]*.*
>
> *- Elizabeth Denham, commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique*

Des représentants de trois organismes de réglementation de la vie privée aux niveaux fédéral et provincial s'accordaient à dire que, même si les dispositions législatives du Canada limitent la durée de conservation des renseignements, il n'existe actuellement aucune façon d'appliquer cette limite. La commissaire Stoddart, en particulier, a déploré cette situation : « En réalité, il n'y a peut-être aucune limite au temps qu'une entreprise peut conserver des informations[96]. »

La question de la conservation ou de la suppression des renseignements, le soi-disant « droit de se faire oublier », se pose davantage dans les médias sociaux, où la communication rapide de renseignements personnels transmis par les utilisateurs peut en compliquer la suppression. Qui plus est, les renseignements peuvent être recueillis et utiliser par des tierces parties inconnues des utilisateurs. Jason Zushman a dit au Comité :

> Si les consommateurs choisissent de communiquer des renseignements aux sites de tiers, les moyens d'obliger la destruction de toute donnée qu'ils communiquent devraient être disponibles dans le média par lequel ils communiquent avec le tiers. C'est difficile quand il y a des ramifications comme celles-là d'imposer la production et la destruction de données d'utilisateurs[97].

La commissaire à l'information et à la protection de la vie privée de l'Ontario, Ann Cavoukian, croit que le système de réglementation du Canada pourrait tirer parti de ce qui se fait à l'étranger :

> La FTC et d'autres organisations cherchent actuellement à intégrer l'obligation de vérification par un tiers, de sorte que si l'on ordonne la suppression de dossiers, il sera possible de le vérifier[98].

Outre la transparence accrue sur le plan de la conservation des renseignements personnels et du traitement réservé aux comptes désactivés et supprimés[99], des témoins

---

95 *Ibid.*, 1250 (Elizabeth Denham, commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique).

96 ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1205 (Jennifer Stoddart, commissaire à la protection de la vie privée).

97 ETHI, *Témoignages*, 1re session, 41e législature, 16 octobre 2012, 1655 (Jason Zushman, Merchant Law Group).

98 ETHI, *Témoignages*, 1re session, 41e législature, 7 juin 2012, 1250 (Ann Cavoukian, commissaire à l'information et à la protection de la vie privée de l'Ontario).

99 ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1150 (Jennifer Stoddart, commissaire à la protection de la vie privée).

estiment que les entreprises doivent prévoir des mécanismes pour l'élimination des dossiers, en particulier les renseignements personnels des jeunes[100]. Dans le même ordre d'idées, Tamir Israel, de la CIPPIC, a préconisé la création d'un « endroit centralisé où les personnes peuvent envoyer un message à ces courtiers de données et faire des recherches à leur sujet […] pour voir si leurs noms s'y trouvent[101] » et y apporter des correctifs s'il y a lieu. En outre, selon M. Israel et compte tenu des principes d'accès et de transparence de la LPRPDE, un mécanisme pourrait être mis en place « pour parler à ces organismes et avoir une idée de l'endroit où ils envoient leurs données, de la façon dont ils les utilisent et de la source à laquelle elles sont puisées. C'est un genre de mission d'information qui, selon moi, serait vraiment utile, mais c'est très difficile pour les particuliers d'entreprendre la leur[102]. »

Les représentants de certaines entreprises qui se sont présentés devant le Comité ont mentionné que les entreprises conservaient les renseignements personnels indéfiniment ou bien qu'elles ne facilitaient pas le traitement des demandes de suppression des données. Devant le Comité, les représentants de Google et de Facebook ont fait part de nouveaux services (la fonction Takeout de Google et la fonction de téléchargement des renseignements de Facebook) grâce auxquels les utilisateurs peuvent télécharger les renseignements qui les concernent s'ils veulent s'en servir ailleurs. Ils ont tous deux mentionné les services de « tableau de bord » qui permettent aux utilisateurs d'examiner les renseignements que les entreprises détiennent à leur sujet et de demander de les corriger ou de les supprimer. BlueKai dispose aussi d'un produit semblable, un registre, qui permet aux utilisateurs de voir quelles préférences sont stockées sur leur ordinateur, de gérer leurs sujets et de demander à « ne plus utiliser leurs données de préférence[103] ».

Au nom de Google Canada, Colin McKay a dit au Comité : « [N]ous ne conservons pas toutes les données recueillies. Lorsqu'elles ne sont plus utiles, nous les détruisons. » Et il a ajouté : « Nous ne sommes pas là pour réunir une quantité énorme d'information sur vous, mais pour vous fournir, comme client, des produits et services très utiles[104]. »

Kevin Bartus, de Nexopia, site de réseautage social établi au Canada, a expliqué que l'élaboration de lignes directrices et de technologies pour la conservation et la suppression des données occasionne des difficultés, en particulier pour les petites entreprises qui disposent de peu de ressources :

> S'agissant des données appartenant à d'anciens utilisateurs, si elles sont encore là, c'est parce que nous n'avons pas encore trouvé le moyen technique de nous en débarrasser, et aussi parce que nous ne savons pas précisément ce dont nous devons nous débarrasser. Nous sommes tout à fait d'accord pour que les renseignements personnels

---

100 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1705 (Jennifer Stoddart, commissaire à la protection de la vie privée).

101 ETHI, *Témoignages*, 1re session, 41e législature, 19 juin 2012, 1210 (Tamir Israel, CIPPIC).

102 *Ibid.*

103 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1530 (Alan Chapell, BlueKai).

104 ETHI, *Témoignages*, 1re session, 41e législature, 30 octobre 2012, 1610 (Colin McKay, Google Canada).

> et les messages enregistrés par un utilisateur — un blogue par exemple — soient supprimés si ce dernier quitte le réseau. Mais ce serait bien de pouvoir les garder ne serait-ce que quelques mois, au cas où il déciderait de revenir […] Mais je ne vois vraiment pas quel avantage financier il y a à conserver ces données pendant plus de deux ans[105].

Devant le Comité, Robert Sherman, de Facebook, a reconnu que l'entreprise recueille certaines données auprès des utilisateurs et qu'elle les stocke dans un registre d'activité. Ce registre est accessible aux utilisateurs qui peuvent ensuite décider de les supprimer. Le but est « d'être tout à fait transparent au sujet des renseignements que nous avons » et la raison pour laquelle les renseignements sont conservés est d'« améliorer le service de sorte que, selon ce que les gens recherchent et ce sur quoi ils cliquent, il est plus facile d'améliorer la fonctionnalité de recherche » de Facebook, sans parler des « utilisations à des fins techniques et de débogage[106] ». Quand les utilisateurs décident de supprimer les renseignements qui les concernent, Facebook entame un processus de « suppression active » qui élimine le contenu ou retire les registres de bord contenant de l'information permettant d'identifier les utilisateurs[107]. La durée de ce processus n'est pas claire et même si Facebook peut conserver des registres rendus anonymes après la suppression, « en gros l'information [reçue] est supprimée[108] ».

Le processus de suppression des comptes qu'utilise l'entreprise de média social Twitter est précédé d'« une période de grâce de 30 jours » pendant laquelle le compte est désactivé[109]. Ce n'est qu'après 30 jours que le processus de suppression commence. Le Comité n'a pu savoir clairement combien de temps exigerait ce processus additionnel.

D'après les témoignages, bien que la LPRPDE et ses principes limitent la durée de conservation des renseignements personnels par les organisations et permettent aux individus un accès à leurs renseignements personnels, il n'y a pas toujours de mécanismes en place pour garantir le respect de ces limites. De plus, les témoignages entendus par le Comité indiquent que des individus peuvent souhaiter voir supprimer les renseignements personnels que détiennent des organisations à leur sujet.

---

105 ETHI, *Témoignages*, 1re session, 41e législature, 6 novembre 2012, 1540 (Kevin Bartus, Nexopia). Pour plus de renseignements sur Nexopia, voir les témoignages concernant spécifiquement certaines entreprises privées, dans le présent rapport.

106 ETHI, *Témoignages*, 1re session, 41e législature, 27 novembre 2012, 1550 (Robert Sherman, Facebook).

107 *Ibid.*, 1625.

108 *Ibid.*

109 ETHI, *Témoignages*, 1re session, 41e législature, 6 décembre 2012, 1550 (Laura Pirri, Twitter). Pour plus de renseignements sur Twitter, voir les témoignages concernant spécifiquement certaines entreprises privées, dans le présent rapport.

Recommandation 3

Le Comité recommande que la commissaire à la protection de la vie privée du Canada établisse des lignes directrices à l'intention des entreprises de médias sociaux et de gestion de données pour les aider à mettre en œuvre des mécanismes assurant aux individus un accès à tout renseignement personnel que ces entreprises pourraient détenir sur eux, qui limitent la durée de rétention de ces renseignements par les entreprises et qui en facilitent la suppression.

LES ENFANTS ET LES MÉDIAS SOCIAUX

> *Je dirais qu'il faut être prudent lorsqu'on affirme que les jeunes ne se soucient pas de la protection de la vie privée parce qu'ils affichent les détails de leur vie sur Facebook. Ceux qui disent cela n'ont tout simplement pas pris le temps de parler aux jeunes; ils se préoccupent énormément de la protection de la vie privée en ligne*[110].
>
> *- Valerie Steeves, professeure à l'Université d'Ottawa*

À l'heure actuelle, la LPRPDE ne contient pas de dispositions portant spécifiquement sur les renseignements personnels des enfants et des jeunes. De façon générale, la collecte, l'utilisation et la communication de renseignements personnels des personnes mineures sont régies par les dispositions concernant l'obligation d'informer les personnes de la collecte de renseignements personnels et d'obtenir leur consentement, de même que sur la responsabilité qui incombe aux entreprises d'obtenir un consentement valable et de prendre en considération la sensibilité des renseignements. C'est pourquoi les entreprises de médias sociaux ont pris soin d'établir différentes mesures de protection des renseignements pour les jeunes utilisateurs (par exemple, exiger le consentement d'un parent ou d'un tuteur) et elles interdisent parfois aux mineurs de moins de 13 ans l'accès à leurs réseaux sociaux.

Le projet de loi C-12 : Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques[111] précise de quelle façon le consentement valable doit être obtenu par application de la LPRPDE, grâce à l'adjonction de l'article 6.1, qui se lit comme suit :

---

110 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1120 (Valerie Steeves, Université d'Ottawa)

111 Projet de loi C-12 : Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques, 1re session, 41e législature. Le projet de loi est traité plus en détail dans la partie du présent rapport intitulée « Le cadre législatif du Canada dans un paysage en mutation ».

> Pour l'application des articles 4.3 à 4.3.8 de l'annexe 1, le consentement de l'intéressé n'est valable que s'il est raisonnable de s'attendre à ce que ce dernier comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles il a consenti[112].

Selon la représentante d'Industrie Canada, les modifications qui seraient apportées à la LPRPDE amélioreraient les dispositions relatives au consentement et elles ont pour « but de protéger la vie privée des personnes mineures lorsqu'elles utilisent Internet[113] ». Janet Goulding a par ailleurs expliqué que les dispositions en question nécessiteraient des organisations qu'elles fassent un effort raisonnable lorsqu'elles recueillent des renseignements personnels concernant des mineurs pour indiquer clairement pourquoi ces renseignements sont recueillis et faire en sorte que ceux-ci comprennent[114].

Le Comité a entendu de nombreux commentaires sur la situation particulière et la vulnérabilité des enfants et des jeunes qui utilisent les médias sociaux. Des témoins craignent, entre autres que les entreprises en ligne cherchent à mettre la main sur des renseignements personnels qui concernent des enfants et des jeunes sans que ceux-ci ne puissent bénéficier des mesures de protection ayant pour but de garantir que les enfants soient pleinement informés de la collecte et qu'eux ou leurs parents y consentent. Ces témoins ont aussi longuement parlé de la nécessité de concilier le droit des enfants à la vie privée et la responsabilité qu'ont leurs parents ou leurs tuteurs de s'assurer qu'ils adhèrent en toute sécurité à des réseaux sociaux.

A. La prise pour cible des enfants par les entreprises de médias sociaux

Les témoins ont, de façon répétée, attiré l'attention sur la recherche qui montre la situation particulière dans laquelle se trouvent les enfants lorsqu'ils naviguent dans Internet. Selon Janet Goulding,

> [l]a recherche montre que les enfants n'ont pas la capacité de comprendre les conséquences associées au partage de leurs renseignements personnels. Les actions de mise en marché visant les enfants ne sont pas toutes inappropriées. Toutefois, certains services électroniques recueillent subrepticement des renseignements personnels concernant des enfants dans un environnement conçu pour s'apparenter à un terrain de jeu ou à un site éducatif[115].

Sara Grimes, professeure à l'Université de Toronto, a expliqué au Comité que les études montrent que « dès les débuts du Web, le droit à la vie privée des enfants a été bafoué à des fins commerciales dans certains forums sociaux en ligne [116] ». Elle estime que cela se produit à une fréquence bien plus grande que pour la plupart des autres risques liés aux enfants en ligne; les interactions en ligne entre enfants, a-t-elle dit, « sont

---

112 Projet de loi C-12, ch. 5.

113 ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1225 (Janet Goulding, Industrie Canada).

114 *Ibid.*

115 *Ibid.*

116 ETHI, *Témoignages*, 1re session, 41e législature, 19 juin 2012, 1100 (Sara Grimes, Université de Toronto).

surveillées et explorées, la plupart du temps sans que les enfants, ni les parents ou les tuteurs, en soient informés ni y aient consenti[117] ».

Matthew Johnson, d'HabiloMédias, un centre sans but lucratif s'intéressant à la culture numérique et médiatique, a attiré l'attention sur la recherche réalisée par son organisation et celle faite ailleurs dans le monde qui montrent comment « l'environnement en ligne est extrêmement commercialisé et que la majorité des sites les plus prisés sont des sites commerciaux », de sorte que les jeunes « sont suivis et surveillés en ligne d'une manière beaucoup plus agressive que les adultes[118] ». En conséquence, a-t-il souligné, les jeunes sont exposés à des risques plus grands que les adultes au chapitre de leur vie privée en ligne.

En fait, les témoignages présentés au Comité par Nexopia montrent comment les membres de ce site, qui est axé expressément sur les jeunes, « se révèlent davantage engagés que ceux de la majorité des autres réseaux sociaux, puisqu'ils enregistrent près de 6 minutes et 14 pages par visite, comparativement à une moyenne de 5 minutes et de 10 pages[119] » pour les autres sites de réseautage social. Pareil engagement illustre à quel point les enfants et les jeunes peuvent exposer leurs informations personnelles et leurs pratiques en ligne aux entreprises de médias sociaux.

Jane Tallim, codirectrice exécutive d'HabiloMédias, a souligné que les jeunes se préoccupent de leur vie privée même si leur compréhension de la notion de vie privée et de l'exercice de leurs droits en cette matière diffère de celle des adultes.

> Il est généralement admis que les jeunes, qu'il s'agisse de fanatiques de Facebook ou d'artistes en herbe essayant de percer sur YouTube, se soucient peu de protéger leur vie privée. Ce n'est pourtant pas vrai. En réalité, la façon dont les jeunes comprennent la vie privée est peut-être plus proche qu'on ne le croit de la perception qu'en ont les adultes. En effet, il s'agit moins pour eux de décider s'il convient ou non de communiquer des renseignements que d'avoir un certain contrôle sur ce qu'ils souhaitent communiquer[120].

Répondant à l'inquiétude du Comité face aux pratiques des entreprises de médias sociaux visant les jeunes usagers et à leur vulnérabilité particulière, Robert Sherman a fait valoir que les « paramètres par défaut en général sont plus limités pour les adolescents » et que Facebook veut « placer les mineurs dans une situation qui est un peu plus limitée, pour qu'ils s'adressent à une communauté plus petite[121] ».

D'autres entreprises, notamment Twitter, ne permettent pas la participation d'usagers de moins de 13 ans. Si, malgré cette politique de protection de la vie privée, des usagers de moins de 13 ans se joignent au site, et que Twitter l'apprenne, leur compte est

---

117 *Ibid.*

118 ETHI, *Témoignages*, 1re session, 41e législature, 1er novembre 2012, 1615 et 1620 (Matthew Johnson, HabiloMédias).

119 ETHI, *Témoignages*, 1re session, 41e législature, 6 novembre 2012, 1530 (Kevin Bartus, Nexopia).

120 ETHI, *Témoignages*, 1re session, 41e législature, 1er novembre 2012, 1535 (Jane Tallim, HabiloMédias).

121 ETHI, *Témoignages*, 1re session, 41e législature, 27 novembre 2012, 1600 (Robert Sherman, Facebook).

supprimé[122]. En outre, Twitter met à la disposition des parents et des adolescents des ressources montrant comment utiliser sa plate-forme, notamment la façon de divulguer du harcèlement[123].

En parlant des façons de protéger les enfants contre l'exploration des données et les pratiques susceptibles de violer le droit à la protection de la vie privée, M[me] Grimes a suggéré qu'on observe ce que font d'autres pays qui ont adopté des lois traitant expressément de protection de la vie privée des enfants :

> [L']exemple le plus frappant est la Children's Online Privacy Protection Act, ou COPPA, aux États-Unis, qui a été élaborée en réponse à la pratique de plus en plus fréquente, à l'époque, de demander les noms et adresses des enfants afin de les solliciter directement[124].

D'autres témoins ont attiré l'attention sur ce que les enfants et les parents pourraient faire pour se protéger. Jason Zushman, du Merchant Law Group, a proposé que l'on offre « des programmes d'éducation et de sensibilisation du public qui disent aux enfants qu'Internet n'est pas nécessairement sûr et qui utilisent divers moyens pour les aider à constater qu'on ne peut pas nécessairement récupérer une chose qu'on y met et que les conséquences peuvent être de longue durée[125] ». HabiloMédias a fait valoir également que l'éducation et l'apprentissage précoce des outils numériques constituent des moyens de prévenir l'exposition non voulue des renseignements personnels des enfants en ligne. Comme Jane Tallim l'a dit : « [L]a sensibilisation à la vie privée doit bénéficier d'un appui national, aussi bien dans les programmes scolaires, du jardin d'enfants à la 12[e] année, que dans des campagnes publiques destinées à informer tous les Canadiens[126] ».

Recommandation 4

Le Comité recommande que le gouvernement du Canada et les entreprises de médias sociaux continuent à supporter les organisations qui font de l'éducation et qui fournissent de la formation sur l'activité numérique et la protection de la vie privée.

---

122 ETHI, *Témoignages*, 1re session, 41e législature, 6 décembre 2012, 1555 (Laura Pirri, Twitter).

123 *Ibid.*, 1620.

124 ETHI, *Témoignages*, 1re session, 41e législature, 19 juin 2012, 1100 (Sara Grimes, Université de Toronto).

125 ETHI, *Témoignages*, 1re session, 41e législature, 16 octobre 2012, 1700 (Jason Zushman, Merchant Law Group).

126 ETHI, *Témoignages*, 1re session, 41e législature, 1er novembre 2012, 1535 (Jane Tallim, HabiloMédias).

B. Réalisation du consentement informé

Le Comité a également entendu d'importants témoignages concernant la façon dont les entreprises de médias sociaux demandent le consentement des enfants, des adolescents et des parents. David Elder, de l'ACM, a rappelé au Comité que la disposition de la LPRPDE sur le consentement est déjà « assez flexible et qu'elle reconnaît qu'il faut appliquer une norme différente quand on s'adresse à des enfants[127] ». Néanmoins, d'autres témoins craignaient que, en dépit de la flexibilité de la LPRPDE, la protection accordée ne soit pas suffisante et que certaines entreprises ne profitent de cette lacune.

Sara Grimes s'est fondée sur sa recherche pour conclure qu'il est régulièrement demandé aux enfants de donner leur accord aux activités de collecte de données au moyen des politiques relatives à la protection de la vie privée et des conditions à respecter pour participer aux sites conçus expressément pour les adolescents et les prenant pour cible. Cela soulève la question du consentement informé, car « ces documents sont longs et extrêmement complexes […] [et] décrivent une grande variété d'activités de collecte de données et comprennent de nombreux termes qui sont inappropriés et qui ne peuvent pas même être utilisés pour demander le consentement des enfants[128] ». Elle était d'avis qu'on ne pouvait pas s'attendre à ce que ces contrats soient respectés, mais que leur utilisation et les risques en résultant restaient les mêmes[129].

Normand Landry, professeur à la TÉLUQ, partageait lui aussi les préoccupations relatives aux usages actuels qui rendent les adolescents responsables de la compréhension de ce à quoi ils donnent leur accord et de l'acquisition des connaissances voulues pour prévenir les atteintes à la vie privée. Il a fait remarquer que si les enfants ont accès aux sites des réseaux sociaux, en revanche, ils sont incapables d'exercer un contrôle réel sur leurs renseignements personnels; ainsi, il conviendrait d'imposer plus d'obligations aux sites puisque ce sont eux qui « mobilisent [les enfants en bas âge] alors qu'ils ne disposent ni de la formation, ni des ressources, ni des compétences nécessaires pour faire attention aux données fournies[130] ».

De l'avis de M[me] Grimes, pour résoudre ce problème, le Comité devrait envisager de recourir aux pratiques exemplaires actuelles, qui pourraient comprendre les suivantes :

> [F]ournir une version de ces documents [politiques sur la confidentialité et conditions d'utilisation] qui serait adaptée aux enfants pour s'assurer que les enfants et leurs parents savent précisément ce à quoi ils consentent. Même s'il existe d'excellents exemples de cette pratique, il y a très peu de sites destinés aux enfants qui se donnent la peine de le faire. Lorsqu'ils le font, les versions adaptées aux enfants sont rarement complètes; la plupart n'expliquent pas en détail les raisons de la collecte des données de

---

127 ETHI, *Témoignages*, 1re session, 41e législature, 16 octobre 2012, 1700 (David Elder, ACM).

128 ETHI, *Témoignages, 1re session, 41e législature*, 19 juin 2012, 1100 (Sara Grimes, Université de Toronto).

129 *Ibid.*, 1145.

130 ETHI, *Témoignages*, 1re session, 41e législature, 20 novembre 2012, 1620 (Normand Landry, TÉLUQ).

> l'utilisateur ou ne décrivent que les éléments qui présentent l'entreprise de médias sociaux sous un jour favorable[131].

Les représentants d'HabiloMédias étaient d'accord, présentant au Comité leur point de vue selon lequel les jeunes doivent comprendre ce à quoi ils consentent. Selon Matthew Johnson :

> Lorsqu'ils utilisent n'importe quel service, [les jeunes] doivent savoir quels renseignements ils donnent, quels renseignements le service peut recueillir au sujet de leurs activités et ce qu'il adviendra de ces renseignements lorsqu'ils seront entre les mains de l'exploitant du service ou des tiers à qui ils peuvent être vendus[132].

De l'avis d'HabiloMédias, la solution au problème comprendrait une plus grande ouverture ou transparence, qui pourrait vraisemblablement « découler de mesures législatives, de règles adoptées par l'industrie et d'initiatives des consommateurs », aussi bien que la sensibilisation des jeunes à la question de la protection de la vie privée « pour que les jeunes soient en mesure de comprendre que l'information est à leur disposition et qu'ils doivent s'en servir à bon escient[133] ». Pareil programme de sensibilisation devrait, selon eux, viser aussi à faire comprendre aux enfants et aux parents qu'ils ont droit à la protection de leur vie privée, que leurs renseignements personnels ont de la valeur et qu'ils disposent de recours juridiques et contractuels pour les protéger[134].

Recommandation 5

Le Comité exhorte les entreprises de médias sociaux à jouer un rôle plus étendu dans la promotion d'activités en ligne sécuritaires et actives qui protègent la vie privée et les renseignements personnels des individus, particulièrement à l'égard des groupes vulnérables comme les enfants et les jeunes.

---

131 ETHI, *Témoignages*, 1re session, 41e législature, 19 juin 2012, 1100 (Sara Grimes, Université de Toronto).

132 ETHI, *Témoignages*, 1re session, 41e législature, 1er novembre 2012, 1555 (Matthew Johnson, HabiloMédias).

133 *Ibid.*

134 *Ibid.*, 1535 (Jane Tallim, HabiloMédias).

C. Conciliation des droits des enfants à la protection de leur vie privée et des devoirs et préoccupations des parents

Tout en étant conscients des risques que représentent les médias sociaux et les autres sites Web pour les renseignements personnels des enfants, les témoins ont mis en garde le Comité contre les risques que représente la surprotection; c'est ce que Jane Tallim a appelé la « surveillance constante des parents, des écoles et des sociétés ainsi que son acceptation par les jeunes[135] ». De l'avis de M[me] Tallim:

> Le droit à la vie privée est un droit fondamental de la personne. Une surveillance constante réduit progressivement notre espace privé. De plus, le fait d'être perpétuellement épié sape la confiance mutuelle et la communication entre adultes et jeunes qui sont essentielles pour donner à ceux-ci l'autonomie dont ils ont besoin pour développer leur littératie numérique[136].

En guise de réponse, HabiloMédias a proposé, en plus de la sensibilisation à la protection de la vie privée, l'élargissement de « notre interprétation des risques pour la vie privée de façon à y inclure le droit à la vie privée, l'utilisation éthique des renseignements, les mécanismes de recours ainsi que les dimensions civiques et démocratiques de la vie privée[137] ». En inculquant aux jeunes l'idée que la protection de la vie privée a une dimension éthique, HabiloMédias estime que les jeunes seront en mesure de vouloir et même d'exiger « que leurs renseignements personnels soient traités d'une façon éthique par les sites et les sociétés qui les recueillent[138] ».

En plus de recommander une sensibilisation accrue et l'élargissement de la portée des droits à la protection de la vie privée, Valerie Steeves, professeure à l'Université d'Ottawa, a proposé que les entreprises de médias sociaux renforcent la capacité des enfants à effacer les renseignements les concernant dans Internet. Comme elle l'a dit, « on a certes besoin d'un bouton "effacer" », car « [l]e contexte est certainement différent quand on est mineur[139] ».

Dans leur témoignage, des témoins ont parlé de différents outils dont on se sert actuellement pour aider les enfants et leurs parents à protéger leurs renseignements personnels et leur vie privée en ligne. HabiloMédias, par exemple, a parlé de certains des programmes et lignes directrices qu'elle a conçus pour aider les jeunes à comprendre la notion de protection de la vie privée, comme le jeu *Privacy Pirates* et le programme *Digital and Media Literacy Fundamentals* ainsi que les ressources créées par suite de son sondage sur l'éducation numérique et les médias dans l'ensemble du Canada.

Les entreprises de médias sociaux qui ont comparu devant le Comité ont souligné qu'elles étaient à l'écoute des préoccupations des parents, des enseignants et des

---

135 *Ibid.*, 1530.

136 *Ibid.*

137 *Ibid.*, 1535.

138 *Ibid.*, 1635 (Matthew Johnson, HabiloMédias).

139 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1155 (Valerie Steeves, Université d'Ottawa).

organismes de réglementation en ce qui concerne l'utilisation de leurs réseaux par les enfants. Témoignant au nom de Google Canada, Colin McKay a souligné que son entreprise avait renforcé la protection dans son produit de réseautage social, Google +, expressément pour les jeunes afin de les inciter à avoir un comportement sûr en ligne. Il a dit au Comité :

> Spécialement pour les jeunes, c'est une grande affaire que de mettre un message que tous pourront voir sur un réseau social. Donc, lorsqu'ils essaient de communiquer en dehors de leurs cercles, nous ajoutons une étape de confirmation de plus pour les inciter à réfléchir avant de diffuser un message. Nous avons aussi prévu des protections par défaut qui empêchent les étrangers d'établir un contact direct et même de dire bonjour à des adolescents sans leur permission expresse[140].

Pour sa part, Robert Sherman de Facebook a fait valoir que son entreprise fournit des ressources en matière de sécurité en ligne et de sensibilisation à la sécurité, notamment « un centre de sécurité des familles » qui met à la disposition des parents, des adolescents, des enseignants et des autorités policières de l'information ainsi qu'un « comité consultatif de sécurité » qui offre son expertise en matière de produits et de politiques[141].

Le Comité a également été informé des ressources destinées aux jeunes qui ont été produites par le CPVP, notamment le site Web « youthprivacy.ca » ainsi que les études de fond qu'il a financées, dont la série *Les jeunes Canadiens dans un monde branché* et *eGirls Project* (auxquels M[mes] Tallim et Steeves ont participé à titre de chercheures).

Recommandation 6

Le Comité recommande que le gouvernement du Canada et les entreprises de médias sociaux continuent à supporter les organisations dédiées à l'éducation et à la sensibilisation des enfants, de leurs parents et enseignants, nécessaires à la protection de leurs renseignements personnels et de leur vie privée en ligne.

140 ETHI, *Témoignages*, 1re session, 41e législature, 30 octobre 2012, 1535 (Colin McKay, Google Canada).

141 ETHI, *Témoignages*, 1re session, 41e législature, 27 novembre 2012, 1535 (Robert Sherman, Facebook).

D. L'Importance de la littératie numérique

> *D'une manière générale, la capacité d'une personne à déterminer par elle-même les paramètres de protection de sa vie privée sur un site de média social requiert un haut niveau d'alphabétisme informationnel*[142].
>
> *- Normand Landry, professeur, TÉLUQ, et Leslie Regan Shade, professeure, Université de Toronto*

Une question liée à celle des enfants et des réseaux sociaux est celle de la littératie numérique. Par « littératie numérique », on entend l'ensemble des connaissances dont on a besoin pour prendre des décisions en ligne qui soient judicieuses, éclairées et conformes à l'éthique[143]. La gestion des renseignements personnels constitue une des principales compétences nécessaires à acquérir en littératie numérique. Cette dernière est considérée comme une composante centrale de la stratégie globale de l'économie numérique[144].

Selon Brendan Wicks, de l'ARIM, l'expérience des chercheurs en médias sociaux indique que la plupart des Canadiens qui affichent de l'information en ligne « ont une bonne compréhension de l'impact de leurs actions et ils savent quelles mesures il faut prendre afin de protéger leurs renseignements personnels[145] ». Conséquemment, l'ARIM estime que des pratiques d'entreprise fondées sur des normes éthiques strictes, combinées à des actions informées et délibérées des Canadiens lorsqu'ils affichent des renseignements en ligne, constituent un « moyen terme » qui devrait être maintenu[146].

Cependant, le Comité a entendu d'autres témoins qui étaient moins convaincus des niveaux de compréhension des usagers des médias sociaux canadiens et qui ont fait valoir qu'il était nécessaire que l'on crée des outils de littératie numérique afin de sensibiliser les Canadiens à l'utilisation des services en ligne et, en fin de compte, de maximiser les occasions inhérentes à cette industrie naissante. Colin McKay, de Google Canada, a invité le Canada, en tant que société, à s'

> assurer, comme société qui communique en ligne, que les jeunes, et aussi les autres générations, ont accès à des outils d'information qui leur permettent de s'y retrouver, de savoir comment communiquer des renseignements sur les médias sociaux, d'utiliser les services en ligne et de connaître le contexte dans lequel ils veulent communiquer des renseignements ou les rendre publics ou en restreindre la diffusion[147].

---

142 ETHI, mémoire de Normand Landry et de Leslie Regan Shade, « Renseignements personnels et médias sociaux : enjeux de vie privée », 15 novembre 2012, p. 10.

143 ETHI, *Témoignages*, 1re session, 41e législature, 1er novembre 2012, 1530 (Jane Tallim, HabiloMédias).

144 Voir, par exemple, les mémoires présentés pour les consultations publiques de 2010 sur l'économie numérique du Canada par Bell Canada, l'Ontario Literacy Coalition, ABC Life Literacy Canada, Catherine Middleton, professeure, et le Media Awareness Network, entre autres. [disponibles en anglais seulement]

145 ETHI, *Témoignages*, 1re session, 41e législature, 5 juin 2012, 1115 (Brendan Wycks, ARIM).

146 *Ibid.*

147 ETHI, *Témoignages*, 1re session, 41e législature, 30 octobre 2012, 1605 (Colin McKay, Google Canada).

Le Comité a aussi entendu des chercheurs et des universitaires qui ont souligné fermement la nécessité de « prendre l'enseignement de la culture numérique au sérieux » et d'« appuyer les organismes d'intérêt public, afin qu'ils puissent fournir aux gens les renseignements dont ils ont besoin pour faire des choix éclairés et prendre des décisions informées en ce qui concerne Internet[148] ». Au dire de Jane Tallim, dans le cadre d'une stratégie numérique globale, pareille assistance devrait être accordée aux enseignants pour qu'ils disposent des outils voulus pour assurer l'uniformité dans leur enseignement des compétences de base en matière de sensibilisation à la protection de la vie privée et d'autres compétences en littératie numérique[149].

M[me] Tallim a fait ressortir ensuite les rôles des divers acteurs, comme les pouvoirs publics, l'industrie et les populations locales, soulignant que :

> Le rôle fédéral peut consister à faire preuve de leadership en appuyant des rencontres et des manifestations et en favorisant des réunions d'intervenants pour donner forme au cadre dont j'ai parlé et mieux cerner les besoins. Dans les pays où la littératie numérique constitue un pilier de la stratégie nationale, il est clair que les mesures prises ne sont pas simplement dirigées par le gouvernement, par l'industrie ou par la collectivité. Il s'agit d'un effort collectif dans le cadre duquel de multiples intervenants se rencontrent pour travailler ensemble[150].

M. Gupta, de l'Association canadienne de la technologie de l'information (ACTI), a en outre attiré l'attention sur les différents acteurs qui doivent participer à la conception d'une stratégie numérique, estimant que :

> Pour réunir ces conditions, nous avons besoin d'un cadre pouvant contenir toutes les pièces. La protection des renseignements personnels et les médias sociaux n'en sont qu'un aspect. Les autres sont également importants. Nous avons besoin d'un régime de propriété intellectuelle approprié. Nous avons besoin de politiques fiscales appropriées. Nous avons besoin de normes appropriées en matière d'éducation. Tous ces points ont besoin d'être reliés[151].

La commissaire à la vie privée a dit être du même avis :

> [L]e temps est également venu pour les gouvernements, les éducateurs et les collectivités de se concentrer sérieusement sur l'éducation numérique des Canadiennes et Canadiens de tous âges […] Les gens doivent comprendre que les renseignements publiés sur Internet peuvent s'y retrouver pour l'éternité et qu'il faut faire très attention à ce que l'on publie à propos de nous et des autres[152].

À son avis, même si les taux de littératie numérique augmentent, cela ne constitue qu'un élément de la question de la protection de la vie privée et des médias sociaux, un élément « qui ne dispense pas les entreprises de leurs responsabilités en vertu des lois en

---

148 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1130 (Valerie Steeves, Université d'Ottawa).

149 ETHI, *Témoignages*, 1re session, 41e législature, 1er novembre 2012, 1600 (Jane Tallim, HabiloMédias).

150 *Ibid.*, 1605.

151 ETHI, *Témoignages*, 1re session, 41e législature, 20 novembre 2012, 1640 (Karna Gupta, ACTI).

152 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1625 (Jennifer Stoddart, commissaire à la protection de la vie privée du Canada).

matière de protection de la vie privée[153] ». Le Comité a convenu que les Canadiens ont besoin d'avoir un meilleur accès aux outils de sensibilisation à la protection de la vie privée.

Recommandation 7

Le Comité recommande que le gouvernement du Canada continue à supporter les programmes de littératie numérique.

LE CADRE LÉGISLATIF DU CANADA DANS UN PAYSAGE EN MUTATION

Le Comité a entendu des témoins louanger la législation canadienne en matière de protection de la vie privée pour la promotion qu'elle fait de l'autoréglementation et pour le fait qu'elle est flexible et neutre sur le plan technologique. Néanmoins, le Comité a aussi entendu divers témoins mettre en doute la capacité de la législation canadienne en matière de protection de la vie privée, la LPRPDE en particulier, de relever les défis induits par les changements technologiques; les témoignages allaient du maintien du statu quo à la refonte totale de la LPRPDE, en passant par des modifications mineures. La discussion ci-dessous souligne comment la législation canadienne en vigueur et le principal organisme de réglementation fédéral, le CPVP, ont pu s'adapter aux défis et aux occasions créés par les médias sociaux; elle vise aussi à éclairer les débats à venir sur la façon d'adapter la loi et les pouvoirs de la commissaire à la protection de la vie privée à la nouvelle donne.

Ceux qui étaient favorables au maintien du libellé actuel de la LPRPDE étaient des témoins représentants le secteur privé ou les associations de l'industrie. Ces témoins ont fait valoir que, telle qu'elle est maintenant écrite et appliquée, la LPRPDE est une bonne loi qui répond à la demande de l'industrie et aux besoins de la protection de la vie privée et qui facilite l'autoréglementation. Ils ont dit qu'il n'était pas nécessaire ni souhaitable de la modifier.

Colin McKay a félicité le Canada pour son « cadre particulièrement intéressant et utile de protection des renseignements personnels » qui facilite la consultation et le dialogue avec la commissaire à la protection de la vie privée sur les produits et services projetés[154]. De même, David Elder de l'ACM, a souligné que le « délicat équilibre législatif entre les intérêts individuels et les besoins commerciaux profite grandement aux

153 *Ibid.*

154 ETHI, *Témoignages*, 1re session, 41e législature, 30 octobre 2012, 1545 (Colin McKay, Google Canada).

consommateurs et au marketing axé sur l'information, qui représente une part de plus en plus importante de l'économie du Canada[155] ».

Warren Everson, de la Chambre de commerce du Canada, a signalé que, dans son libellé actuel, la LPRPDE interdit déjà la collecte de renseignements personnels pour la revente sans le consentement de l'intéressé, rendant l'autoréglementation non pertinente à cet égard[156]. Selon la Chambre de commerce du Canada, « les médias sociaux ne présentent aucun problème qui puisse faire échouer la LPRPDE[157] ». De plus, M. Everson a fait valoir que « les règles touchant la protection de la vie privée au Canada sont bien connues et bien comprises et, [qu'] à [s]on avis, elles donnent de bons résultats. Elles se sont adaptées remarquablement bien au monde numérique, et offrent ainsi d'assez bonnes protections à la population canadienne[158]. »

Adam Kardash, de chez Heenan Blaikie, était lui aussi favorable à l'applicabilité de la LPRPDE au contexte des médias sociaux :

> Selon moi, le point fort de la LPRPDE a été et continue d'être le fait qu'elle nous permet de relever les défis posés par les nouvelles technologies relativement à la protection de la vie privée […] Une des raisons pour lesquelles la loi demeure efficace aujourd'hui, c'est parce que son libellé est neutre sur le plan technologique. En gros, les règles de base de la LPRPDE sont énoncées dans un langage simple sous forme de principes généraux. Elles peuvent donc s'appliquer à tout nouveau système, technologie ou application qui met en jeu le traitement de renseignements personnels, et cela comprend aussi les plateformes des médias sociaux[159].

Il a ajouté que sous le régime « de la LPRPDE, un cadre d'autoréglementation élaboré au moyen d'un processus de consultation valable aurait une valeur juridique. Les cadres d'autoréglementation établissent des normes industrielles et, si celles-ci sont bien conçues, elles permettent d'éclairer la définition du critère fondamental de la LPRPDE, soit celui de la personne raisonnable[160]. »

D'autres témoins, bien que généralement favorables à la LPRPDE, ont attiré l'attention sur les dangers et les risques inhérents à la modification du cadre canadien de la protection de la vie privée. Kevin Bartus, propriétaire de Nexopia.com, un site de réseautage social pour les jeunes, a souligné le rôle important que joue la réglementation canadienne en matière de protection de la vie privée « dans la protection des Canadiens et pour garantir des règles du jeu équitables entre les entreprises numériques », invitant toutefois le Comité à y « aller doucement afin d'éviter de rendre les choses encore plus difficiles qu'elles ne le sont déjà[161] ». Annie Pettit, de l'ARIM, a fait ressortir que si les

---

155 ETHI, *Témoignages*, 1re session, 41e législature, 16 octobre 2012, 1540 (David Elder, ACM).

156 ETHI, *Témoignages*, 1re session, 41e législature, 5 juin 2012, 1140 (Warren Everson, Chambre de commerce du Canada).

157 *Ibid.*, 1100.

158 *Ibid.*

159 ETHI, *Témoignages*, 1re session, 41e législature, 19 juin 2012, 1120 (Adam Kardash, Heenan Blaikie).

160 *Ibid.*

161 ETHI, *Témoignages*, 1re session, 41e législature, 6 novembre 2012, 1530 (Kevin Bartus, Nexopia).

entreprises canadiennes de recherche en marketing n'arrivent pas « à affronter la concurrence dans le domaine de la recherche par médias sociaux, simplement parce que nos normes en matière de protection de la vie privée nous limitent au lieu de nous permettre de nous autoréglementer, nos clients devront se servir de recherches par médias sociaux menées dans des pays dont les normes déontologiques sont insuffisantes[162] ».

Enfin, Alan Chapell, de BlueKai, a signalé que les modifications législatives peuvent avoir des conséquences indésirées et ne pas pouvoir suivre le rythme de l'évolution technologique rapide, tout en soulignant que « [c]e qu'il y a de bien avec l'autoréglementation, si elle est assortie d'un mécanisme d'application adéquat, est qu'elle peut continuer à s'adapter à l'innovation sur le marché[163] ».

Cependant, la commissaire à la protection de la vie privée ainsi que d'autres témoins du secteur universitaire et de groupes d'intérêt public étaient moins portés à laisser inchangée la législation canadienne en matière de protection de la vie privée, faisant valoir que la loi doit être renforcée pour qu'elle puisse relever les défis que présentent les nouvelles technologies, les médias sociaux notamment, à la protection de la vie privée. Selon Tamir Israel, de la CIPPIC, bien que « la LPRPDE ait très bien résisté à l'épreuve du temps, la protection des renseignements personnels a considérablement évolué depuis son adoption, et une décennie d'expérience a mis en lumière un certain nombre de lacunes qui doivent être corrigées pour que la *Loi* puisse continuer à atteindre ses objectifs[164] ».

Les avis exprimés par ce groupe de témoins allaient de la reconnaissance de la façon dont le paysage de la protection de la vie privée a changé et du besoin du Canada de s'adapter à ces changements au moyen de réformes particulières du régime de la protection de la vie privée, à des examens globaux d'un plus large éventail de données et de lois sur la protection des consommateurs.

John Lawford, du CDIP, était d'avis que la LPRPDE a « seulement besoin de quelques rajustements visant à donner du mordant à son application[165] ». Jason Zushman, du Merchant Law Group, a déclaré également que les lois sur la protection de la vie privée « devraient être resserrées » au moyen de mécanismes d'application stricte :

> Des sanctions efficaces devraient être appliquées en ce qui concerne les dommages-intérêts en matière de responsabilité délictuelle, la common law, ou d'autres infractions

---

162 ETHI, *Témoignages*, 1re session, 41e législature, 5 juin 2012 1115 (Annie Pettit, ARIM).

163 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1610 (Alan Chapell, BlueKai).

164 ETHI, *Témoignages*, 1re session, 41e législature, 19 juin 2012, 1110 (Tamir Israel, CIPPIC).

165 ETHI, *Témoignages*, 1re session, 41e législature, 18 octobre 2012, 1550 (John Lawford, Centre pour la défense de l'intérêt public).

> aux règles. Des sanctions sévères devraient être imposées à titre de mesures de dissuasion, de façon à protéger le droit à la vie privée de tous les Canadiens[166].

Colin Bennett, professeur à l'Université de Victoria, a examiné attentivement la question des modifications de la législation sur la protection de la vie privée à la lumière de la popularité grandissante des médias sociaux et des nouvelles raisons pour lesquelles on recueille des renseignements personnels, de la façon dont on le fait et de la façon dont on les utilise :

> [l]l est vrai que les règles de protection des renseignements personnels doivent être actualisées en fonction des médias sociaux, et particulièrement sous cet angle. Notre législation, c'est-à-dire la *Loi sur la protection des renseignements personnels* et la LPRPDE, a été conçue en fonction d'une nette distinction entre l'organisation et le sujet ou entre un contrôleur de données et un individu. Aujourd'hui, cette distinction s'estompe puisque les médias sociaux produisent et vendent des données qui proviennent en fait des utilisateurs. Cette notion de données produites par l'utilisateur remet en cause quelques-uns des grands principes sur lesquels repose notre législation[167].

Par ailleurs, Teresa Scassa, professeure à l'Université d'Ottawa, a dit au Comité que « la collecte, l'utilisation et la divulgation de renseignements personnels ne concernent plus seulement la protection de la vie privée, mais ces activités soulèvent aussi, entre autres des questions relatives à la protection du consommateur, aux lois sur la concurrence et aux droits de la personne[168] ». Ainsi, « la réforme de la Loi sur la protection des données n'a que trop tardé, et elle pourrait maintenant nécessiter une reconsidération ou une modification de l'approche fondée sur le consentement, surtout dans les contextes où les données personnelles sont traitées comme une ressource et que la cueillette de ces renseignements s'étend aux déplacements, aux activités et aux intérêts[169] ». Elle est d'avis que « certaines questions pourraient nécessiter une approche plus multidisciplinaire et polyvalente », une approche qui ferait appel à d'autres mesures, comme le droit de la concurrence et les droits de la personne[170].

Janet Goulding, d'Industrie Canada, a fait valoir que le deuxième examen quinquennal parlementaire de la LPRPDE, qui doit maintenant être tenu, représenterait une bonne occasion de jeter un nouveau regard sur les questions législatives soulevées dans cette étude du Comité[171].

Enfin, résumant les témoignages entendus par le Comité et donnant son propre point de vue, la commissaire Stoddart a dit être en faveur de changements visant à renforcer la LPRPDE et, notamment son modèle d'application :

---

166 ETHI, *Témoignages*, 1re session, 41e législature, 16 octobre 2012, 1555 (Jason Zushman, Merchant Law Group).

167 ETHI, *Témoignages*, 1re session, 41e législature, 1er novembre 2012, 1625 (Colin Bennett, Université de Victoria).

168 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1110 (Teresa Scassa, Université d'Ottawa).

169 *Ibid.*

170 *Ibid.*, 1150.

171 ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1235 (Janet Goulding, Industrie Canada).

> La plus importante question mise de l'avant tout au long de l'étude concernait la capacité de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) de relever les défis liés à l'évolution de la technologie. La plupart des témoins étaient d'avis que la LPRPDE avait besoin d'être modernisée, tandis que d'autres estimaient que la LPRPDE n'avait pas besoin d'être modifiée, que son modèle d'application de la loi fonctionnait et que sa force résidait dans sa neutralité par rapport à la technologie.
>
> Selon moi, l'émergence de géants Internet menace l'équilibre recherché par l'esprit et la lettre de la LPRPDE. Le quasi-monopole exercé par ces multinationales a rendu inefficace, selon moi, l'approche toute en douceur de [la] LPRPDE, qui repose sur des recommandations non contraignantes et sur une menace de ternir la réputation. Nous avons vu des organisations ignorer nos recommandations jusqu'à ce que la Cour soit saisie de l'affaire, et nous avons vu de grandes entreprises, au nom d'une consultation avec le commissariat, s'engager à mettre en place des mesures répondant à nos préoccupations pour ensuite ignorer nos conseils. Par ailleurs, compte tenu des vastes quantités de renseignements personnels détenus par les organisations sur des plateformes de plus en plus complexes, le risque lié à des atteintes importantes et à des utilisations inattendues, non souhaitées, voire même envahissantes, de ces renseignements exige la mise en place de mesures de sécurité et de conséquences financières adaptées qui ne sont pas actuellement prévues par la LPRPDE.
>
> De nouvelles mesures incitatives, y compris l'apport de changements au modèle d'application de la loi, sont requises pour inciter les organisations à se montrer proactives, à mettre en place des protections qui s'appliquent dès le départ et à veiller au traitement sécuritaire des renseignements personnels des gens. Je suis d'accord avec les témoins qui ont déclaré que la force de [la] LPRPDE est qu'elle est neutre sur le plan technologique et qu'elle est fondée sur des principes. Nous croyons que ces caractéristiques doivent demeurer[172].

Le Comité a entendu une grande diversité de témoignages sur le cadre législatif canadien et particulièrement sur la LPRPDE. Bien que la présente étude porte sur les médias sociaux et la protection de la vie privée — et non sur un examen législatif de la LPRPDE —, les témoignages entendus devraient servir de fondement à tout futur débat sur l'examen ou la modification de la LPRPDE.

---

172 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1615 (Jennifer Stoddart, commissaire à la protection de la vie privée).

A. Modifications dont est maintenant saisie la Chambre des communes (projet de loi C-12)

> *[L]e projet de loi C-12 donnera lieu à un outil encore plus puissant pour protéger et habiliter les consommateurs en ligne*[173].
>
> *Janet Goulding, ministère de l'Industrie*

Le Comité a entendu plusieurs témoins qui se sont présentés devant lui pour parler du projet de loi C-12 : Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques[174], qui en est maintenant à l'étape de la première lecture à la Chambre des communes. Cette mesure est le résultat du premier examen quinquennal de la LPRPDE réalisé par le Comité entre le 20 novembre 2006 et le 22 février 2007, le rapport final du Comité ayant été publié le 2 mai 2007.

Selon Janet Goulding, d'Industrie Canada :

> Le projet de loi C-12 oblige les organisations à informer les personnes concernées lorsqu'une atteinte à la sécurité des données présente un risque réel de préjudice grave à leur endroit, comme le vol d'identité, la fraude ou l'atteinte à la réputation. La commissaire doit également être informée des atteintes aux mesures de sécurité pour lui permettre d'assurer la surveillance de la conformité avec les nouvelles exigences. En accord avec ses pouvoirs actuels, elle peut rendre public le nom des organisations qui ne respectent pas leurs obligations si elle estime que cela est dans l'intérêt public. Cela constitue une excellente incitation pour les organisations à agir de bonne foi[175].

À propos de ce projet de loi, des témoins, dont Tamir Israel, ont déclaré au Comité que le projet de loi C-12 était une première mesure législative positive pour donner suite aux préoccupations concernant la protection de la vie privée. Ils jugeaient toutefois que d'autres mesures s'imposaient. Le projet de loi C-12 « prévoit un cadre raisonnable pour la notification des atteintes à la protection des données, sous réserve de quelques ajustements et d'un engagement à imposer des pénalités pour la non-conformité, afin d'en assurer l'efficacité[176] ».

Le projet de loi C-12 prévoit notamment une nouvelle disposition qui a trait à la notification des atteintes à la protection des données et qui permet aux entreprises victimes d'une atteinte aux mesures de protection de déterminer si cette atteinte est suffisamment importante pour être déclarée à la commissaire à la protection de la vie privée. Toutefois, John Lawford a fait observer que cette disposition ne sera pas efficace parce qu'« il est fort peu probable qu'une société, et surtout un réseau social qui vend des données, ne déclare qu'elle a un problème systématique d'atteinte à la protection des données et des procédures de traitement de données qui donnent lieu à des fuites[177] ».

---

173 ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1225 (Janet Goulding, Industrie Canada).

174 Projet de loi C-12 : Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques, 1re session, 41e législature.

175 ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1225 (Janet Goulding, Industrie Canada).

176 ETHI, *Témoignages*, 1re session, 41e législature, 19 juin 2012, 1115 (Tamir Israel, CIPPIC).

177 ETHI, *Témoignages*, 1re session, 41e législature, 18 octobre 2012, 1530 (John Lawford, CDIP).

S'exprimant au nom du CDIP, M. Lawford a ajouté : « [N]ous prédisons avec confiance qu'aux termes du projet de loi C-12, un réseau ou une autre société en ligne n'informera presque jamais la commissaire à la protection de la vie privée d'une atteinte qui n'a pas été rendue publique autrement[178]. »

La commissaire Stoddart abonde généralement dans le sens de M. Lawford : « [D]ans sa forme actuelle, le projet de loi C-12 n'était pas une réponse adéquate à la menace continue et grandissante que constituent la fuite des données et les bris de confidentialité relatifs aux données[179]. » Elle a suggéré que soit établi un système de pénalités qui inciterait les entreprises à investir dans la protection des données et qui aurait un effet dissuasif à l'égard des violations de confidentialité, tout en restant souple pour ne pas nuire aux petites organisations. Selon elle, il se peut que le projet de loi C-12 soit déjà désuet.

B. Pouvoirs d'exécution de la commissaire à la protection de la vie privée

> *Ce qu'ils aiment à propos de la loi, c'est qu'elle n'exclut pas de secteurs et qu'elle est non normative. Pourtant, un grand nombre de mes homologues étrangers ont des outils plus puissants en matière d'application de la loi, ou ils en font la demande. C'est donc dire que ce n'est pas notre modèle d'application de la loi qu'ils admirent[180].*
>
> *- Jennifer Stoddart, commissaire à la protection de la vie privée*

La LPRPDE confère à la commissaire à la protection de la vie privée le pouvoir de recevoir les plaintes, d'en prendre l'initiative, de les examiner et tenter de régler toute plainte relative au respect des dispositions sur la protection des données. Elle n'a pas le pouvoir d'appliquer les recommandations découlant de ses examens et tentera généralement de régler toute infraction par la persuasion et la négociation. Cependant, lorsque les tentatives de la commissaire échouent et que des questions demeurent non résolues, elle peut intenter des poursuites devant la Cour fédérale, qui tiendra une audience *de novo* et qui peut accorder réparation, notamment en rendant une ordonnance et en accordant des dommages-intérêts.

Le Comité a entendu des témoins faire tantôt l'éloge tantôt la critique du modèle de l'ombudsman et du rôle du CPVP que prévoit la LPRPDE. Les témoins qui ont fait l'éloge du modèle, dont Adam Kardash, représentant de Heenan Blaikie, ont indiqué que le modèle était bien reçu par des organisations du secteur privé, car il « facilite une interaction flexible et concertée » entre eux et le Commissariat[181]. Selon Mark Hayes, de Nexopia, c'est une bonne chose que la commissaire à la protection de la vie privée ne rende pas de décisions arbitrales et ne puisse donc ainsi jouer le rôle de « juge ». Il estime

---

178 *Ibid.*

179 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1625 (Jennifer Stoddart, commissaire à la protection de la vie privée).

180 *Ibid.*, 1620.

181 ETHI, *Témoignages*, 1re session, 41e législature, 19 juin 2012, 1125 (Adam Kardash, Heenan Blaikie).

cependant que si ce rôle change, « vous risquez […] d'entraver son rôle de protecteur, sa capacité de collaborer avec ses homologues du monde entier, ce qu'elle fait extrêmement bien.Ce faisant, vous modifiez l'équilibre établi[182]. » David Elder a formulé un argument semblable et ajouté que des changements apportés au modèle de l'ombudsman modifieraient « fondamentalement » la relation entre le Commissariat et les gens d'affaires, ce qui nuirait considérablement à la communication et à la coopération entre eux[183]. Pour sa part, Adam Kardash a indiqué qu'un changement au modèle de l'ombudsman serait coûteux et nécessiterait des changements à la structure du Commissariat[184].

Colin McKay, de Google Canada, a abondé dans ce sens en signalant au Comité que le « passage à un système plus coercitif inciterait les entreprises à plus de prudence » et il a fait observer que cela obligerait les entreprises comme la sienne à « considérer les répercussions possibles d'une discussion ouverte sur le déploiement de nos produits et l'interprétation que la commissaire à la protection de la vie privée donne de ce que nous faisons[185] ». Dans la même veine, Karna Gupta, de l'ACTI, a affirmé que les entreprises du secteur de la TI sont généralement d'avis que « nous n'avons pas besoin de créer autre chose. L'industrie fait confiance à la commissaire à la protection de la vie privée, et ils travaillent extrêmement bien ensemble, et ce, sur une base continue. L'industrie voudrait conserver le statu quo[186]. »

Les commissaires à l'information et à la protection de la vie privée de la Colombie-Britannique et de l'Ontario, qui ont le pouvoir de rendre des ordonnances, un « instrument très puissant », étaient au nombre des témoins qui ont fait part de leurs préoccupations au sujet des pouvoirs d'exécution de la commissaire fédérale à la protection de la vie privée[187]. À leur avis, c'est le manque de pouvoirs qui fait que des sociétés passent outre aux recommandations de la commissaire et maintiennent des pratiques contraires aux dispositions législatives du Canada concernant la protection des renseignements personnels[188]. À ce propos, John Lawford a fait observer ce qui suit :

> [L]a commissaire à la protection de la vie privée ne peut rendre des ordonnances, ni imposer des amendes. Si les décisions en matière de protection des renseignements personnels coûtent trop cher aux réseaux sociaux ou leur causent trop d'inconvénients, ces réseaux peuvent, semble-t-il, continuer à violer la vie privée des gens […] ce refus révèle la vraie nature des réseaux sociaux : ils sont financés par les renseignements

182 ETHI, *Témoignages*, 1re session, 41e législature, 6 novembre 2012, 1545 (Mark Hayes, Nexopia).

183 ETHI, *Témoignages*, 1re session, 41e législature, 16 octobre 2012, 1635 (David Elder, ACM).

184 ETHI, *Témoignages*, 1re session, 41e législature, 19 juin 2012, 1130 (Adam Kardash, Heenan Blaikie).

185 ETHI, *Témoignages*, 1re session, 41e législature, 30 octobre 2012, 1605 (Colin McKay, Google Canada).

186 ETHI, *Témoignages*, 1re session, 41e législature, 20 novembre 2012, 1600 (Karna Gupta, ACTI).

187 ETHI, *Témoignages*, 1re session, 41e législature, 7 juin 2012, 1250 (Elizabeth Denham, commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique) et 1145 (Ann Cavoukian, commissaire à l'information et à la protection de la vie privée de l'Ontario).

188 Voir la citation de la commissaire à la protection de la vie privée à laquelle renvoie la note de bas de page 172.

> personnels. Leur demander de détruire des données, c'est leur demander de se priver d'un bien[189].

Contrairement aux autres témoins du secteur privé ayant comparu devant le Comité, l'ARIM est « en faveur de pouvoirs d'exécution plus forts pour le CPVP[190] ». Quant à Tamir Israel, il juge cette question « essentielle » pour deux raisons : d'abord pour encourager la conformité et ensuite pour faciliter les rapports avec les sociétés multinationales dans l'accomplissement du mandat du Commissariat, qui est de protéger la vie privée des Canadiens[191].

Au sujet des pouvoirs d'exécution qui permettraient à la commissaire à la protection de la vie privée d'intervenir dans les cas d'atteinte à la confidentialité, des témoins ont fait mention du pouvoir de rendre des ordonnances, d'accorder des dommages-intérêts et d'infliger des sanctions. Mme Teresa Scassa a indiqué que le pouvoir d'infliger des amendes ou des sanctions devrait être accordé à la commissaire et utilisé « dans les cas d'infractions graves ou de récidives[192] ». Elle a ajouté :

> Les sanctions administratives seraient un important moyen dans l'arsenal du commissaire. Non seulement elles punissent les fautifs, ce qui peut être utile pour signaler un comportement problématique auquel il faut remédier, mais elles acquièrent aussi une dimension d'humiliation publique. Je pense que l'un des reproches fréquents contre la *Loi sur la protection des renseignements personnels et les documents électroniques* est la bonasserie du commissaire pour les fautifs, dont il tait les noms, particulièrement de ceux dont on se plaint le plus, etc., de sorte que l'information est insuffisante[193].

Estimant que nul n'est besoin d'infliger des « amendes très sévères » aux fautifs, Tamir Israel croyait cependant que des menaces de sanction sont absolument nécessaires « pour obtenir une conformité tant proactive que réactive », car « s'ils ne risquent pas de recevoir une sanction, peu de choses les inciteront à découvrir en quoi consistent ces principes sur le plan pratique et à les intégrer dans leur modèle d'affaires[194] ».

Jason Zushman, du Merchant Law Group, a évoqué la possibilité d'adopter des lois qui prévoient que l'évaluation quantitative des dommages-intérêts est calculée directement en fonction des profits ou des multiples de capitalisation des entreprises qui ont utilisé de façon inadéquate les renseignements des utilisateurs. À son avis, il serait possible d'avoir un modèle hybride qui favoriserait la collaboration des entreprises et des organisations mondiales de médias sociaux avec lesquels le Parlement pourrait travailler

---

189 ETHI, *Témoignages*, 1re session, 41e législature, 18 octobre 2012, 1530 (John Lawford, CDIP).

190 ETHI, *Témoignages*, 1re session, 41e législature, 5 juin 2012, 1120 (Brendan Wycks, ARIM).

191 ETHI, *Témoignages*, 1re session, 41e législature, 19 juin 2012, 1115 (Tamir Israel, CIPPIC).

192 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1110 (Teresa Scassa, Université d'Ottawa).

193 *Ibid.*, 1130.

194 ETHI, *Témoignages*, 1re session, 41e législature, 19 juin 2012, 1135 (Tamir Israel, CIPPIC).

à la rédaction de lois et de règlements pour protéger le droit des Canadiens à la vie privée[195].

Colin Bennett estime aussi que des pouvoirs d'exécution étendus sont nécessaires « compte tenu de l'évolution rapide de la technologie » et qu'avec des pouvoirs accrus, « il y aurait plus de certitude pour les consommateurs et, en fait, pour les entreprises »[196]. Selon lui :

> Cela permettrait d'établir une jurisprudence plus claire grâce à laquelle les règles et les rapports d'enquête auraient une interprétation juridique plus claire que ce n'est le cas à l'heure actuelle. Il est d'ailleurs un peu étrange que certains de nos commissaires provinciaux — notamment au Québec, en Colombie-Britannique et en Alberta — soient investis de pouvoirs d'exécution en vertu de leurs lois respectives tandis que notre commissaire n'en a pas[197].

À des fins de comparaison, il a souvent été question de ce qui se fait dans d'autres secteurs de compétence, une question traitée plus en détail ci-dessous. La commissaire à la protection de la vie privée en a discuté à fond lors de sa deuxième comparution devant le Comité. Elle a alors signalé que les lois fédérales doivent conférer des pouvoirs d'exécution comparables à ceux des autres gouvernements afin d'avoir un plus grand impact sur la protection de la vie privée et de renforcer la confiance qu'accorde la population canadienne à l'environnement en ligne[198].

> Une loi qui a été créée à une époque où les réseaux sociaux, les téléphones mobiles et les technologies intelligentes n'existaient pas encore ne peut rester inchangée. Les moyens par lesquels les renseignements personnels peuvent être recueillis et utilisés dans cet environnement par de nombreux acteurs font en sorte qu'il devient de plus en plus urgent de mener une étude officielle à propos de l'efficacité de notre cadre de protection de la vie privée[199].

En ce qui concerne les préoccupations soulevées par ceux qui craignent qu'elle devienne « le juge, le jury et le bourreau », la commissaire Stoddart a relaté les expériences d'autres gouvernements, incluant ceux de provinces canadiennes, où les commissaires jouissent de puissants pouvoirs d'exécution. Elle a indiqué que cela ne les empêchait pas « de faire de la sensibilisation, de travailler avec les chefs de la protection des renseignements personnels et de tenir des réunions avec le secteur privé[200] ».

> Le concept de ce que nous appelons les organisations administratives multifonctionnelles est, en fait, très bien connu dans le droit canadien. Je crois qu'il en va de même avec le droit britannique et le droit australien, si on examine les lois d'intérêt public qui

---

195 ETHI, *Témoignages*, 1re session, 41e législature, 16 octobre 2012, 1555 et 1615 (Jason Zushman, Merchant Law Group).

196 ETHI, *Témoignages*, 1re session, 41e législature, 1er novembre 2012, 1625 (Colin Bennett, Université de Victoria).

197 *Ibid*.

198 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1625 (Jennifer Stoddart, commissaire à la protection de la vie privée).

199 *Ibid.*

200 *Ibid.*, 1635.

> ressemblent le plus à la nôtre. Mes collègues de l'Australie et du Royaume-Uni ont différentes fonctions de sensibilisation de l'entreprise et de la population, d'arbitrage et de médiation. Le commissaire au Royaume-Uni peut imposer des amendes. Celui de l'Australie peut intenter une poursuite et exiger une amende de plus d'un million de dollars australiens. Ce modèle est très bien connu à l'échelle internationale.
>
> Il est très bien connu au pays aussi. Je répète que mes collègues de la Colombie-Britannique et de l'Alberta font de la sensibilisation avec nous. Nous avons produit ensemble plusieurs documents d'orientation. Ces commissariats sensibilisent la population et rendent des jugements. Leurs conclusions sont contraignantes. Je ne sais pourquoi, tout d'un coup, nous n'aurions plus les mêmes pouvoirs qu'avant. Ces pouvoirs sont la norme en Alberta, en Colombie-Britannique, au Québec et à l'étranger depuis 15 ans[201].

Les faits présentés au Comité montrent que les opinions divergent en ce qui a trait aux pouvoirs d'exécution de la commissaire à la protection de la vie privée. D'une part, le modèle actuel, qui s'est avéré efficace pour assurer des rapports cordiaux et non conflictuels, facilite la circulation constante de l'information entre le secteur privé et la commissaire, et prouve leur bonne volonté. D'autre part, on peut dire beaucoup de choses, et on l'a fait, sur la manière dont le modèle actuel préconise l'autoréglementation et sur le fait qu'il ne permet pas d'assurer adéquatement le respect de la loi lorsqu'il y a échec de l'autoréglementation. Le Comité espère que son analyse sera utile lors de futurs examens des mesures législatives dans ce domaine.

MESURES FAVORISANT LA PROTECTION DE LA VIE PRIVÉE ET PRATIQUES EXEMPLAIRES

Lors des audiences du Comité, des témoins ont fait diverses propositions importantes sur les mesures favorisant la protection de la vie privée et les pratiques exemplaires pour l'étude des entreprises de médias sociaux, les organismes de réglementation, les décideurs et les utilisateurs des médias sociaux en général.

Dans ce rapport, le Comité ne cherche pas à formuler des recommandations précises sur des modifications législatives, mais il tient compte des préoccupations soulevées à l'égard des mesures favorisant la protection de la vie privée et incite les entreprises de médias sociaux à poursuivre leurs efforts visant à favoriser une telle protection, un principe essentiel à leurs activités et à la conception de leurs produits.

---

201 *Ibid.*

A. La protection de la vie privée comme paramètre par défaut

> *[L]'architecture de chaque technologie inclut un certain nombre de choix dans la conception. Certains de ces choix créent des états par défaut […] Le diable est dans les détails*[202].
>
> *- Ian Kerr, professeur à l'Université d'Ottawa*

Ann Cavoukian, commissaire à l'information et à la protection de la vie privée de l'Ontario, a présenté au Comité le concept de protection intégrée de la vie privée. Selon elle,

> [l]e concept prévoit, essentiellement, l'intégration de fonctions de protection de la vie privée non seulement dans les technologies de l'information mais aussi dans les pratiques, politiques et procédures commerciales responsables, de façon proactive, pour prévenir les atteintes à la vie privée plutôt que d'y réagir après coup[203].

Elle a expliqué que la protection intégrée de la vie privée « vise à garantir que l'utilisateur détermine ce qui est fait de ses renseignements personnels[204] ». Dans le mémoire qu'elle a présenté au Comité, elle explique que la protection intégrée de la vie privée repose sur sept principes fondamentaux : elle est proactive et non réactive, elle est implicite, elle est enchâssée dans la conception, la fonctionnalité intégrale est assurée, la sécurité est assurée de bout en bout, la visibilité et la transparence sont assurées et la protection est axée sur les utilisateurs, ce qui assure le respect de la vie privée des utilisateurs[205].

Ces principes mettent l'accent sur le respect de la vie privée de l'utilisateur et font de la protection de la vie privée un paramètre par défaut, ce qui permet à l'utilisateur, la personne visée par les renseignements, de savoir que ses renseignements sont protégés. Puisque la protection est intégrée dans le système, c'est automatique et garanti[206]. Dans une publication que M^me^ Cavoukian a rédigée avec Jeff Jonas, expert scientifique en chef du groupe analytique — entités à IBM, et qu'elle cite dans son témoignage, la vie privée est mieux protégée lorsque les principes de protection sont appliqués le plus tôt possible, soit pendant la planification de l'architecture, la conception du système et les procédures opérationnelles. La protection est ainsi intégrée aux processus et aux pratiques opérationnels dès le début et n'engendre pas de coûts supplémentaires par la suite pour les entreprises[207].

---

202 ETHI, *Témoignages*, 1re session, 41e législature, 12 juin 2012, 1210 (Ian Kerr, Université d'Ottawa).

203 ETHI, *Témoignages*, 1re session, 41e législature, 7 juin 2012, 1150 (Ann Cavoukian, commissaire à l'information et à la vie privée de l'Ontario).

204 *Ibid.*, 1145.

205 ETHI, Mémoire présenté par la commissaire à l'information et à la protection de la vie privée de l'Ontario, « La protection intégrée de la vie privée » *: Une règle d'or*, 7 juin 2012.

206 ETHI, *Témoignages*, 1re session, 41e législature, 7 juin 2012, 1150 (Ann Cavoukian, commissaire à l'information et à la vie privée de l'Ontario).

207 Ann Cavoukian et Jeff Jonas, « Privacy by Design in the Age of Big Data », 8 juin 2012.

Lors de son témoignage devant le Comité, le représentant de Facebook a affirmé qu'un programme complet de protection des renseignements personnels qui intègre une telle protection dès la conception avait été mis en œuvre. Selon Robert Sherman, « [c]e programme comprend un vaste examen interfonctionnel de la protection des renseignements personnels à toutes les étapes de l'élaboration d'un produit avant qu'il soit lancé[208] ».

De même, Alan Chapell, de BlueKai, a fait observer que, depuis sa fondation en 2007, l'entreprise s'efforce d'appliquer les principes de protection intégrée puisqu'elle reconnaît « l'importance d'intégrer la protection de la vie privée à [ses] produits et services[209] ». Il a décrit le résultat obtenu comme une culture de protection de la vie privée des consommateurs depuis le tout début.

Soulignant lui aussi l'importance des choix initiaux en matière de protection de la vie privée faits par les sociétés au moment de la conception de leurs sites Web ou de leurs logiciels, Michael Geist, professeur à l'Université d'Ottawa, a expliqué que

> […] les choix faits par les plus grandes sociétés de médias sociaux quant aux paramètres par défaut en matière de protection de la vie privée sont les choix par défaut pour des millions d'utilisateurs. Étant donné la pression grandissante en vue de la création de revenus, nous pouvons nous attendre à ce que ces choix par défaut subissent des modifications considérables visant à permettre une utilisation optimale des données d'utilisateur[210].

Tamir Israel, de la CIPPIC, a mentionné qu'une récente consultation sur la protection de la vie privée en ligne avait fait ressortir le fait que de nombreux services en ligne sont publics par défaut et privés moyennant certains efforts. Ainsi,

> [a]u moment de s'inscrire pour la première fois, les nouveaux utilisateurs savent rarement comment configurer l'ensemble complexe de services de contrôle de la confidentialité, qui sont d'ailleurs souvent conflictuels. Les paramètres changent constamment, à mesure que de nouvelles fonctions viennent remplacer les anciennes ou que d'autres attributs viennent se greffer aux services existants. Pour maintenir un niveau constant de confidentialité, il faut donc déployer sans cesse des efforts[211].

L'éducation et une meilleure culture numérique peuvent faire partie de la solution à ce problème, mais M. Geist croit qu'il faut déployer des efforts soutenus à l'égard des paramètres par défaut et signale l'importance d'élaborer des initiatives visant à fournir aux utilisateurs davantage d'information et de transparence et de prendre des mesures pour faire en sorte que les entreprises respectent leurs engagements en matière de protection de la vie privée[212].

---

208 ETHI, *Témoignages*, 1re session, 41e législature, 27 novembre 2012, 1535 (Robert Sherman, Facebook).

209 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1530 (Alan Chapell, BlueKai).

210 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1110 (Michael Geist, Université d'Ottawa).

211 ETHI, *Témoignages*, 1re session, 41e législature, 19 juin 2012, 1115 (Tamir Israel, CIPPIC).

212 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1110 (Michael Geist, Université d'Ottawa).

Cependant, son collègue, Ian Kerr, bien que d'accord avec ces observations, a laissé entendre que la protection de la vie privée au moyen de paramètres par défaut ne peut se régler que par l'adoption de mesures législatives[213]. Dans le contexte du commerce électronique, des médias sociaux et des sites Web pour enfants, M. Kerr considère que

> […] les valeurs par défaut seraient tout de même établies en fonction des principes de pratique équitable entourant la collecte, l'utilisation et la communication d'information. Tout dépendrait donc de la collecte d'information et des renseignements recueillis. Je crois que nous allons être en mesure d'étudier suffisamment la question pour définir les valeurs par défaut qui pourraient s'appliquer à une vaste gamme de technologies, dont le but est la collecte, l'utilisation et la communication de l'information, les trois mots clés de la LPRPDE[214].

B. Fonction de non-suivi

> *Il serait plus réaliste de prévoir des mécanismes comme l'interdiction de suivi pour que, ses choix faits, la personne raisonnable soit susceptible de se trouver bien à l'aise de fournir une certaine quantité de renseignements[215].*
>
> *- Michael Geist, professeur à l'Université d'Ottawa*

Le Comité a aussi entendu des témoignages intéressants sur la fonction de non-suivi pour la navigation Internet. Certains navigateurs et sites Internet offrent cette fonction aux utilisateurs, ce qui leur permet de refuser que leur comportement en ligne soit suivi. Elle s'inspire de la liste nationale des numéros de télécommunication exclus qui permet au consommateur de choisir de ne pas recevoir d'appels de télémarketing. Dans le même ordre d'idées, John Lawford, du CDIP, a recommandé au Comité de créer une « liste nationale d'interdiction du suivi des télécommunications[216] ».

Warren Everson, de la Chambre de commerce du Canada, a expliqué que certains navigateurs offrent déjà la fonction de non-suivi, qui empêche le placement de témoins dans l'ordinateur[217]. Comme il l'a fait observer, plusieurs fonctions de suivi sont préapprouvées à cause de la présence de témoins dans l'ordinateur. La fonction de non-suivi empêcherait ces témoins de suivre l'utilisateur, qui serait alors un inconnu chaque fois qu'il consulte un site Web ou utilise un service. M. Everson a dit au Comité :

> À l'heure actuelle, quand vous vous identifiez et vous indiquez la langue de votre choix et d'autres éléments d'information que vous souhaitez fournir au service, ces informations sont enregistrées et un témoin s'installe dans votre ordinateur pour que, chaque fois qu'il

---

213 ETHI, *Témoignages*, 1re session, 41e législature, 12 juin 2012, 1210 (Ian Kerr, Université d'Ottawa).

214 *Ibid.*, 1245.

215 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1140 (Michael Geist, Université d'Ottawa).

216 ETHI, *Témoignages*, 1re session, 41e législature, 18 octobre 2012, 1535 (John Lawford, CDIP).

217 ETHI, *Témoignages*, 1re session, 41e législature, 5 juin 2012, 1220 (Warren Everson, Chambre de commerce du Canada).

y a un contact, l'ordinateur puisse se dire : « Très bien; il s'agit de tel ou tel autre algorithme et voici les préférences[218]. »

M. Geist considérait que de nombreux sites Web avaient été lents à adopter la fonction de non-suivi. Il a cité l'exemple de Facebook, qui aurait refusé de le faire jusqu'à maintenant[219]. Il estime que le fait que l'industrie n'ait pas réussi à s'autoréglementer justifierait l'intervention du gouvernement sur le plan de l'adoption de mesures rigoureuses qui garantiraient le respect du choix de l'utilisateur[220].

Colin McKay, représentant de Google Canada, a fait valoir que l'entreprise avait conçu une fonction pour son navigateur qui comprend un mode de « navigation privée ». À son avis, cette fonction permet à l'utilisateur de naviguer sur Internet en mode invisible, c'est-à-dire sans être suivi ou sans que Google ou d'autres entreprises puissent recueillir des informations sur ses recherches ou les sites qu'il a consultés[221].

De même, Laura Pirri, de Twitter, a mentionné que la société était fière « d'être l'un des premiers services Internet d'importance à mettre en œuvre la fonction "pas de suivi"[222] ». De l'avis de M[me] Pirri, Twitter a intégré cette fonction pour que « les utilisateurs [puissent lui] faire savoir qu'ils ne veulent pas que ces renseignements soient recueillis[223] ». Twitter espère ainsi « que de plus en plus d'utilisateurs activeront cette fonction pour protéger leurs données personnelles[224] ».

Enfin, Alan Chapell a souligné que le registre de BlueKai permet à l'utilisateur de voir quelles préférences sont stockées sur son ordinateur par les témoins BlueKai et de refuser que la société les utilise pour suivre son comportement en ligne. Selon lui, une telle fonction « est gage de transparence pour les consommateurs » même si « relativement peu de consommateurs qui consultent le registre BlueKai […] demandent de ne plus utiliser leurs données de préférence[225] ». Cela lui fait croire que « les consommateurs qui comprennent les façons de faire de BlueKai s'en inquiètent généralement moins[226] ». Le niveau de connaissance ou de culture numérique requis des utilisateurs pour choisir cette fonction ou d'autres fonctions de refus d'utilisation des renseignements personnels ne ressort pas clairement.

---

218 *Ibid.*

219 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1115 (Michael Geist, Université d'Ottawa).

220 *Ibid.*

221 ETHI, *Témoignages*, 1re session, 41e législature, 30 octobre 2012, 1530 et 1630 (Colin McKay, Google Canada).

222 ETHI, *Témoignages*, 1re session, 41e législature, 6 décembre 2012, 1545 (Laura Pirri, Twitter).

223 *Ibid.*

224 *Ibid.*

225 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1530 (Alan Chapell, BlueKai).

226 *Ibid.*

C. Charte de la vie privée

En terminant, Normand Landry, professeur à la TÉLUQ, a recommandé au Comité de créer une « charte de la vie privée sur les sites de médias sociaux ». Selon lui, la charte pourrait être rédigée par des organismes de réglementation de la protection de la vie privée en partenariat avec la société civile canadienne afin d'établir un ensemble de normes uniformes qui « servirait de cadre et enjoindrait très clairement les divers acteurs, peu importe leur modèle d'entreprise, à respecter les normes partout au pays[227] ». Tous les médias sociaux exerçant des activités au Canada devraient alors se conformer à la charte[228]. Il a recommandé que les efforts en ce sens comprennent des processus non judiciarisés qui responsabiliseraient davantage les entreprises de médias sociaux en ce qui concerne la population canadienne. À son avis :

> Il nous faut également des processus non judiciarisés — et j'insiste sur le terme « non judiciarisés » — pour régler les conflits entre les utilisateurs et les gestionnaires de sites de médias sociaux. Il faut améliorer les voies de communication entre les gens qui gèrent les sites et ceux qui les utilisent. L'absence de mécanismes productifs et non judiciarisés en matière de gestion des conflits engendre les tensions que nous constatons à l'heure actuelle[229].

M. Landry a rappelé que les Canadiens sont très préoccupés par le respect de leur droit à la vie privée[230]. Évoquant des sondages à ce sujet, il a expliqué que les Canadiens sont particulièrement inquiets de la tendance qui prévaut à l'heure actuelle au sein de l'univers numérique quant à la protection de la vie privée. Selon M. Landry, les Canadiens ont également très peu confiance dans les politiques de confidentialité des principaux sites de médias sociaux[231]. Il a fait par ailleurs le constat suivant :

> Présentement, les règles ne fonctionnent pas de manière adéquate. Ce qu'on voit lorsqu'il y a des solutions qui sont judiciarisées, c'est qu'un fardeau très lourd repose sur les épaules de quelques individus qui disposent des compétences, des ressources et du désir d'en faire un exemple précis. Ce n'est pas une façon de gérer une problématique à grande échelle[232].

---

227 ETHI, *Témoignages*, 1re session, 41e législature, 20 novembre 2012, 1605 (Normand Landry, TÉLUQ).

228 *Ibid.*, 1540.

229 *Ibid.*, 1605.

230 *Ibid.*, 1615.

231 *Ibid.*

232 *Ibid.* Un mémoire (Renseignements personnels et médias sociaux : enjeux de vie privée, 15 novembre 2012), rédigé avec Leslie Regan Shade de l'Université de Toronto et remis au Comité lors du témoignage de M. Landry, fait la même recommandation.

TÉMOIGNAGES CONCERNANT SPÉCIFIQUEMENT CERTAINES ENTREPRISES PRIVÉES

A. Google

Fondée en 1998, Google est une société cotée en bourse qui offre des produits et des services liés à l'Internet, notamment des services de recherche et d'infonuagique ainsi que des technologies logicielles et publicitaires. Son service de réseautage social et d'identité, Google+, a été lancé en juin 2011 et compte déjà 400 millions d'utilisateurs inscrits, dont 100 millions sont actifs chaque mois[233].

Google s'est attirée de nombreuses critiques à cause de ses pratiques en matière de protection de la vie privée. En août 2012, la Commission fédérale du commerce des États-Unis [Federal Trade Commission (FTC)] lui a imposé une amende de 22,5 millions de dollars pour avoir contourné les mécanismes de protection de la vie privée du navigateur Safari d'Apple afin de pouvoir retracer les utilisateurs du navigateur et leur présenter des messages publicitaires, enfreignant ainsi une entente antérieure conclue avec la FTC[234].

Par ailleurs, l'Union européenne (UE) a demandé à Google en septembre 2012 de modifier sa politique de protection de la vie privée, lui fixant un ultimatum de quatre mois pour apporter les changements recommandés afin de « donner aux utilisateurs un contrôle plus détaillé sur leurs données personnelles »[235].

La demande, présentée par la commissaire à la protection des données de France au nom des 27 autorités nationales de protection des données, fait suite aux changements apportés par Google en mars 2012[236] et soulève plusieurs préoccupations concernant, notamment la pratique de Google consistant à combiner des données anonymes provenant des historiques de navigation des utilisateurs de l'ensemble de ses services afin de mieux cibler ses messages publicitaires[237].

---

233 Données statistiques de septembre 2012, publiées sur la page Web Google+ page de Vic Gundotra, vice-président de l'ingénierie chez Google [DISPONIBLE EN ANGLAIS SEULEMENT].

234 Claire Cain Miller, « F.T.C. Fines Google $22.5 Million for Safari Privacy Violations », *The New York Times*, 9 août 2012.

235 Charles Arthur, « Google privacy policy slammed by EU data protection chiefs », *The Guardian*, 16 octobre 2012 [TRADUCTION].

236 Les changements effectués par Google ont consisté à réunir des « silos » distincts de données provenant de ses divers services, notamment de son moteur de recherche, de You Tube et de Google Maps, en une seule base de données afin de pouvoir mieux cibler ses messages publicitaires et le contenu.

237 Dan Lalor, « EU gives Google four months to amend privacy policy », *Reuters*, 16 octobre 2012.

La commissaire à la protection de la vie privée du Canada, Jennifer Stoddart, a indiqué qu'elle ne pouvait endosser les recommandations formulées par l'UE parce que le Canada avait adopté une démarche différente dans ce dossier[238]. La commissaire a toutefois partagé les préoccupations des autorités de protection des données « en ce qui a trait à la politique consistant à combiner des données de même qu'à ses pratiques de conservation des données et de transparence en général »[239].

Au Canada, Google a fait l'objet de plusieurs enquêtes liées à la protection de la vie privée. Le 31 mai 2010, le CPVP a déposé trois plaintes contre Google, alléguant qu'il avait des motifs raisonnables de croire que l'entreprise avait recueilli des renseignements personnels à partir de données utiles provenant de réseaux Wi-Fi canadiens non chiffrés[240]. En juin 2011, le CPVP a publié les conclusions de son enquête, déterminant que Google avait enfreint la LPRPDE. Il a recommandé à Google de revoir et d'améliorer la formation qu'elle dispense à tous ses employés, d'adopter un modèle de gouvernance en matière de protection de la vie privée et de détruire les données utiles canadiennes recueillies, dans la mesure où elle y est autorisée par les lois du Canada et des États-Unis. Le CPVP a toutefois reconnu et salué la façon dont Google a réagi à cet incident. Même si Google a accepté de mettre en œuvre les recommandations du CPVP, la commissaire Stoddart lui a demandé de se prêter à une vérification indépendante, menée par un tiers, de ses programmes de protection de la vie privée et de transmettre les résultats à son bureau, au plus tard en juin 2012. Les résultats de la vérification n'ont pas encore été envoyés.

La commissaire à la protection de la vie privée et Google ont également correspondu concernant diverses préoccupations suscitées par les changements apportés par l'entreprise à ses politiques de protection de la vie privée. Dans des lettres de février et mars 2012[241], la commissaire constate que la politique entrée en vigueur le 1er mars 2012 comprend moins de détails sur la conservation et la suppression des renseignements personnels, et demande à Google d'expliquer plus clairement ses politiques et pratiques à cet égard. Après avoir pris connaissance des explications de Google, la commissaire a exprimé son inquiétude concernant les futurs changements possibles que l'entreprise

---

238 La commissaire à la protection de la vie privée a expliqué sa démarche en ces termes : « nous avons examiné les répercussions des modifications apportées aux règles de confidentialité, notamment l'absence d'information précise concernant la conservation des données, les conséquences du couplage des données personnelles des utilisateurs d'un service à l'autre et les répercussions pour les utilisateurs du système Android. Nous n'avons mené aucune enquête officielle sur ces pratiques en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*, mais nous avons écrit à Google pour lui faire part de nos préoccupations ». CPVP, « Lettre à l'autorité de protection des données de France concernant son examen des nouvelles règles de confidentialité de Google », *Annonce*, 16 octobre 2012.

239 *Ibid*. Voir aussi Rick Mitchell, « Article 29 Working Party Urges Google to Reconsider Privacy Policies by Year's End », *Bloomberg*, 22 octobre 2012.

240 CPVP, « Rapport des conclusions : la collecte de données Wi-Fi par Google Inc. », *Rapport des conclusions en vertu de la LPRPDE n° 2011-001*, juin 2011.

241 CPVP, « Réponse à Google à l'égard des changements à sa politique de protection de la vie privée », *Annonce*, 8 mars 2012, CPVP, « Lettre de Google », *Annonce*, 29 février 2012, et CPVP, « Lettre à Google concernant ses règles de confidentialité », 24 février 2012.

pourrait apporter à ses politiques en matière de conservation et de suppression des données[242].

M. Colin McKay, de Google Canada, a fait valoir qu'une vérification en deux étapes des comptes Google donnerait une protection accrue contre un accès non autorisé aux renseignements de chaque utilisateur. Selon M. McKay, Google garantit la sécurité de l'information de l'utilisateur et s'efforce de créer des contrôles et des expériences axés sur l'utilisateur qui facilitent des choix éclairés sur l'information à communiquer à Google et à d'autres et sur la façon de le faire[243].

Quant à Google Dashboard, il s'agirait d'un « outil qui aide à savoir ce que Google sait de moi. Il montre à chaque utilisateur son information conservée dans son compte Google. À partir d'un lieu central, il est facile de modifier les paramètres de tout service Google qu'on utilise comme Blogger, Calendrier, Documents, Gmail, Google+, etc.[244] »

M. McKay a également décrit le rôle de Google Takeout, une application qui facilite l'exportation de données de plusieurs services populaires de Google et à laquelle de nouveaux services sont ajoutés régulièrement[245]. Selon M. McKay, « Nous facilitons la tâche aux utilisateurs qui veulent nous quitter et optent pour un autre service, ce qui nous incite à rester honnêtes. Nos utilisateurs sont en sécurité avec nous, mais ils n'ont pas à se sentir prisonniers[246] » M. McKay a mentionné l'existence d'un outil appelé Préférences, concernant les annonces, qui permet d'aller voir, de corriger ou de supprimer les centres d'intérêt que Google a identifiés comme étant ceux d'un utilisateur[247].

Par ailleurs, M. McKay a affirmé au Comité que Google ne vendait pas de données à des tiers[248]. Il a expliqué :

> …il y avait des données abondantes qu'on pourrait considérer comme des données « transactionnelles », des données de réseau. Il s'agit de la façon dont le trafic est acheminé sur le réseau et dont nous voyons des attaques contre les comptes des clients. Ce ne sont pas nécessairement des données de l'utilisateur, mais elles le concernent. Ces données sont très précieuses. Elles permettent d'offrir des services de sécurité non seulement au particulier, mais aussi à l'ensemble de l'entreprise et à tout le réseau Internet[249].

M. McKay considère que Google est très précise au sujet des renseignements qu'elle recueille auprès des utilisateurs et des raisons pour lesquelles elle le fait[250].

---

242 *Ibid.*

243 ETHI, *Témoignages*, 1re session, 41e législature, 30 octobre 2012, 1530 et 1535 (Colin McKay, Google Canada).

244 *Ibid.*, 1535.

245 *Ibid.*, 1540.

246 *Ibid.*

247 *Ibid.*, 1555.

248 *Ibid.*, 1550.

249 *Ibid.*, 1555.

250 *Ibid.*, 1625.

Selon lui, Google est tout aussi précise au sujet des renseignements qu'elle n'utilise pas pour créer des banques de données et offrir des services aux publicitaires[251].

> Nous ne tenons aucun compte des données que vous jugeriez les plus délicates, par exemple sur les opinions politiques ou les problèmes de santé. Dans d'autres cas, lorsque vous utilisez nos produits, comme Google+, il vous est dit très explicitement pourquoi vous fournissez des renseignements et quelle utilisation nous en faisons[252].

Lors de son témoignage devant le Comité, la commissaire adjointe à la protection de la vie privée, Chantal Bernier, a rappelé que le rapport du Commissariat de 2011 sur Google Wi-Fi prévoyait un délai d'un an pour que Google remette au Commissariat une vérification réalisée par un tiers[253]. Selon M^me^ Bernier, le Commissariat voulait avoir la garantie que Google appliquait toutes ses recommandations[254]. M^me^ Bernier a souligné que :

> L'échéance était le 20 mai. Durant notre réunion au début mai avec les représentants de l'entreprise, nous avons constaté que Google ne semblait même pas envisager de présenter la vérification par un tiers que nous avions clairement exigée dans notre lettre. Les représentants se sont excusés et ont demandé une prolongation. En juillet, ils nous ont envoyé une vérification par un tiers qui répondait, en fait, à une demande de la FTC [la Federal Trade Commission des États-Unis][255].

B. Nexopia

Nexopia.com est un site de réseautage social créé en 2003 par un adolescent et établi à Edmonton, qui se décrit comme étant le plus important site du genre au Canada destiné expressément aux jeunes[256]. Il compte plus de 1,7 million d'utilisateurs inscrits, dont la grande majorité (environ 80 %) réside au Canada et près de la moitié, en Alberta et en Colombie-Britannique. Selon Nexopia, ses utilisateurs cherchent notamment à rencontrer des gens, à s'exprimer et à se faire connaître. Pour cela, ils créent des profils, interviennent dans des blogues à structure libre et des forums, créent des galeries de photos et diffusent des articles, des œuvres d'art, de la musique, des poèmes et des vidéos[257].

En vertu de la politique de l'entreprise, les jeunes qui souhaitent s'inscrire auprès de Nexopia doivent être âgés d'au moins 13 ans[258]. Ceux qui déclarent avoir entre 13 et 18 ans représentent plus de 34 % des utilisateurs actifs du site. Le deuxième groupe démographique en importance est celui des 19-22 ans. Selon une commentatrice, ce site

---

251 *Ibid.*

252 *Ibid.*

253 CPVP, « Rapport des conclusions : la collecte de données Wi-Fi par Google Inc. », *Rapport des conclusions en vertu de la LPRPDE n^o^ 2011-001*, juin 2011.

254 ETHI, *Témoignages*, 1^re^ session, 41^e^ législature, 11 décembre 2012, 1640 (Chantal Bernier, commissaire adjointe à la protection de la vie privée).

255 *Ibid.*

256 Nexopia.com, *About* [disponible en anglais seulement].

257 *Ibid.*

258 *Ibid*.

est « une utopie en ligne pour les adolescents » puisqu'il « échappe au radar de la surveillance parentale[259] ». L'abonnement de base étant gratuit, le site génère des revenus au moyen de la publicité et offre aux utilisateurs un service « Plus », qui leur donne des options et des privilèges supplémentaires. Nexopia a confirmé que 7 % des utilisateurs sont inscrits à ce service[260].

M. Bartus, en tant que chef de la direction de Nexopia, a expliqué au Comité que Nexopia fait partie de ces petits sites qui se concentrent sur un créneau particulier. Dans le cas de Nexopia, il s'agit des jeunes canadiens âgés de 16 à 24 ans[261].

Le 18 janvier 2010, des représentants du CDIP ont déposé une plainte contre Nexopia auprès du CPVP[262]. La plainte du CDIP concernait la protection de la vie privée des jeunes dans un monde en ligne. Elle soutenait que Nexopia ne protégeait pas la vie privée des utilisateurs de son site de réseautage en ligne axé sur les jeunes, en violation de ses obligations au titre de la LPRPDE[263].

Le 1er mars 2012, le CPVP a publié ses conclusions à la suite de l'enquête concernant cette plainte et, fait inusité, a nommé l'entreprise en cause. L'enquête du CPVP a conclu que Nexopia enfreignait la LPRPDE en ce qui concerne la divulgation des profils des utilisateurs au public; les paramètres de confidentialité par défaut; la collecte, l'utilisation et la divulgation de données personnelles recueillies au moment de l'inscription; le partage de données personnelles avec les annonceurs et d'autres tierces parties; ainsi que la conservation des renseignements personnels des non-utilisateurs[264]. Le CPVP a donc adressé 24 recommandations à Nexopia afin que cette dernière se conforme aux diverses dispositions de la LPRPDE. Nexopia a accepté de mettre en œuvre 20 recommandations dans les délais prescrits, notamment celle de fournir au CPVP des rapports d'étape périodiques, de la documentation et la preuve qu'elle a apporté les modifications demandées à son site. À ce jour, Nexopia n'a pas encore diffusé de rapport démontrant qu'elle s'est conformée aux recommandations du CPVP[265].

Les quatre autres recommandations concernaient l'archivage des données personnelles des utilisateurs. Au moment de la publication des conclusions, Nexopia avait refusé de mettre en œuvre les recommandations du CPVP à cet égard, sans toutefois proposer de mesures de rechange. Le 13 avril 2012, la commissaire à la protection de la vie privée a déposé une demande de contrôle judiciaire auprès de la Cour fédérale à

---

259 Scaachi Koul, « Nexopia is an online utopia for teens », *Maclean's*, 14 août 2012 [DISPONIBLE EN ANGLAIS SEULEMENT].

260 Nexopia.com, *About* [disponible en anglais seulement].

261 ETHI, *Témoignages*, 1re session, 41e législature, 6 novembre 2012, 1530 (Kevin Bartus, Nexopia).

262 Public Interest Advocacy Centre, «PIAC Files Privacy Complaint Against Nexopia», 19 January 2010, [disponible en anglais seulement].

263 *Ibid*.

264 CPVP, Rapport des conclusions en vertu de la LPRPDE no 2012-001, «Rapport de conclusions-Nexopia, site de réseautage social pour jeunes, a enfreint la loi canadienne sur la protection des renseignements personnels».

265 ETHI, *Témoignages*, 1re session, 41e législature, 18 octobre 2012, 1615 (M. John Lawford, Centre pour la défense de l'intérêt public).

l'endroit de Nexopia dans le but d'obliger cette dernière à appliquer ses conclusions concernant l'archivage des renseignements personnels des utilisateurs[266].

En septembre 2012, Nexopia a été vendue à un nouveau groupe d'investisseurs, dirigé par M. Kevin Bartus. Dans son témoignage, M. Bartus a expliqué qu'il a rencontré le CPVP dans le cadre du processus d'achat. Alors qu'il n'était pas en mesure de commenter les décisions prises par le groupe de propriétaires précédents, il a exprimé au Comité que la nouvelle administration de Nexopia a l'intention de répondre à toutes les recommandations du CPVP.

C. Facebook

Facebook est une entreprise de médias sociaux fondée en 2004. Elle a procédé à son premier appel public à l'épargne le 18 mai 2012[267]. À la fin de septembre 2012, Facebook comptait 4 331 employés[268]. Selon son site Web, en automne 2012, Facebook comptait un milliard d'utilisateurs actifs, 584 millions d'utilisateurs actifs quotidiennement en moyenne, et 604 millions d'utilisateurs actifs mensuellement qui utilisaient les produits mobiles Facebook[269].

En 2011, le CPVP a mené des enquêtes à la suite de plaintes contre Facebook concernant la protection des renseignements personnels, issues surtout des nouvelles fonctionnalités ajoutées par l'entreprise à sa plateforme de réseautage social[270]. Le rapport du CPVP suggère que Facebook semblait donner plus d'importance à la protection des renseignements personnels que par le passé.

Toutefois, le CPVP s'est dit déçu que l'entreprise n'ait pas prévu dès la conception des mesures de protection dans ses nouvelles fonctionnalités concernant la suggestion d'amis[271]. Une plainte concernant les fonctionnalités pour la suggestion d'amis a soulevé des questions à l'effet que Facebook ait pu accéder de façon inappropriée aux carnets d'adresses électroniques de certains individus[272]. L'entreprise a accepté d'apporter des changements aux fonctionnalités, comme de retirer la suggestion d'ami de l'invitation initiale et de ne la fournir que dans des rappels subséquents, ainsi que de permettre à des non utilisateurs de ne pas recevoir de message de Facebook[273].

---

266 *Commissaire à la protection de la vie privée du Canada* c. *Nexopia.com inc.*, Cour fédérale, dossier n° T-764-12.

267 Facebook, Newsroom, Facebook Announces Pricing of Initial Public Offering, [disponible en anglais seulement].

268 Facebook, Newsroom, Keyfacts, [disponible en anglais seulement].

269 *Ibid.*

270 CPVP, Rapport des conclusions en vertu de la LPRPDE n° 2012-002, «Rapport de conclusions - Une enquête révèle que Facebook n'a pas obtenu le consentement des non membres en vue de l'utilisation de leurs adresses électroniques pour leur proposer des amis»,.

271 *Ibid.*

272 CPVP, Document d'information, Conclusions détaillées des enquêtes sur Facebook.

273 *Ibid.*

Une autre fonctionnalité de Faceboook, les plugiciels sociaux qui permettent aux utilisateurs de voir le contenu tiré de leur profil d'utilisateur sur des sites Web de tierces parties, a également fait l'objet d'une plainte[274]. L'enquête du CPVP a révélé qu'aucun renseignement personnel n'était partagé par Facebook avec des sites Web de tierces parties, mais a suggéré que Facebook s'améliore en ce qui concerne l'éducation du public et de ses utilisateurs sur l'utilisation de cette fonctionnalité et ses conséquences sur la protection des renseignements personnels[275].

Une troisième plainte concernait le fait que Facebook, en vérifiant l'identité de ses utilisateurs, recueillait plus de renseignements personnels que nécessaire[276]. Le CPVP a considéré que de demander aux utilisateurs de télécharger des numéros de téléphones portables ou des numéros d'identification gouvernementaux afin d'identifier les utilisateurs ne contrevenait pas à la LPRPDE. Le CPVP a trouvé que la procédure de Facebook permettant de faire une plainte concernant la protection des renseignements personnels était accessible et facile à utiliser[277].

Le 21 novembre 2012, Facebook a apporté des modifications à sa politique d'utilisation des données, qui explique la façon dont la compagnie recueille et utilise les données quand les gens utilisent Facebook, et à sa Déclaration des droits et responsabilités, qui explique les conditions régissant l'utilisation de ses services[278]. Parmi les changements annoncés, Facebook va maintenant combiner les données des utilisateurs avec celles du service de partage de photos Instagram qu'elle a récemment acquis, et va assouplir les restrictions sur les courriels entre les membres du réseau social. En outre, Facebook propose de mettre fin au processus qui permettait à ses utilisateurs de voter sur les modifications à ses politiques et à ses conditions de services, en le remplaçant par d'autres canaux d'engagement, y compris une fonction pour soumettre des questions à propos de la vie privée au dirigeant de l'entreprise en charge de la politique de la protection des renseignements personnels[279].

M. Robert Sherman, le représentant de Facebook ayant comparu devant le Comité, a affirmé que l'entreprise était déterminée à offrir des outils de protection des renseignements personnels qui permettent de contrôler l'information échangée et les connexions qui se font par l'entremise de sa plate-forme[280]. Selon M. Sherman,

---

274 CPVP, Rapport des conclusions en vertu de la LPRPDE n^{o} 2011-006, «Rapport de conclusions - Une enquête révèle qu'aucune preuve ne permet d'établir que Facebook communique des renseignements personnels à d'autres sites par l'entremise d'extensions sociales».

275 *Ibid.*

276 CPVP, Résumé de conclusions d'enquête de LPRPDE n^{o} 2011-005, «L'enquête conclut que les pratiques d'authentification de Facebook sont raisonnables».

277 *Ibid.*

278 Alexei Oreskovic, "Privacy in spotlight again with Facebook's latest changes," Globe and Mail, 22 novembre 2012 [Disponible en anglais seulement].

279 Facebook, « Suggestions de modification des documents régissant le site ».

280 ETHI, *Témoignages*, 1re session, 41^{e} législature, 27 novembre 2012, 1530 (Robert Sherman, Facebook inc.).

la confiance des utilisateurs de Facebook a une importance fondamentale pour l'entreprise[281].

M. Sherman a noté que « Le Canada, avec 18 millions d'utilisateurs actifs par mois, est l'un des pays de la planète où la population est parmi les plus actives sur Facebook. Quatre internautes sur cinq au Canada sont sur Facebook[282]. » Précisant l'approche de Facebook en ce qui concerne sa politique de protection de la vie privée, M. Sherman a expliqué qu'elle était progressive, en résumant ses pratiques sur la page d'accueil et en laissant ensuite les utilisateurs cliquer sur le lien de la politique pour obtenir des précisions[283].

> Le contenu est organisé par sujet, ce qui permet de trouver vite et facilement ce qu'on cherche. Ceux qui veulent lire toute la politique sur une seule page peuvent aussi le faire. S'ils ont des questions sur des sujets précis, ils peuvent obtenir une réponse en effectuant une recherche dans notre centre d'aide[284].

Par ailleurs, M. Sherman a expliqué que l'outil « Téléchargez votre information » [Download your information] permet de télécharger une archive des informations liées à un compte Facebook, ce qui comprend les photos, les affichages et les messages. Il a précisé que cet outil permet à un utilisateur d'avoir une copie de ses informations quand il veut les utiliser ailleurs. M. Sherman a également expliqué que Facebook offre une application « tableau de bord » permettant aux utilisateurs d'examiner les types de renseignements auxquels chaque application peut accéder sur Facebook et de décider quel accès les applications auront sur leurs comptes Facebook à l'avenir[285].

Le principal modèle de gestion de Facebook, selon M. Sherman, consiste à offrir son utilisation gratuitement à tous, en échange de quoi Facebook fait de la publicité sur son site. Une page intitulée « Publicités sur Facebook » [Ads on Facebook] explique d'ailleurs ce modèle[286]. Il a ajouté que :

> De façon générale, quand on verse des renseignements dans Facebook, par exemple, sur nos intérêts personnels, vous aimez une page qui porte sur un sujet particulier, ces données peuvent nous servir à déterminer quelles publicités vous montrer[287].

M. Sherman a expliqué que des publicitaires demandent à Facebook de présenter certaines publicités visant des gens qui s'intéressent à un sujet particulier. Facebook montre ensuite cette publicité aux utilisateurs, sans fournir aux publicitaires de renseignements personnels sur les personnes qui voient la publicité. Facebook leur

---

281 *Ibid.*
282 *Ibid.*
283 *Ibid.*
284 *Ibid.*
285 *Ibid.* 1535.
286 *Ibid.*, 1550.
287 *Ibid.*

fournirait plutôt des renseignements généraux sur le nombre de personnes qui ont vu une certaine publicité[288].

Selon M. Sherman, Facebook cherche à gérer son service de manière uniforme à l'échelle mondiale afin que tout le monde vive la même expérience sur Facebook[289]. Les décisions prises par Facebook relativement à la protection de la vie privée feraient en sorte qu'elles s'appliquent à tous les utilisateurs, dans tous les pays avec lesquels l'entreprise entretient des rapports[290].

> Normalement, quand nous recevons de la rétroaction d'un organe de réglementation, nous prenons ces commentaires très au sérieux. Il peut arriver que nous décidions que certaines caractéristiques soient différentes d'un pays à un autre, mais nous préférons éviter cela autant que possible et faire en sorte que l'expérience soit la même pour tout le monde[291].

Quant à la relation qu'entretient Facebook avec le CPVP, M. Sherman la juge très productive et positive. Il considère que Facebook peut discuter avec la commissaire des décisions qu'elle prend au sujet de la protection de la vie privée et obtenir ses commentaires. Cette situation aide Facebook à offrir un meilleur produit et à mieux protéger les renseignements personnels des Canadiens, selon M. Sherman. Il estime que Facebook est un exemple du bon fonctionnement du régime existant[292].

> Nous consultons régulièrement la commissaire à la protection de la vie privée et nous avons en fait apporté des changements à notre produit suite à ses observations. Nous avons pris ces décisions, car la commissaire à la protection de la vie privée a suggéré des façons pour mieux protéger la vie privée des Canadiens[293].

D. Twitter

Twitter est un service de réseautage social en ligne et de microblogage qui permet aux utilisateurs d'envoyer et de recevoir des messages contenant au plus 140 caractères, appelés « tweets » (en anglais), « gazouillis » ou encore « micromessages ». L'entreprise, qui a pignon sur rue à San Francisco, a été fondée en 2006 et connaît depuis une croissance forte et stable. En 2012, Twitter comptait plus de 500 millions d'utilisateurs produisant chaque jour plus de 340 millions de micromessages. En outre, plus de 1,6 milliard de recherches sont effectuées chaque jour[294]. Le Canada se classe au

---

288 *Ibid.*

289 *Ibid.*, 1555.

290 *Ibid.*

291 *Ibid.*

292 *Ibid.*, 1610.

293 *Ibid.*

294 Lauren Dugan, « Unofficial Reports Suggest Twitter Surpassed 500M Registered Users In June », *All Twitter*, 31 juillet 2012. [DISPONIBLE EN ANGLAIS SEULEMENT]

huitième rang des pays ayant le plus grand nombre d'utilisateurs de Twitter, avec 11 millions d'abonnés[295].

Les micromessages peuvent être publics ou privés. Les personnes qui n'ont pas de compte Twitter peuvent lire les messages publics, tandis que les abonnés de Twitter peuvent afficher des messages publics et privés et envoyer des messages privés à d'autres abonnés. Dans sa politique de vie privée, Twitter précise qu'elle recueille de l'information personnelle au sujet de ses utilisateurs et la communique à des tiers offrant des services et des applications clientes[296]. Certains de ces renseignements, y compris le nom et le nom d'utilisateur, sont affichés publiquement. Bien qu'une bonne partie de ses services n'y ait pas recours, Twitter utilise la technologie des « fichiers témoins » pour « [recueillir] des données supplémentaires sur l'utilisation du site Web et pour améliorer [ses] services[297] ».

Selon sa politique de vie privée, Twitter précise qu'elle ne divulgue pas les « données qui sont personnelles et privées » sans le consentement des utilisateurs, mais elle se réserve le droit de divulguer ou partager les « données qui ne sont pas privées ou qui sont agrégées ou qui sont rendues autrement anonymes, telles que les informations de votre profil public, vos gazouillis, les personnes que vous suivez ou qui vous suivent ou le nombre d'utilisateurs qui ont cliqué sur un lien particulier » sans préalablement demander le consentement des utilisateurs[298].

M[me] Laura Pirri, la représentante de Twitter ayant comparu devant le Comité, a affirmé que Twitter a des valeurs d'entreprise comme la défense et le respect de la voix de l'utilisateur, ce qui comprend le respect de ses données personnelles[299]. Selon elle :

> Il n'est pas nécessaire de donner beaucoup de renseignements personnels pour se servir de Twitter. Comme je l'ai dit, on peut s'en servir sans même avoir un compte. Si vous avez un compte, vous n'avez pas à fournir votre vrai nom ou votre véritable adresse. Vous n'avez pas à inscrire votre âge ni votre sexe[300].

M[me] Pirri a affirmé que lorsque Twitter conçoit ou lance une nouvelle fonction pour son produit, elle le fait dans le respect de la vie privée[301]. « Ainsi, suivant cette philosophie, nous fournissons des avis contextuels et des informations aux utilisateurs lorsqu'ils nous donnent des renseignements, pour renforcer nos politiques en matière de protection des renseignements personnels[302]. »

---

295 Shea Bennett, « The Top 20 Countries and Cities on Twitter », *All Twitter*, 13 août 2012. [DISPONIBLE EN ANGLAIS SEULEMENT]

296 Twitter, *Politique de Vie Privée de Twitter*.

297 *Ibid*.

298 *Ibid*.

299 ETHI, *Témoignages*, 1re session, 41e législature, 6 décembre 2012, 1535 (Laura Pirri, Twitter inc.).

300 *Ibid.*

301 *Ibid.*, 1540.

302 *Ibid.*

M^me^ Pirri a souligné le fait que Twitter a communiqué avec le CPVP au moment du lancement de la fonction d'interdiction de suivi, pour que la commissaire soit au courant de ses projets[303].

M^me^ Pirri a mentionné que des lignes directrices relativement à l'application des lois sont disponibles sur le site de Twitter. M^me^ Pirri a expliqué qu'afin de protéger la vie privée de ses abonnés, Twitter exige qu'une demande pour obtenir des renseignements personnels au sujet d'un abonné suive les voies judiciaires normales, c'est-à-dire de présenter une ordonnance du tribunal ou une assignation à témoigner. Elle a ajouté que Twitter tient aussi à la transparence au sujet des demandes des forces de l'ordre et qu'elle avise toujours les utilisateurs lorsqu'une demande d'information a été faite de cette façon à leur sujet. C'est la procédure que Twitter demande aux parties de suivre quand elles veulent obtenir des données[304].

À propos de l'anonymat sur Twitter, M^me^ Pirri a formulé l'objectif suivant :

> [N]ous voulons constituer une plate-forme où s'expriment toutes sortes d'utilisateurs. Nous trouvons important de permettre à ces voix d'être entendues, et qu'elles puissent s'exprimer sans fournir de renseignements permettant d'en identifier les auteurs, ce qui pourrait avoir des conséquences autour d'eux[305].

Selon M^me^ Pirri, plusieurs principes relatifs à la protection de la vie privée qui sont mis de l'avant aux États-Unis ne concernent pas seulement les avis, la divulgation, la sécurité, l'accès à l'information et le droit de supprimer ou de modifier de l'information[306] :

> Notre politique vise à informer les utilisateurs de tous les différents contrôles et outils que nous mettons à leur disposition à l'égard de l'information que nous recueillons, et à leur expliquer comment la modifier et la supprimer. Nous fournissons aux utilisateurs ce genre de contrôles et d'accès à l'information […][307].

M^me^ Pirri a souligné l'importance d'expliquer clairement aux utilisateurs pourquoi l'entreprise recueille l'information et comment elle l'utilise et de leur donner la possibilité de la supprimer et de le faire d'une manière plus fragmentaire que de simplement supprimer leur compte[308].

> Nous essayons de faire les choses d'une manière un peu plus précise, comme permettre aux utilisateurs de supprimer l'emplacement où ils se trouvaient quand ils ont rédigé leur gazouillis, sans effacer le gazouillis en tant que tel[309].

---

303 *Ibid.*, 1545.
304 *Ibid.*
305 *Ibid.*, 1600.
306 *Ibid.*, 1610.
307 *Ibid.*
308 *Ibid.*, 1620.
309 *Ibid.*

E. Acxiom

Fondée en 1969, Acxiom Corporation est une entreprise mondiale de services et de technologie de marketing ayant des bureaux aux États-Unis, en Europe, en Asie et en Amérique du Sud[310]. Les services offerts par Acxiom permettent aux spécialistes du marketing de gérer les publics cibles, de personnaliser les expériences des consommateurs et de tisser des liens avec la clientèle. Ses activités en ligne et hors ligne comprennent la collecte et l'analyse de données sur les consommateurs, des banques de données, l'intégration de données et des conseils pour établir des stratégies de marketing personnalisées dans de multiples formats[311].

En 2005, Acxiom a fait l'acquisition de Digital Impact et a mis sur pied Acxiom Digital, ce qui lui a permis d'intégrer ses services numériques et en ligne, et d'ainsi créer l'une des plus vastes banques de données commerciales sur les consommateurs. Des analyses récentes indiquent que les serveurs d'Acxiom traitent plus de 50 billions de « transactions » de données par année. Les dirigeants de l'entreprise ont affirmé que leur banque de données contient de l'information sur environ 500 millions de consommateurs actifs partout dans le monde et environ 1 500 points de données par consommateur[312]. La valeur annuelle d'Acxiom est estimée à 1,15 milliard de dollars, soit plus de 12 % des 11 milliards de dollars que représentent les ventes annuelles du secteur des services de marketing direct[313].

M[me] Jennifer Barrett Glasgow, la représentante d'Acxiom ayant comparu devant le Comité, a affirmé que « [n]ous mettons un point d'honneur à respecter toutes les obligations juridiques dans chaque pays où nous recueillons des données. Je tiens également à ajouter que lorsqu'elles sont utilisées correctement, les données des consommateurs peuvent apporter une importante contribution à l'économie, à son essor et à sa stabilité[314]. »

M[me] Barrett Glasgow a expliqué qu'ailleurs dans le monde, Acxiom offre une plus large gamme de produits et de services, mais qu'au Canada, elle fournit seulement des produits d'annuaires téléphoniques d'entreprises et de consommateurs, ce qui représenterait un peu moins de 1,5 million de dollars de revenus annuels. Elle a précisé qu'Acxiom fait affaire au Canada sans y avoir de place d'affaires, en offrant un soutien à partir de son siège social de Little Rock, en Arkansas, aux États-Unis[315].

M[me] Barrett Glasgow a précisé la nature des activités canadiennes de l'entreprise ainsi :

---

310 Voir : Axciom, About.

311 *Ibid*.

312 Natasha Singer, « Acxiom, The Quiet Giant of Consumer Database Marketing », *The New York Times*, 16 juin 2012. [DISPONIBLE EN ANGLAIS SEULEMENT]

313 *Ibid*.

314 ETHI, *Témoignages*, 1[re] session, 41[e] législature, 6 décembre 2012, 1635 (Jennifer Barrett Glasgow, Acxiom).

315 *Ibid.*

> Les annuaires d'entreprises et de consommateurs canadiens d'Acxiom sont offerts sous licence à des entreprises et à des organismes sans but lucratif pour leur utilisation interne à titre d'assistance annuaire automatisée et à faible coût ou à des fins de publipostage et de télémarketing. Nous délivrons également des licences d'annuaire aux entreprises qui hébergent des moteurs de recherche d'annuaires sur Internet utilisés tant par les consommateurs que les entreprises. Dans ces cas-là, les listes d'Acxiom peuvent être fusionnées aux listes téléphoniques provenant d'autres sources[316].

Selon M[me] Barrett Glasgow, Acxiom ne vend pas les données à des particuliers, mais seulement à des entreprises qualifiées[317]. La sélection se ferait en vérifiant « qu'il s'agit d'une société digne de foi, avec un nom légitime pour les données précises qu'elle demande[318]. »

M[me] Barrett Glasgow a expliqué que, « Aux États-Unis, nous avons des produits qui identifient les personnes utilisant beaucoup les médias sociaux et indiquent quels types de médias sociaux un particulier fréquente, comme Twitter ou Facebook, mais ce n'est pas un service que nous offrons au Canada […]»[319]. « Au Canada », a-t-elle poursuivi, « nous apparions le nom, l'adresse et le numéro de téléphone car ce sont des données d'annuaire téléphonique et nous avons un numéro de téléphone pour chaque dossier[320] ».

M[me] Barrett Glasgow a expliqué qu'Acxiom pouvait livrer les données à ses clients de deux façons[321]. La première consiste à acheter d'Acxiom une liste déterminée en fonction de certains critères que le client a précisés[322]. La deuxième façon est par une « liste améliorée », qui consiste à apparier la base de données de l'entreprise avec les renseignements fournis par le client afin de compléter ces renseignements[323].

F. BlueKai

Fondée en 2008, BlueKai est l'une des principales entreprises d'agrégation de données en ligne et se décrit comme la plate-forme de gestion de données, d'échange de données et de système analytique fonctionnant sur n'importe quel support d'information la plus interconnectée de l'industrie[324]. Il s'agit d'une société privée dont le siège social se trouve à Cupertino, en Californie, et qui a des bureaux à New York et à Seattle[325].

Le logiciel de BlueKai permet à ses clients de trier les consommateurs dans environ 30 000 segments de marché, par exemple les consommateurs économes ou

---

316 *Ibid.*
317 *Ibid.*, 1645.
318 *Ibid.*
319 *Ibid.*, 1655.
320 *Ibid.*
321 *Ibid.*, 1705.
322 *Ibid.*
323 *Ibid.*
324 Voir : BlueKai, About us [disponible en anglais seulement].
325 *Ibid.*

les chasseurs d'aubaines modérés[326]. La catégorisation des internautes facilite les soumissions en temps réel pour les publicités qui ciblent une catégorie particulière d'utilisateurs. Le vaste réseau de partenariats de l'entreprise lui permet de suivre chaque mois plus de 160 millions de personnes qui envisagent l'achat de biens tels que des voitures, des services financiers, des marchandises au détail, des produits de consommation ou l'hébergement dans le cadre de voyages. En triant les utilisateurs en fonction de leurs intérêts ou de leur pouvoir d'achat, le logiciel de BlueKai aide les annonceurs à déterminer dans quelle mesure chaque personne vaut la peine d'être suivie et à quel prix. Bien que BlueKai ne recueille ni ne trie des données sur les consommateurs, elle fournit un logiciel qui permet aux sites Web de suivre les utilisateurs et de les inclure dans des segments de marché[327].

Selon le président-directeur général de la société, M. Omar Tawakol, BlueKai et d'autres entreprises du domaine du marketing axé sur les données jouent deux rôles : elles veillent à ce qu'un ensemble pertinent de contenu et de possibilités soit offert aux consommateurs et puisse les intéresser, et assurent l'efficience des entreprises qui veulent atteindre ces consommateurs. Il résulte de cette relation un Internet gratuit, tout simplement[328].

Alan Chapell, le représentant de BlueKai ayant comparu devant le Comité, a exprimé la mission de BlueKai comme étant « de créer la première plateforme d'entreprise complète de marketing axé sur les données avec le plus grand souci possible de protection de la vie privée des consommateurs[329] ». M. Chapell a présenté son entreprise ainsi :

> Nous offrons une plateforme de gestion des données qui permet aux publicitaires de recueillir, de stocker et d'utiliser des données anonymes sur les préférences des consommateurs[330].

M. Chapell a précisé que la plateforme de BlueKai permet aux entreprises de marketing d'utiliser des données pseudonymes à des fins d'analyse et de publicité comportementale en ligne[331]. Selon M. Chapell, cette plateforme :

> […] permet aux entreprises de créer des publics cibles établis en fonction de leurs propres données et de données tierces afin d'atteindre leurs publics cibles grâce à des réseaux de publicité et à des échanges avec des tiers. Elle aide également les entreprises à déterminer avec précision quel type de campagne mener pour mieux cibler les achats dans les médias et trouver des idées de publicité créatives[332].

---

326 Jeffrey Rosen, « Who Do Online Advertisers Think You Are? », *The New York Times Magazine*, 30 novembre 2012 [disponible en anglais seulement].

327 *Ibid.*

328 Omar Tawakol, « Statement Correcting Recent NY Times' Story Assertions », 1er décembre 2012 [disponible en anglais seulement].

329 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1530 (Alan Chapell, BlueKai inc.).

330 *Ibid.*

331 *Ibid.*

332 *Ibid.*

En donnant l'exemple de Ghostery[333], M. Chapell a noté que de plus en plus d'utilisateurs d'Internet téléchargent leurs propres outils pour assurer la transparence[334]. M. Chapell a expliqué comment ces outils fonctionnent :

> Il s'agit de modules externes axés sur les navigateurs qui indiquent aux utilisateurs d'Internet quels témoins sont communiqués par quelles entreprises sur les sites Web qu'ils visitent. Il est clair que l'on peut fournir aux utilisateurs ce mécanisme assorti d'une transparence accrue. Nous voyons de plus en plus d'utilisateurs d'Internet employer exactement ces types d'outils[335].

En ce qui concerne la situation aux États-Unis, M. Chapell a rappelé la présence grandissante de petites icônes dans les publicités numériques qui sont ciblées grâce aux données de publicité comportementale en ligne[336].

> Il est possible que l'utilisateur ne sache pas quelle entreprise le cible simplement en regardant le petit point sur la publicité, mais c'est un mécanisme qui lui permet de comprendre un peu mieux la pratique de la publicité comportementale en ligne et d'ensuite aller à la page où il peut se prévaloir de son option de retrait[337].

EXEMPLES INTERNATIONAUX

Comme l'a rappelé au Comité la commissaire Stoddart[338], les lois en matière de protection de la vie privée des différents pays ne diffèrent pas beaucoup, étant toutes fondées sur le principe du traitement équitable de l'information adopté en 1980 par l'Organisation de coopération et de développement économiques (OCDE). Selon la commissaire, le Canada ayant choisi de s'inspirer de la norme européenne en matière de loi sur la vie privée, notre système de transfert des données est adéquat[339]. La commissaire Stoddart a noté que :

> Récemment, aux États-Unis, le département du Commerce et la Commission fédérale du commerce ont fait des progrès très intéressants en vue de rendre plus explicite la norme en matière de protection des renseignements personnels des États-Unis. Il y a aujourd'hui très peu de différences entre les pays.
>
> J'aimerais ajouter que les organismes responsables de l'application des lois sur la protection de la vie privée travaillent de plus en plus de concert[340].

M[me] Janet Goulding, d'Industrie Canada, a noté que l'OCDE effectuait présentement un examen de ses lignes directrices sur la protection de la vie privée, qui ont été adoptées internationalement et qui ont influé sur l'élaboration du Code type sur la

---

333 Voir : Ghostery, About.

334 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1600 (Alan Chapell, BlueKai inc.).

335 *Ibid.*

336 *Ibid.*

337 *Ibid.*

338 ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1210 (Jennifer Stoddart, commissaire à la protection de la vie privée of Canada).

339 *Ibid.*

340 *Ibid.*

protection des renseignements personnels du Conseil canadien des normes sur lequel repose la LPRPDE[341].

A. Union européenne et pouvoirs d'application de la loi

Le 25 janvier 2012, la Commission européenne a proposé une réforme globale des règles adoptées par l'Union européenne (UE) en 1995 en matière de protection des données afin de renforcer les droits en matière de respect de la vie privée et de donner un coup d'accélérateur à l'économie numérique européenne[342]. À l'heure actuelle, les 27 États membres de l'UE ont adopté une approche différente pour mettre en œuvre les règles de 1995, d'où des divergences dans l'application du texte. La Commission cherche à doter l'UE d'un corpus unique de règles pour tous les États membres.

En plus d'uniformiser les règles, le nouveau régime cherche à améliorer la protection des données. Par exemple, les entreprises doivent obtenir le consentement explicite des personnes visées avant d'utiliser et de traiter les données les concernant. Elles ne peuvent recueillir plus de renseignements que ce qui est strictement nécessaire et ne les conserver que pendant qu'elles en ont besoin. Les nouvelles règles créent également un « droit à l'oubli numérique », ou « droit d'être oublié », qui permettra aux citoyens de supprimer leurs données, ou d'en demander leur suppression, si aucun motif légitime ne justifie leur conservation[343].

Les nouvelles règles s'appliqueront à tous les États membres et viseront toute entreprise faisant affaire avec un État membre, même si son siège social se trouve à l'extérieur de l'UE. Les propositions de la Commission ont été transmises au Parlement européen et aux États membres à des fins de discussion. Elles entreront en vigueur deux ans après leur adoption, prévue en 2016[344].

En ce qui concerne la situation européenne, Valerie Steeves, de l'Université d'Ottawa, a expliqué au Comité que :

> Ce sont surtout les pays européens qui ont abordé ces questions selon une perspective générale et qui ont trouvé des solutions qui tiennent compte des intérêts généraux liés aux droits de la personne. En Europe, la protection des renseignements personnels est assurée selon une approche axée sur les droits de la personne, et il y a des mesures solides de protection des droits de la personne en ce qui concerne le respect de la vie privée et l'inviolabilité de la personne[345].

---

341 *Ibid.*, 1225 (Janet Goulding, ministère de l'Industrie du Canada).

342 Commission européenne, « Communiqué de presse : La Commission propose une réforme globale des règles en matière de protection des données pour accroître la maîtrise des utilisateurs sur leurs données, et réduire les coûts grevant les entreprises », 25 janvier 2012.

343 *Ibid.*

344 *Ibid.*

345 ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1150 (Valerie Steeves, Université d'Ottawa).

En ce qui concerne le pouvoir d'imposer des amendes, la commissaire Stoddart a cité les exemples du commissaire du Royaume-Uni et de plusieurs autorités internationales de protection des données[346].

> Au Royaume-Uni, mes homologues détiennent plus de pouvoirs en matière d'application de la loi, ce qui n'a pas empêché la mise en place d'une approche de l'ombudsman. Des amendes sont en effet imposées lorsqu'une méthode plus indulgente n'a pas fonctionné. Nos homologues nous disent que les entreprises qui s'engagent dès le départ à adopter de bonnes pratiques pour la protection de la vie privée croient qu'imposer un fardeau financier à celles qui ne le font pas rend la concurrence plus équitable[347].

À cet égard, la commissaire Stoddart a fait un parallèle avec les commissaires du Québec, de l'Alberta et de la Colombie-Britannique, qui ont le pouvoir de délivrer des ordonnances et de régir le secteur privé. La commissaire a précisé :

> Ils ont également d'autres fonctions, prescrites par la loi, qui leur permettent de jouer de nombreux rôles, soit celui d'éducateur, d'arbitre, d'exécuteur, de défenseurs, etc. J'ai remarqué que les témoins ayant pris la parole devant le présent comité n'avaient que de bons commentaires à faire sur les relations qu'ils avaient eues avec eux. Des témoins ont dit que le modèle canadien faisait l'envie de nombreux pays partout dans le monde[348].

La commissaire Stoddart a rappelé au Comité que l'objectif lors de l'adoption de la LPRPDE était de respecter les normes de l'UE. Elle a souligné qu'à ce jour, 80 pays dans le monde ont adopté le modèle européen[349]. Selon la commissaire, une quinzaine de pays en dehors de l'Union européenne respectent clairement les normes européennes. Le Canada est d'ailleurs le premier pays qui a emboité le pas. D'après elle:

> Nous devons continuer d'examiner le modèle européen. Il faut prévoir divers niveaux d'amendes qui vont de quelques milliers d'euros à des montants très élevés. L'entreprise visée peut être une petite entreprise locale et familiale qui ne veut pas respecter la loi ou une grande multinationale[350].

La commissaire Stoddart a présenté au Comité un document intitulé « Pouvoirs d'exécution en vertu des lois internationales sur la protection de la vie privée », qui compare les pouvoirs d'application des lois qui protègent la vie privée dans plusieurs pays. Ce document se trouve à l'Annexe B.

B. États-Unis d'Amérique et Federal Trade Commission

Par ailleurs, aux États-Unis, où la norme générale est de laisser les entreprises se réglementer elles-mêmes, il n'existe aucun cadre particulier régissant l'utilisation des

---

346 ETHI, *Témoignages*, 1re session, 41e législature, 11 décembre 2012, 1620 (Jennifer Stoddart, commissaire à la protection de la vie privée).

347 *Ibid.*

348 *Ibid*.

349 *Ibid.*, 1645.

350 *Ibid.*

données personnelles. La Commission fédérale du commerce[351] n'intervient que lorsqu'une entreprise néglige de manière patente de s'autoréglementer. La FTC est dotée de vastes pouvoirs l'autorisant à faire enquête sur les pratiques commerciales déloyales et trompeuses, pouvoirs qu'elle a invoqués pour rendre des décisions concernant Facebook[352] et Google[353].

La FTC a publié un rapport en mars 2012 dans lequel elle demande, d'une part, au Congrès d'envisager la possibilité d'adopter une loi sur la protection de la vie privée dans le but de protéger les consommateurs et, d'autre part, à l'industrie de mettre en œuvre le cadre de protection de la vie privée en invitant les entreprises à prendre des initiatives individuelles et des mesures d'autoréglementation rigoureuses et applicables[354].

En ce qui concerne le cadre de protection de la vie privée proposé, la FTC a formulé des recommandations dans trois secteurs clés. Premièrement, elle recommande que les entreprises adoptent une approche garantissant le respect de la vie privée à l'étape de la conception en faisant de la protection de la vie privée un critère fondamental de leurs pratiques commerciales. Deuxièmement, les entreprises devraient offrir des choix plus simples et mieux structurés aux consommateurs sur leurs pratiques touchant les renseignements. Troisièmement, les entreprises devraient adopter des mesures pour que ces pratiques soient plus transparentes. Plus particulièrement, les entreprises qui ne font pas directement affaire avec les consommateurs, telles que les courtiers de données, devraient donner aux consommateurs un accès raisonnable aux données qu'elles conservent à leur sujet. Le rapport encourage les entreprises individuelles et les organismes d'autoréglementation à accélérer l'adoption des principes contenus dans le cadre de protection de la vie privée[355].

Le rapport de la FTC recommande également la poursuite de la mise en œuvre d'un mécanisme offrant aux consommateurs l'option d'interdire la collecte par les publicitaires et des tiers de renseignements au sujet de leurs activités sur Internet. Le rapport mentionne les initiatives importantes prises par un certain nombre d'entreprises à la suite de la recommandation de la Commission relative à l'interdiction de collecte de renseignements : Microsoft, Mozilla, Apple, Google, l'industrie de la publicité en ligne par le truchement de la Digital Advertising Alliance, et le World Wide Web Consortium, organisme international de normalisation[356]. Pour discuter de son rapport, la FTC a

---

351 Federal Trade Commission (FTC), About the Federal Trade Commission.

352 FTC, « Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises », 29 novembre 2011.

353 FTC, « FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network », 30 mars 2012..

354 « Protecting Consumer Privacy in an Era of Rapid Change:Recommendations for Businesses and Policymakers », mars 2012.

355 *Ibid.*

356 *Ibid.*

comparu devant le Comité sénatorial permanent du commerce, des sciences et de la technologie[357].

VOYAGE DU COMITÉ À WASHINGTON (D.C.)

Six membres du Comité se sont rendus à Washington du 3 au 5 octobre 2012 pour y rencontrer différentes parties prenantes et approfondir leur compréhension de la question de la protection de la vie privée en lien avec les médias sociaux aux États-Unis.

A. Système juridique des États-Unis

1. Définition de vie privée

Chuck Curran, directeur exécutif au Center for Data Innovation[358], a présenté les médias sociaux comme une forme de citoyenneté numérique[359]. Le professeur Howard Beales, du département de Gestion stratégique et Politique gouvernementale de l'Université George Washington, a répondu à la question de comment définir la vie privée en mettant la notion de vie privée en relation avec les six principes suivants : le contrôle qu'exerce une personne sur l'information qui la concerne; l'équité concernant le traitement de l'information; le droit à la solitude, ou le droit de se retirer; le droit à la sécurité de sa personne; le droit à la liberté de sa personne; et le droit à la dignité [360].

2. Cadre législatif

Eric Miller, conseiller principal en politiques à l'ambassade du Canada pour Industrie Canada, a rappelé aux membres du Comité que le système juridique de protection de la vie privée aux États-Unis remonte aux années 1980 et que ses règles et normes ne répondent pas aux questions liées, par exemple à la géolocalisation et aux appareils mobiles. Il a expliqué que le gouvernement Obama a essayé de moderniser le système en publiant une « déclaration du droit à la vie privée » sous la forme d'un document intitulé *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy*[361]. Selon M. Miller, ce document atteste que de nouvelles méthodes de protection des renseignements personnels sont nécessaires compte tenu des activités de géants d'Internet comme Google et Facebook. D'après lui, la FTC assume présentement son pouvoir de

---

357 Pour le témoignage de la FTC, voir : FTC, Testimony.

358 Le *Center for Data Innovation* est une compagnie sans but lucratif basée à Washington (D.C.) qui se concentre sur les avantages offerts par les perspectives guidées par les données dans l'industrie, l'administration et la société civile. Voir : http://www.securityprivacyandthelaw.com/uploads/file/testimony_curran.pdf.

358 Chuck Curran, Center for Data Innovation, 4 octobre 2012.

359 Howard Beales, Université George Washington, 4 octobre 2012.

361 Voir : WhiteHouse, « Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy ».

réglementation faute d'un système juridique complet en matière de protection de la vie privée[362].

En recommandant au Congrès d'adopter une loi générale sur la protection de la vie privée, la FTC n'a pas proposé de formulation précise[363]. Les représentants de la FTC ont fait remarquer que 47 États étaient actuellement dotés d'une réglementation sur l'atteinte à la protection des données[364].

Marc Rotenberg, directeur exécutif à l'Electronic Privacy Information Center (EPIC), a noté que les États-Unis n'avaient pas de loi exhaustive sur la protection des renseignements personnels comme la LPRPDE : le principal instrument dont ils disposent est l'article 5 de la *Federal Trade Commission Act*[365]. Christopher Soghoian, technologue principal et analyste principal de politiques du Projet discours, vie privée et technologie à l'American Civil Liberties Union (ACLU)[366], a fait remarquer que l'expression « vie privée » n'apparaît pas dans la *Federal Trade Commission Act* et qu'il serait utile de conférer explicitement à la FTC un pouvoir en matière de protection de la vie privée[367].

D'un autre point de vue, M. Curran pense que les lacunes qui doivent être comblées devraient être identifiées avant d'envisager l'adoption d'une loi sur la protection des renseignements personnels. Il estime que les lois en vigueur sont trop facilement écartées et il a noté que des instruments non législatifs sont également disponibles. Selon lui, on doit commencer par se demander s'il existe des recours juridiques contre les actes répréhensibles visés et en quoi consiste le fondement du tort spécifique. M. Curran estime que les législateurs doivent proposer des recours précis[368].

3. Federal Trade Commission

Le principal pouvoir de la FTC découle de l'article 5 de la *Federal Trade Commission Act*. Entre autres cette disposition déclare illégales les méthodes déloyales dans le commerce ou affectant celui-ci, et les actes ou pratiques de concurrence déloyaux ou trompeurs dans le commerce ou affectant celui-ci[369]. Elle fait également en sorte que la FTC est investie du pouvoir, et instruite, d'empêcher les personnes et les entreprises, sauf certaines exceptions, d'avoir recours à des méthodes de concurrence déloyales dans le

362 Eric T. Miller, Industrie Canada, ambassade du Canada, 3 octobre 2012.

363 Markus B. Heyder, Christopher N. Olsen, Mark Eich, FTC, 4 octobre 2012.

364 *Ibid.*

365 Marc Rotenberg, Electronic Privacy Information Center, (EPIC), 4 octobre 2012. Cornell University Law School, Legal Information Institute, 15 USC § 45, http://www.law.cornell.edu/uscode/text/15/45.

366 L'American Civil Liberties Union (ACLU) est une organisation apolitique sans but lucratif dont la mission est de défendre et de préserver les droits et les libertés individuelles. L'organisation exerce ses activités par l'entremise d'actions en justice, de lobbying et d'éducation communautaire.

367 Christopher Soghoian, ACLU, 4 octobre 2012.

367 Chuck Curran, Center for Data Innovation, 4 octobre 2012.

369 15 USC § 45(a)(1).

commerce ou affectant celui-ci et les actes ou pratiques déloyaux ou trompeurs dans le commerce ou affectant celui-ci[370].

Selon les représentants de la FTC, cette disposition suppose que l'on fasse la preuve d'un préjudice important et prévoit un critère coût-avantage[371]. Ils ont expliqué que les entreprises doivent prendre des mesures de sécurité raisonnables afin de respecter cette obligation. Quant aux médias sociaux, dans le cas de Facebook et Google, ils ont reconnu que les consommateurs avaient des motifs raisonnables en vertu de cette disposition de s'attendre à ce que leurs renseignements ne soient pas communiqués[372].

L'article 5 de la *Federal Trade Commission Act* ne permet pas à la Commission d'imposer des amendes, mais elle lui permet d'émettre des ordonnances comportant des amendes : une amende civile s'élève à 16 000 $ pour chaque infraction. Les représentants de la FTC ont également insisté sur l'importance du rôle de leur direction d'application de la loi dans le cadre de ce processus[373].

Les représentants de la FTC ont rappelé aux membres du Comité que la Commission n'a pas le pouvoir de légiférer ou d'adopter de la réglementation. Ils ont expliqué que le rapport publié par la FTC en mars 2012 énonce ce qu'elle considère être des meilleures pratiques. Par la publication de ce rapport, la FTC espérait donner aux consommateurs la possibilité de faire des choix. L'idée d'une interdiction de suivi et celle de protection intégrée de la vie privée font partie de cette perspective[374].

Selon les représentants de la FTC, l'un des principaux messages qui ressortent du rapport de 2012 est le suivant : compte tenu de l'état de la technologie actuelle, on devrait veiller à la protection des données. Ils ont souligné le fait que ce message a été énoncé de manière délibérément vague afin de le rendre adaptable[375].

Une particularité du système des États-Unis est la possibilité pour la FTC de rendre publiques les enquêtes qu'elle mène sur certaines entreprises et de rendre publiques les éventuelles ententes négociées avec ces entreprises à la suite des enquêtes les concernant. M. Soghoian a d'ailleurs fait remarquer que seules les enquêtes rendues publiques par la FTC se sont soldées par des ententes[376]. Les représentants de la FTC ont exprimé le souhait que ces ententes servent d'exemple aux autres entreprises concernées par le type d'activités visées[377].

---

370 15 USC § 45(a)(2).

371 Markus B. Heyder, Christopher N. Olsen, Mark Eich, FTC, 4 octobre 2012.

372 *Ibid.*

373 *Ibid.*

374 *Ibid.*

375 *Ibid.*

376 Christopher Soghoian, ACLU,

377 Markus B. Heyder, Christopher N. Olsen, Mark Eich, FTC, 4 octobre 2012.

Les représentants de la FTC ont rappelé que les diverses enquêtes de la FTC sur Facebook, Google et MySpace ont donné lieu à des ententes[378]. Dans le cas de Facebook, ils ont expliqué que la FTC avait allégué que l'entreprise enfreignait l'article 5 de la *Federal Trade Commission Act*. La FTC a négocié une ordonnance de consentement aux termes de laquelle Facebook devait obtenir le consentement de ses utilisateurs, instaurer un programme de protection de la vie privée permettant d'évaluer les risques avec l'aide d'un spécialiste et faire vérifier son programme de protection de la vie privée.

À la lumière d'une entente conclue en août 2012 entre Facebook et la FTC, M. Miller considère que Facebook essaiera désormais de monnayer toutes les données qui transitent par l'entreprise[379]. Abondant dans le même sens, M. Rotenberg estime que Facebook sait parfaitement que le seul moyen qu'elle a de faire de l'argent est d'utiliser les données relatives à ses utilisateurs[380]. Quant aux représentantes du National Network to End Domestic Violence (NNEDV)[381], elles pensent que, maintenant que Facebook est une entreprise publique, elle cherchera des moyens de faire encore plus d'argent avec ses données[382].

M. Rotenberg estime par ailleurs que les ententes récentes attestent que Facebook n'a pas changé sa façon de faire. Il a souligné que la reconnaissance faciale est l'un des problèmes les plus importants à régler et a rappelé les questions que soulève l'association entre Facebook et Datalogix[383].

M. Rotenberg a souligné que lorsque Facebook a modifié ses caractéristiques de réglage en matière de vie privée en 2009, la FTC s'est rangée à l'opinion de l'EPIC, à savoir qu'il s'agissait d'une pratique déloyale et trompeuse selon l'article 5 de la FTC Act, et l'entente obtenue par la suite entre Facebook et la FTC découlait du pouvoir de celle-ci de faire enquête sur ce genre de pratiques[384].

En somme, M. Rotenberg estime que le rôle de la FTC est devenu crucial, puisqu'elle assume la responsabilité de protéger les consommateurs. Cependant, dès que

---

378 *Ibid.*

379 Eric T. Miller, Industrie Canada, ambassade du Canada, 3 octobre 2012.

380 Marc Rotenberg, EPIC, 4 octobre 2012.

381 Le NNEDV agit en tant que porte-parole des victimes de violence familiale et de leurs défenseurs. Il s'agit d'une organisation-cadre qui offre un appui et de la formation pour des projets spéciaux et qui collabore avec le ministère américain de la Justice. Le NNEDV s'intéresse de très près aux questions relatives à la technologie.

382 Cindy Southworth, Cynthia Fraser, NNEDV, 4 octobre 2012.

383 Marc Rotenberg, EPIC, 4 octobre 2012. Facebook a conclu une entente avec Datalogix, une entreprise de gestion de données, afin de fournir des statistiques aux annonceurs de nature à les rassurer quant à l'efficacité de leurs campagnes publicitaires sur Facebook. Voir : Alexei Oreskovic, Reuters, «Facebook's new pitch to brand advertisers: forget about clicks», 1er octobre 2012.

384 Marc Rotenberg, EPIC, 4 octobre 2012.

la FTC cesse de faire respecter ses ordonnances, les entreprises retournent à leurs pratiques antérieures[385].

B. Équilibre entre innovation et réglementation

M. Harper, directeur des études de politique d'information de l'Institut Cato[386], a fait remarquer que certains éléments de l'évolution technologique ont transformé les réseaux sociaux, comme l'usage croissant de capteurs, qui transforment un signal analogique en signal numérique, ainsi que le stockage, le traitement et le transfert des données[387]. La question de l'impact de l'évolution technologique sur les médias sociaux en appelle une autre : celle de l'équilibre entre innovation technologique et réglementation en matière de protection de la vie privée.

Selon M. Miller, de l'ambassade du Canada, le débat actuel aux États-Unis sur le rôle du gouvernement et du marché renvoie à l'idée que de solides mesures de protection de la vie privée auront pour effet d'interdire l'accès à de nouvelles technologies. Quant à savoir s'il est plus profitable ou non pour les entreprises de compter sur un système juridique prévisible, il a suggéré d'envisager l'instauration d'une norme internationale et d'analyser les répercussions de ce système projeté sur l'emploi et sur l'infonuagique[388].

Pour M. Mandel, stratège économique en chef du Progressive Policy Institute (PPI)[389], le cœur du problème est d'instaurer un équilibre entre protection de la vie privée et croissance économique. Son argument principal pour aborder cette question est que la réglementation de la protection de la vie privée et la croissance économique envisagées de pair donnent de meilleurs résultats que la seule réglementation[390].

Le véritable enjeu, selon M. Mandel, est que les pays développés ont des problèmes économiques et que le secteur d'exploitation des données y est le plus florissant. Le législateur ne devrait pas essayer d'anticiper ce que devrait être la réglementation : cela ferait obstacle à la croissance. M. Mandel estime donc que la réglementation est plus efficace lorsqu'elle est limitée le plus possible. Le problème est que, lorsque la réglementation entre en vigueur, la technologie a déjà évolué, et il est alors possible que le gouvernement empiète accidentellement sur l'innovation. Selon M. Mandel, si le secteur d'exploitation des données a pu s'épanouir, c'est justement parce qu'il n'était pas réglementé durant une décennie de réglementation couplée à un ralentissement de l'économie[391].

---

385 *Ibid.*

386 L'Institut Cato est une organisation de recherche en politiques publiques indépendant et apolitique qui s'intéresse aux principes de la liberté individuelle, du gouvernement limité, du libre marché et de la paix.

387 Jim Harper, Institut Cato, 4 octobre 2012.

388 Eric T. Miller, Industrie Canada, ambassade du Canada, 3 octobre 2012.

389 Le PPI est une organisation sans but lucratif indépendant qui fait la promotion de la croissance économique, de la sécurité nationale et d'un gouvernement axé sur le rendement.

390 Michael Mandel, PPI, 3 octobre 2012.

391 *Ibid.*

M. Schulman, conseiller en réglementation et politique gouvernementale à la Computer and Communication Industry Association (CCIA)[392], estime que la réglementation n'est pas une mauvaise chose en soi, à condition qu'elle laisse place à une saine concurrence entre les entreprises. La raison pour laquelle la réglementation de la technologie est une tâche délicate, selon lui, s'explique par le fait que la technologie est toujours en avance sur la réglementation[393].

Selon M. Curran, on ne devrait pas essayer de réglementer ce qui concerne la géolocalisation dans les nouvelles applications pour leur imposer une limite : on devrait plutôt insister sur les aspects bénéfiques de la technologie. Il a suggéré que le Comité envisage d'autres solutions que la réglementation pour tenir compte des avantages produits par l'innovation technologique[394].

Quant à lui, M. Soghoian, de l'ACLU, pense que la réglementation peut effectivement faire du tort à certains secteurs de l'économie, mais qu'elle peut en avantager d'autres : elle peut donner de l'élan à un nouveau secteur d'activité[395].

M. Schulman considère pour sa part qu'une entreprise ayant de bonnes pratiques en matière de protection de la vie privée peut avoir un avantage concurrentiel et que des produits assortis de garanties à cet égard sont en cours d'élaboration. Selon lui, on doit fournir un minimum de renseignements personnels afin d'obtenir en échange des services gratuits. Le problème serait que les gens n'aiment pas apprendre que des étrangers suivent leurs données et qu'ils ignorent comment cela se passe[396].

M. Mandel a expliqué qu'il s'inquiète plus des données recueillies par le gouvernement que des données recueillies par les entreprises privées. Il estime que les entreprises sont vulnérables, puisqu'elles doivent payer le prix de leurs erreurs. Le gouvernement, lui, jouit d'un pouvoir coercitif qui, conjugué à l'accès à des données, devient dangereux. M. Mandel a proposé l'exemple des bureaux de crédit, qui ont l'obligation de permettre aux consommateurs de consulter leur dossier de crédit, gratuitement, une fois par an. Il serait utile, selon lui, qu'une forme d'autoréglementation du même ordre s'applique au secteur d'exploitation des données pour que les consommateurs aient accès à leurs dossiers de renseignements personnels[397].

James Cooper, directeur, recherche et politique, du Law & Economics Center à l'Université George Mason[398], est d'avis que la politique sur la protection de la vie privée

---

392 La CCIA est une organisation sans but lucratif qui regroupe un large éventail d'entreprises dans le secteur de l'informatique, d'Internet, de la technologie de l'information et des télécommunications. La CCIA cherche à protéger et à promouvoir les intérêts des industries qu'elle représente.

393 Ross Schulman, CCIA, 4 octobre 2012.

394 Chuck Curran, directeur exécutif, Center for Data Innovation, 4 octobre 2012.

395 Christopher Soghoian, ACLU, 4 octobre 2012.

396 Ross Schulman, CCIA, 4 octobre 2012.

397 Michael Mandel, PPI, 3 octobre 2012.

398 Le Law & Economics Center, (LEC), de la Faculté de droit de l'Université George Mason est un centre national de recherche et d'enseignement qui se penche principalement sur l'analyse économique de questions d'ordre juridique relatives aux politiques publiques.

doit porter sur les torts causés et se fonder sur des preuves empiriques. Le premier volet d'une bonne réglementation devrait consister en une définition des pratiques déloyales en vigueur et des torts effectivement causés. Le deuxième volet consisterait à s'interroger sur ce qui pourrait faire l'objet de poursuites à partir de preuves empiriques. Il estime que l'ampleur des torts éventuels permettra de déterminer ce que peut être une pratique raisonnable[399].

Dans le même ordre d'idée, M. Harper, de l'Institut Cato, est d'avis qu'on devrait laisser les gens décider de ce qui importe à leurs yeux en matière de protection de la vie privée. Dans l'échange qui se fait entre vie privée et nouvelle technologie, nous devrions nous intéresser aux torts effectifs[400].

C. Collecte, utilisation et communication de l'information

Selon M. Rotenberg, les entreprises préfèrent croire qu'elles peuvent faire ce qu'elles veulent de l'information qu'elles utilisent parce que celle-ci est rendue publique. Il estime quant à lui que le fait que l'information soit publique ne signifie pas que l'intéressé a perdu tout intérêt pour ses renseignements personnels[401].

Howard Beales, de l'Université George Washington, a expliqué que les données recueillies dans le cadre d'une transaction entre un consommateur et une entreprise soulèvent le problème, en matière de protection de la vie privée, de l'utilisation de ces données. Selon lui, des règles générales sont plus faciles à comprendre pour les consommateurs et incitent les entreprises à s'y conformer. Il pense que la réglementation ne devrait pas faire obstacle aux entreprises, parce que c'est la concurrence entre les réseaux sociaux qui les disciplinera. Il a insisté sur le fait que les données dont les entreprises disposent sont celles que les consommateurs acceptent de rendre publiques[402].

Concernant les politiques de protection de la vie privée, M. Rotenberg a expliqué qu'il a beaucoup été question de « courts préavis », mais que cette idée ne le convainc pas parce qu'on n'a pas affaire à des mesures fixes et que les entreprises modifient sans arrêt leurs politiques. Il pense que la meilleure stratégie est la protection intégrée de la vie privée (« Privacy by Design »)[403].

Les représentantes du NNEDV ont aussi insisté sur cette notion de protection intégrée de la vie privée par défaut, dont l'absence selon elles signifie que les survivantes perdent leurs droits civils, ce qui aurait aussi des effets sur leurs enfants. Elles estiment qu'il y a lieu de soulever la question du consentement éclairé et de s'interroger sur le risque accru que représentent la géolocalisation et le chiffrement biométrique à cet égard.

---

399 James C. Cooper, Université George Mason, 4 octobre 2012.

400 Jim Harper, Institut Cato, 4 octobre 2012.

401 Marc Rotenberg, EPIC, 4 octobre 2012.

402 Howard Beales, Université George Washington, 4 octobre 2012.

403 Marc Rotenberg, EPIC, 4 octobre 2012.

Elles considèrent que la *Children's Online Privacy Protection Act* (COPPA) doit être mise à jour compte tenu de ces éléments[404].

D. Responsabilité et transparence

Les représentants de la FTC ont expliqué que la Commission avait recommandé des mesures législatives concernant les courtiers en données autour de l'idée d'un site Web centralisé. Ces mesures permettraient d'améliorer la transparence et de braquer les projecteurs sur les courtiers en données, car beaucoup de ces entreprises sont inconnues du public. Il s'agirait de créer une liste de ces entreprises afin que les consommateurs puissent faire des choix plus éclairés, étant donné l'accroissement dans la collecte de renseignements[405].

M. Soghoian estime pour sa part que les courtiers en données ne sont pas responsabilisés, parce que les consommateurs ne les connaissent pas. Ces entreprises affirment que leurs activités sont inoffensives parce que les données sont anonymes. Selon lui, cette déclaration est de plus en plus fausse. Il a expliqué que, lorsqu'on consulte un site Web, des enchères sont aussitôt lancées (à la microseconde près) à l'intention des réseaux de publicité : le soumissionnaire qui offre le meilleur prix a aussitôt la possibilité de placer une annonce. M. Soghoian estime que les consommateurs devraient pouvoir disposer de produits sûrs en dehors de leur utilisation et que la collecte de données à long terme aura des effets que personne ne peut vraiment prévoir[406].

Selon M. Beales, le modèle d'affaires principal des réseaux sociaux d'aujourd'hui est le financement publicitaire. Il estime que la publicité, notamment la publicité comportementale, permet de financer des produits gratuits et qu'il est important que la réglementation n'en réduise pas la valeur. M. Beales considère d'ailleurs que la publicité ciblée est sans danger[407].

Dans le même ordre d'idées, M. Mandel a fait le lien entre la façon dont les annonceurs publicitaires payaient autrefois pour des publicités à la télévision et dans les journaux et la méthode qu'ils emploient aujourd'hui pour faire de la publicité en ligne[408]. Quant à lui, M. Curran estime que les annonceurs achètent des auditoires : ils ne s'intéressent pas aux renseignements personnels proprement dits[409].

M. Harper pense que les entreprises n'échangent pas d'énormes listes de renseignements personnels. Il a rappelé qu'il existe des degrés de contrôle et qu'il est possible de désactiver les témoins (« cookies ») des sites Web pour éviter de recevoir de la publicité ciblée[410]. Selon M. Beales, il est impossible d'obtenir une transparence

404 Cindy Southworth, Cynthia Fraser,NNEDV, 4 octobre 2012.

405 Markus B. Heyder, Christopher N. Olsen, Mark Eich,FTC, 4 octobre 2012.

406 Christopher Soghoian, ACLU, 4 octobre 2012.

407 Howard Beales, Université George Washington, 4 octobre 2012.

408 Michael Mandel, PPI, 3 octobre 2012.

409 Chuck Curran, Center for Data Innovation, 4 octobre 2012.

410 Jim Harper, Institut Cato, 4 octobre 2012.

complète du côté des agrégateurs de données. D'ailleurs, il ne croit pas que les consommateurs aient besoin de savoir que certaines entreprises regroupent l'information[411].

E. Consentement

Au sujet des contrats liant les consommateurs aux entreprises, la FTC incite les entreprises à divulguer des renseignements aux consommateurs de façon plus claire, les poussant à innover en ce sens. La politique de protection de la vie privée applicable aux appareils mobiles est un problème plus compliqué. La FTC a fait la promotion de l'idée d'icônes accompagnées d'un court texte et elle travaille dans cette direction avec des développeurs de plateformes, comme Apple[412].

M. Schulman de la CCIA, estime que les politiques de protection de la vie privée devraient être plus conviviales pour les utilisateurs. Il a souligné que les entreprises savent depuis 10 ans qu'elles doivent se doter d'une politique de protection de la vie privée, mais qu'elles élaborent désormais leurs produits selon le principe de la protection intégrée de la vie privée[413].

M. Harper estime quant à lui que la tâche d'éduquer les consommateurs est importante, mais difficile. Personne ne lit les politiques concernant la protection de la vie privée : les consommateurs veulent aller rapidement à ce qu'ils désirent[414].

M. Soghoian a soulevé la question de l'absence de choix pour les utilisateurs d'appareils mobiles en matière de réglages pour la protection de leurs renseignements : leur seul choix consiste à prendre ou à laisser[415]. Selon les représentantes du NNEDV, les utilisateurs ne devraient pas être contraints de choisir entre activer ou désactiver les contrôles relatifs à la vie privée. Ces mécanismes devraient être intégrés. De grandes entreprises comme Google et Facebook doivent tenir compte de la réputation qu'ils tiennent à conserver, alors que de petites entreprises sont largement inconnues du public et ne risquent pas de perdre leur réputation. Le problème le plus important est de contrôler les répercussions de la production d'applications par de petites entreprises[416].

F. Sécurité

M. Soghoian a remarqué que les responsables politiques américains semblent penser qu'ils doivent choisir entre sécurité de la personne et protection de la vie privée. Selon lui, c'est une fausse alternative : il s'agirait plutôt d'une question de sécurité

411 Howard Beales, Université George Washington, 4 octobre 2012.

412 Markus B. Heyder, Christopher N. Olsen, Mark Eich, FTC, 4 octobre 2012.

413 Ross Schulman, CCIA4 octobre 2012.

414 Jim Harper, Institut Cato, 4 octobre 2012.

415 Christopher Soghoian, ACLU, 4 octobre 2012.

416 Cindy Southworth, Cynthia Fraser,NNEDV, 4 octobre 2012.

nationale (étant donné que la sécurité des renseignements personnels n'est pas assurée et donc qu'on ne peut contrôler l'accès à ceux-ci)[417].

M. Rotenberg, de l'EPIC, a expliqué que le seul domaine où il existe une loi exhaustive sur la protection de la vie privée aux États-Unis est celui de la protection des enfants, avec COPPA, et que le secteur privé n'est pas d'accord avec toutes les restrictions qui lui sont imposées à cet égard. Selon lui, la réglementation de la protection de la vie privée devrait contraindre ceux qui recueillent des données à un plus grand sens des responsabilités[418]. Au sujet de l'application de COPPA, Eric Miller, de l'ambassade canadienne, a précisé que la FTC exige le consentement des parents pour la géolocalisation des enfants et les protège contre la publicité ciblée[419].

M. Mandel estime quant à lui qu'il y a deux façons de considérer la nouvelle génération d'applications, par exemple celles qui utilisent la géolocalisation : on peut l'envisager soit comme une innovation dangereuse, soit comme un moyen d'obtenir des renseignements intéressants sur soi-même. Selon lui, en partant de la prémisse que l'entrave à l'innovation est une entrave à la croissance économique, un pays doté d'un très solide système de protection de la vie privée fait obstacle à l'innovation et risque de prendre du retard sur le plan économique. Interrogé sur le rôle du législateur à cet égard, M. Mandel a répondu par une autre question : que pourrait-il bien arriver de pire? Il a rappelé la question de la protection des enfants, faisant remarquer qu'il est facile de désactiver les fonctions de suivi sur les appareils mobiles, de supprimer les témoins, etc[420].

Par ailleurs, les représentantes du NNEDV ont expliqué que certaines entreprises les consultent lorsqu'elles élaborent leurs produits. Par exemple, Google les a consultées pour s'assurer qu'aucun refuge n'apparaitrait sur les produits Google Street View et Google Maps. Twitter les a également consultées pour s'assurer que les communications faites sur son réseau étaient protégées[421].

Les représentantes du NNEDV ont insisté sur le fait que la technologie peut servir à faire violence non seulement aux femmes, mais aussi aux enfants et aux personnes handicapées. Selon elles, la technologie offre, d'un côté, des possibilités plus larges, mais, de l'autre, accroît les risques[422]. Selon les représentantes du NNEDV, le problème est que, d'une part, les innovations associées aux médias sociaux, comme la géolocalisation sur les téléphones mobiles, représentent une menace pour la sécurité des femmes victimes de violence conjugale. D'autre part, les médias sociaux sont pour les victimes isolées un moyen de renouer avec d'autres personnes. C'est pourquoi le NNEDV estime que les femmes doivent prendre garde lorsqu'elles utilisent des médiaux sociaux, mais

417 Christopher Soghoian, ACLU, 4 octobre 2012.

418 Marc Rotenberg, EPIC, 4 octobre 2012.

419 Eric T. Miller, Industrie Canada, ambassade du Canada, 3 octobre 2012.

420 Michael Mandel, PPI, 3 octobre 2012.

421 Cindy Southworth, Cynthia Fraser, NNEDV, 4 octobre 2012.

422 *Ibid.*

qu'il n'est pas indiqué pour autant de les inviter à ne pas utiliser l'Internet, parce que cela aurait pour effet de les isoler davantage[423].

Les représentantes du NNEDV ont expliqué qu'il est possible de retracer un conjoint par courriel ou au moyen d'un logiciel espion, qui est une application enregistrant absolument tout. Elles ont parlé du projet Safety Net, qui a trait aux effets de la technologie sur la violence conjugale. Safety Net est un partenaire de la CIPPIC à Ottawa et a obtenu une subvention du CPVP. Ce projet témoigne de la façon dont la violence peut se produire dans le monde numérique et dont la technologie peut servir à diverses étapes de la violence[424].

Regardant de l'autre côté de la lorgnette, M. Soghoian a expliqué que les services de police peuvent désormais suivre des gens par géolocalisation ou en demandant à Google, par exemple, de leur fournir un exemplaire de leur boîte de réception[425].

Les représentantes du NNEDV ont également soulevé la question de l'anonymat et de l'adoption de pseudonymes, qui peuvent être de puissants instruments[426]. M. Rotenberg, de l'EPIC, a expliqué que, même si les consommateurs ne sont pas opposés à l'innovation, leur crainte principale est le vol d'identité. Il a rappelé le rôle important que doivent jouer les législateurs dans la protection des droits fondamentaux, dont le droit à la vie privée. Selon lui, les utilisateurs ne peuvent pas régler ces problèmes par eux-mêmes : même un utilisateur attentif ne peut se fier aux affirmations des entreprises. En ce sens, M. Rotenberg a mentionné la possibilité d'imposer aux entreprises, au moyen d'une loi, l'obligation de s'auto-réglementer[427].

En ce qui concerne un autre secteur où l'utilisation des renseignements personnels est particulièrement délicate, le secteur médical, M. Mandel estime que l'innovation médicale aux États-Unis est morcelée parce que le cadre de réglementation est trop strict. En réponse aux questions des membres du Comité concernant le secteur dans lequel il estimerait justifié d'intervenir sur le plan juridique, il a répondu : le secteur médical[428].

G. Droit d'être oublié

M. Miller a expliqué que, pendant que les Européens s'intéressent au « droit d'être oublié », ou « droit à l'oubli numérique[429] », les règles en vigueur aux États-Unis ne

---

423 *Ibid.*

424 *Ibid.*

425 Christopher Soghoian, ACLU, 4 octobre 2012.

426 Cindy Southworth, Cynthia Fraser, NNEDV, 4 octobre 2012.

427 Marc Rotenberg, EPIC, 4 octobre 2012.

428 Michael Mandel, PPI, 3 octobre 2012.

429 Voir : Commission européenne, communiqué de presse, « La Commission propose une réforme globale des règles en matière de protection des données pour accroître la maîtrise que les utilisateurs ont sur leurs données et réduire les coûts grevant les entreprises », 25 janvier 2012..

permettent pas de régler les questions liées, d'une part, à la protection de la vie privée et, d'autre part, à la liberté d'expression et à d'autres droits[430].

M. Rotenberg a fait valoir que l'EPIC collabore étroitement avec des organisations vouées à la protection de la vie privée dans le monde entier et qu'ils partagent tous les mêmes préoccupations. Il a fait remarquer qu'au sein de l'UE, le processus d'uniformisation de la réglementation est en cours depuis une vingtaine d'années et que le passage prochain de la Directive en Règlement[431] sera une étape importante : il n'y aura plus qu'une seule réglementation applicable au lieu de 27. Il a également signalé qu'aux États-Unis, l'infonuagique donne accès à des renseignements plus difficiles à contrôler, puisque les données sont stockées dans d'autres pays[432].

Rappelant pour leur part l'importance du « droit d'être oublié » des victimes de violence conjugale, les représentantes du NNEDV ont suggéré que la réglementation sur la protection de la vie privée et la technologie devrait être de nature générale afin qu'elle puisse rester applicable à mesure que la technologie évolue. Elles ont fait remarquer que Facebook est en train d'élaborer une énorme base de photos étiquetées avec reconnaissance faciale[433].

M. Harper a expliqué que, dès qu'une personne inscrit de l'information dans le système, il devient très difficile de la récupérer et de sortir du système. Il a comparé la notion européenne du « droit d'être oublié » à essayer de nager contre le courant d'une rivière[434].

H. Interdiction de suivi

M. Miller a noté que la FTC a déployé beaucoup d'efforts pour contraindre les entreprises à ajouter une rubrique d'interdiction de suivi (« do not track ») à leurs produits et qu'elle fait la même chose pour la protection des enfants[435].

Les questions liées à la protection de la vie privée sont de plus en plus présentes, mais, selon James Cooper, du Law & Economics Center de l'Université George Mason, rien n'indique qu'il existe une crise justifiant l'intervention du gouvernement. Il estime par ailleurs que la notion d'interdiction de suivi est prématurée, car le marché est capable de s'en charger[436].

---

430 Eric T. Miller, Industrie Canadaambassade du Canada, 3 octobre 2012.

431 Voir : Commission européenne, communiqué de presse, « La Commission propose une réforme globale des règles en matière de protection des données pour accroître la maîtrise que les utilisateurs ont sur leurs données et réduire les coûts grevant les entreprises », 25 janvier 2012.

432 Marc Rotenberg, EPIC, 4 octobre 2012.

433 Cindy Southworth, Cynthia Fraser, NNEDV, 4 octobre 2012.

434 Jim Harper, , Institut Cato, 4 octobre 2012.

435 Eric T. Miller, Industrie Canada, ambassade du Canada, 3 octobre 2012.

436 James C. Cooper, Université George Mason, 4 octobre 2012.

D'un autre point de vue, M. Soghoian considère que l'interdiction de suivi lance un signal clair en matière de consentement : cela permet à la FTC d'agir et contraint les entreprises à réagir, sans que l'adoption de réglementation soit nécessaire[437].

I. Pouvoirs de la Commissaire à la protection de la vie privée du Canada

Les représentantes du NNEDV ont fait remarquer que, même si Google et Facebook ont réagi correctement aux enquêtes du CPVP, les petites entreprises doivent, elles aussi, être imputables. Elles ont souligné la difficulté à obtenir des renseignements auprès d'une entreprise située à l'extérieur du Canada. Elles ont également suggéré au Comité de se pencher sur la portée de l'influence de la commissaire et ont argué que cette dernière devrait avoir le pouvoir d'imposer des amendes aux entreprises[438].

M. Rotenberg, de l'EPIC, a insisté sur la qualité du travail accompli par la commissaire à la protection de la vie privée du Canada Jennifer Stoddart. Il a notamment suggéré qu'elle devrait avoir le pouvoir de rendre des ordonnances[439]. M. Soghoian, de l'ACLU, a également fait l'éloge du travail de la commissaire Stoddart, qui, a-t-il précisé, fait l'envie du monde entier. Il a recommandé que la commissaire à la protection de la vie privée du Canada soit dotée du pouvoir d'imposer des sanctions monétaires[440].

437 Christopher Soghoian, ACLU, 4 octobre 2012.

438 Cindy Southworth, Cynthia Fraser, NNEDV, 4 octobre 2012.

439 Marc Rotenberg, EPIC, 4 octobre 2012.

440 Christopher Soghoian, ACLU, 4 octobre 2012.

ANNEXE A — COMPARAISON DES DÉFINITIONS DANS LES CONDITIONS ET POLITIQUES DE CONFIDENTIALITÉ DES MÉDIAS SOCIAUX*

	Définition de "renseignement personnel" ou l'équivalent
PIPEDA	« Tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresse et numéro de téléphone de son lieu de travail. » s.2(1)
Facebook	Par « Informations », nous entendons les faits et autres informations vous concernant, notamment les actions des autres utilisateurs et des non utilisateurs qui interagissent avec Facebook. Par « contenu », nous entendons le contenu et les informations que vous ou d'autres utilisateurs publiez sur Facebook, qui ne répondraient pas à la définition d'informations. Par « données » ou « données utilisateur », nous entendons toute donnée, y compris le contenu ou les informations d'un utilisateur que vous ou un tiers peut récupérer sur Facebook ou fournir à Facebook au moyen de la plate-forme. (Déclaration des droits et responsabilités, s.18, consulté le 15 juin, 2012)
Google+	**« Renseignements personnels :** Il s'agit de renseignements que vous nous avez fournis qui peuvent vous identifier personnellement comme votre nom, votre adresse de courriel, votre adresse de facturation ou toute autre donnée susceptible d'être associée à ce type de renseignement par Google. **Renseignements personnels et confidentiels :** Il s'agit de renseignements personnels en lien avec l'état de santé, l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou la sexualité d'une personne. **Renseignements non personnels :** Il s'agit de renseignements enregistrés au sujet de l'utilisateur de manière à ce qu'ils ne permettent plus d'identifier un utilisateur ou de faire référence à celui-ci de manière personnelle. » (Politique de confidentialité, mots clés, consulté le 15 juin, 2012)
LinkedIn	« Veuillez noter que certaines informations, déclarations, données et certains contenus (tels que les photographies) que vous pouvez fournir à LinkedIn ou les groupes dont vous pouvez faire partie, peuvent potentiellement révéler **votre sexe, origine ethnique, nationalité, âge et/ou orientation sexuelle, et/ou toute autre information vous concernant.** » (Conditions d'utilisation, 2.K, consulté le 15 juin, 2012)

* Source : Par: Centre pour la défense de l'intérêt public (CRDP) – 18 octobre 2012.

Nexopia	*Non-disponible en français*
Twitter	**« Informations collectées au moment de l'enregistrement** : quand vous créez ou reconfigurez un compte Twitter, vous nous fournissez des informations personnelles telles que votre nom, votre nom d'utilisateur, votre mot de passe et votre adresse de courrier électronique. » **« Données non privées et ou non personnelles** : nous pouvons partager et divulguer vos données qui ne sont pas privées ou qui sont agrégées ou qui sont rendues autrement anonymes, telles que les informations de votre profil public, vos Tweets publics, les personnes que vous suivez ou qui vous suivent ou le nombre d'utilisateurs qui ont cliqués sur un lien particulier (même si une seule personne l'a fait). » (Politique de Confidentialité, consulté le 15 juin, 2012)

ANNEXE B — POUVOIRS D'EXÉCUTION EN VERTU DES LOIS INTERNATIONALES SUR LA PROTECTION DE LA VIE PRIVÉE*

Organisation de protection de la vie privée et lois sur la protection de la vie privée	Année à laquelle l'organisation a acquis ses plus récents pouvoirs d'exécution en vertu d'une loi ou d'un amendement	Pouvoir de rendre des ordonnances et responsabilité	Dommages-intérêts d'origine législative et sanctions
Canada CPVP *LPRPDE*	2000	N'a pas le pouvoir de rendre des ordonnances. Peut ouvrir une enquête sur les plaintes ou amorcer une vérification s'il existe des motifs raisonnables de croire que l'organisation contrevient à la LPRPDE. A le pouvoir de recueillir des éléments de preuve et d'entrer sur les lieux.	N'a pas le pouvoir d'imposer une amende ni d'accorder des dommages-intérêts. Doit se présenter devant la Cour fédérale pour donner suite aux constatations.
France Commission nationale de l'informatique et des libertés (CNIL) *Loi relative à l'informatique, aux fichiers et aux libertés* (LIL)	2004	Peut imposer une décision[441]. Doit informer l'entreprise avant d'entrer sur les lieux et de commencer l'enquête. Doit obtenir une autorisation de la cour pour faire enquête si l'organisation s'y objecte au départ.	Peut imposer une amende allant de 10 000 à 50 000 € si un manquement à la sécurité est constaté après une évaluation de conformité. En vertu du *Code criminel*, une amende ne dépassant pas 300 000 € et une peine d'incarcération de 5 ans dans le cas d'un particulier et une amende de 1 500 000 € dans le cas d'une personne morale peut être imposée pour manque de protection.

* Le contenu de ce tableau est tiré en totalité (à moins d'indication contraire) de Baker et McKenzie, « Global Privacy Handbook 2011 », IAPP, 2011, 389 pages.

441 Site Web officiel de la CNIL.

Organisation de protection de la vie privée et lois sur la protection de la vie privée	Année à laquelle l'organisation a acquis ses plus récents pouvoirs d'exécution en vertu d'une loi ou d'un amendement	Pouvoir de rendre des ordonnances et responsabilité	Dommages-intérêts d'origine législative et sanctions
Allemagne Commissaire fédéral à la protection des données et à l'accès à l'information *Loi fédérale sur la protection des données d'Allemagne* (BDSG)	2009	Le commissaire supervise les entreprises de télécommunications et de services postaux. La surveillance de la protection des données dans d'autres sphères du secteur privé incombe aux États. Avis de manquement à la sécurité obligatoire Peut ordonner aux organisations de remédier aux manquements à l'observation.	• A le pouvoir d'imposer une amende de 300 000 € à une organisation pour non-observation des règles sur la protection des données. • Des amendes plus lourdes peuvent être imposées si des bénéfices commerciaux ont été réalisés à la suite d'une infraction.
Irlande Commissaire à la protection des données *Data Protection Act* (loi sur la protection des données)	2003	A le pouvoir d'obtenir des renseignements. A le pouvoir de faire observer. Peut nommer un « agent autorisé » chargé d'entrer sur les lieux d'une organisation et d'effectuer un examen. Peut introduire une instance et mener des poursuites (procédure sommaire).	A le pouvoir d'imposer une amende maximale de 3 000 € sur déclaration de culpabilité par procédure sommaire. Sur déclaration de culpabilité par mise en accusation, la sanction maximale est une amende de 100 000 €[442].
Espagne Agence espagnole de protection des données *Loi espagnole sur la protection des données*	2011	A le pouvoir de rendre des ordonnances, y compris la destruction des données et du matériel d'entreposage de données. Aucune exigence en matière d'avis de manquement.	A le pouvoir d'imposer des sanctions applicables à trois catégories d'infractions, soit mineure, grave et très grave, pouvant faire l'objet d'amendes allant de 600 à 600 000 €.

442 Site Web officiel du commissaire à la protection des données d'Irlande.

Organisation de protection de la vie privée et lois sur la protection de la vie privée	Année à laquelle l'organisation a acquis ses plus récents pouvoirs d'exécution en vertu d'une loi ou d'un amendement	Pouvoir de rendre des ordonnances et responsabilité	Dommages-intérêts d'origine législative et sanctions
Royaume-Uni Bureau du commissaire à l'information *Data Protection Act* (loi sur la protection des données)	2010	A le pouvoir d'imposer des sanctions pécuniaires et de produire des avis d'évaluation. Peut effectuer des vérifications dans le secteur privé mais seulement avec le consentement de l'organisation. Dans le cadre de certaines enquêtes, a le pouvoir d'entrer sur les lieux sans préavis, au besoin en vertu d'un mandat judiciaire. Peut mener ses propres poursuites devant la cour pénale en Angleterre, au Pays de Galles et en Irlande du Nord.	A le pouvoir d'imposer une amende maximale de 500 000 £ aux organisations en cas de manquement grave à la protection des données.

Organisation de protection de la vie privée et lois sur la protection de la vie privée	Année à laquelle l'organisation a acquis ses plus récents pouvoirs d'exécution en vertu d'une loi ou d'un amendement	Pouvoir de rendre des ordonnances et responsabilité	Dommages-intérêts d'origine législative et sanctions
États-Unis d'Amérique Commission fédérale du commerce *Federal Trade Commission Act* (loi sur la commission fédérale du commerce)	1938 (la loi sur la commission fédérale du commerce de 1914 a été modifiée de manière à prévoir des amendes administratives en cas de non-respect des ordonnances rendues en vertu de l'article 5)[443]	A le pouvoir d'assigner des témoins et d'exiger la production de documents. Peut exiger le dépôt de rapports annuels ou spéciaux afin d'obtenir des renseignements sur une organisation, des pratiques et la direction. Peut tenir un procès administratif ou porter l'affaire devant les tribunaux. Peut prescrire des règles définissant les pratiques déloyales ou trompeuses. Peut demander réparation en cas de préjudice causé au consommateur.	Peut demander, avec l'aide des tribunaux, des amendes administratives en cas de non-observation d'une ordonnance définitive de cesser et de s'abstenir à la suite d'un procès administratif.

443 Site Web officiel de la commission fédérale du commerce des États-Unis.

Organisation de protection de la vie privée et lois sur la protection de la vie privée	Année à laquelle l'organisation a acquis ses plus récents pouvoirs d'exécution en vertu d'une loi ou d'un amendement	Pouvoir de rendre des ordonnances et responsabilité	Dommages-intérêts d'origine législative et sanctions
Australie Bureau du commissaire à l'information d'Australie (ADOPTÉ MAIS ENTRERA EN VIGUEUR SEULEMENT EN MARS 2014) *Enhancing Privacy Protection* (meilleure protection des renseignements personnels)	Le projet de loi modifie la *Privacy Act of 1988* (loi sur la protection des renseignements personnels de 1988).	Le commissaire aura le pouvoir d'effectuer des évaluations de la protection des renseignements personnels dans les organisations du secteur privé et dans les organismes gouvernementaux. Le commissaire sera habilité à prendre une décision exécutoire à la suite d'une enquête menée de sa propre initiative. Le commissaire pourra accepter un engagement écrit de la part d'une entité dans lequel celle-ci s'engage à prendre une mesure précise ou à s'en abstenir.	Le commissaire pourra imposer une amende administrative maximale de 1 100 000 $ en cas d'ingérence grave ou d'ingérences répétées dans la vie privée. Si le commissaire est d'avis qu'une organisation n'a pas respecté un engagement, il peut demander à la cour une ordonnance pour obliger celle-ci à respecter son engagement[444].

444 Site Web officiel du Bureau du commissaire à l'information d'Australie.

Organisation de protection de la vie privée et lois sur la protection de la vie privée	Année à laquelle l'organisation a acquis ses plus récents pouvoirs d'exécution en vertu d'une loi ou d'un amendement	Pouvoir de rendre des ordonnances et responsabilité	Dommages-intérêts d'origine législative et sanctions
Union européenne Commission européenne (PROPOSÉ) *Règlement général sur la protection des données*	Actuellement à l'étude	Les autorités chargées de la protection des données ont toutes le pouvoir d'émettre des ordonnances pour faire cesser des activités précises, corriger des données, effacer des données ou détruire des données et donner accès aux particuliers à leurs renseignements personnels. De même, elles seront habilitées à faire enquête pour obtenir du responsable du contrôle ou du traitement : (a) l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires à l'exercice de ses fonctions; (b) l'accès à tous les locaux, y compris tous les équipements et moyens de traitement des données, s'il existe un motif raisonnable de supposer que s'y exerce une activité en violation du présent règlement.	Le règlement précise que chaque autorité de contrôle est habilitée à imposer des sanctions administratives, y compris un avertissement lors d'un premier manquement non intentionnel au règlement et jusqu'à trois niveaux d'amendes : une amende maximale de 250 000 € (dans le cas des organisations gouvernementales ou sans but lucratif) ou une amende maximale équivalent à 0,5 % du chiffre d'affaires annuel mondial de l'organisation (dans le cas des entreprises); une amende maximale de 500 000 € (dans le cas des organisations gouvernementales ou sans but lucratif) ou une amende maximale équivalent à 1% du chiffre d'affaires annuel mondial (dans le cas des entreprises); une amende maximale de 1 000 000 € (dans le cas des organisations gouvernementales ou sans but lucratif) ou une amende maximale équivalent à 2 % du chiffre d'affaires annuel mondial (dans le cas des entreprises)[445].

445 Site Web officiel de la Commission européenne.

LISTE DES RECOMMANDATIONS

ANNEXE C
LISTE DES TÉMOINS

Organismes et individus	Date	Réunion
Ministère de l'Industrie	2012/05/29	41
Janet Goulding, directrice générale Direction générale de la gouvernance, de la coordination de la politique et de la planification		
Jill Paterson, conseillère en politiques Direction de la sécurité et la protection des renseignements personnels		
Bruce Wallace, directeur Direction de la sécurité et la protection des renseignements personnels		
Commissariat à la protection de la vie privée du Canada		
Barbara Bucknell, analyste en politiques stratégiques Direction des services juridiques, des politiques et des recherches		
Daniel Caron, conseiller juridique Direction des services juridiques, des politiques et des affaires parlementaires		
Jennifer Stoddart, commissaire à la protection de la vie privée du canada		
Université d'Ottawa	2012/05/31	42
Michael Geist, titulaire de la chaire de recherche du canada en droit d'internet et du commerce électronique		
Teresa Scassa, chaire de recherche du canada en droit de l'information Faculté de droit, section de common law		
Valerie Steeves, professeure associé Département de criminologie		
Chambre de commerce du Canada	2012/06/05	43
Warren Everson, vice-président principal Politiques		
Association de la recherche et de l'intelligence marketing		
Annie Pettit, vice-présidente		
Brendan Wycks, directeur exécutif		
Bureau du commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique	2012/06/07	44
Elizabeth Denham, commissaire		

Organismes et individus	Date	Réunion
Bureau du commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique	2012/06/07	44
Caitlin Lemiski, analyste des politiques		
Helen Morrison, analyste senior des politiques		
Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario		
Ann Cavoukian, commissaire		
Michelle Chibba, directrice des politiques		
David Goodis, directeur des services juridiques		
Ryerson University	2012/06/12	45
Avner Levin, professeur associé et directeur Institut de la cybercriminalité et de la vie privée		
Université de Montréal		
Vincent Gautrais, professeur titulaire		
Université d'Ottawa		
Ian Kerr, chaire de recherche du Canada en éthique, en droit et en technologie		
Clinique d'intérêt public et de politique d'Internet du Canada	2012/06/19	46
Tamir Israel, avocat-conseil à l'interne		
Heenan Blaikie		
Adam Kardash, directeur général Access Privacy		
University of Toronto		
Sara Grimes, professeure adjointe Faculté de l'information		
À titre personnel	2012/10/16	50
Pierrôt Péladeau, chercheur et conseil Évaluation sociale de systèmes d'information		
Association canadienne du marketing		
David Elder, conseiller juridique spécial, protection des renseignements personnels numériques		
Merchant Law Group		
Jason Zushman, avocat		
Centre pour la défense de l'intérêt public	2012/10/18	51
John Lawford, directeur exécutif et avocat général		

Organismes et individus	Date	Réunion
Google inc.	2012/10/30	53
Colin McKay, gestionnaire responsable des politiques Google Canada		
HabilioMédias	2012/11/01	54
Matthew Johnson, directeur de l'éducation		
Jane Tallim, codirectrice exécutive		
University of Victoria		
Colin J. Bennett, professeur		
Nexopia.com Inc.	2012/11/06	55
Kevin Bartus, chef de la direction		
Mark Hayes, directeur général Heydary Hayes PC		
Association canadienne de la technologie de l'information	2012/11/20	56
Karna Gupta, président et directeur général		
TÉLUQ		
Normand Landry, professeur		
Facebook, inc.	2012/11/27	57
Robert Sherman, directeur Protection des renseignements personnels et politiques publiques		
Acxiom	2012/12/06	58
Jennifer Barrett Glasgow, responsable de la protection des renseignements personnels et des politiques publiques		
Twitter inc.		
Laura Pirri, conseillère juridique		
BlueKai Inc.	2012/12/11	59
Alan Chapell, conseiller juridique externe, responsable de la protection de la vie privée		
Commissariat à la protection de la vie privée du Canada		
Chantal Bernier, commissaire adjointe à la protection de la vie privée		
Barbara Bucknell, analyste en politiques stratégiques Direction des services juridiques, des politiques et des recherches		

Organismes et individus	Date	Réunion
Commissariat à la protection de la vie privée du Canada	2012/12/11	59
Jennifer Stoddart, commissaire à la protection de la vie privée du canada		

ANNEXE D
LISTE DES MÉMOIRES

Organismes et individus
Association de la recherche et de l'intelligence marketing
BC Freedom of Information and Privacy Association
Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario
Centre pour la défense de l'intérêt public
Facebook inc.
Landry, Normand et Leslie Regan Shade
Levin, Avner (Ryerson University)
Parsons, Christopher

ANNEXE E
RÉUNIONS AVEC DES INDIVIDUS ET DES ORGANISATIONS À WASHINGTON 3 AU 5 OCTOBRE 2012

Organisations et individus	Date
Industrie Canada	2012/10/03
Eric Miller, conseiller	
Progressive Policy Institute (PPI)	
Michael Mandel, stratège économique en chef	
American Civil Liberties Union (ACLU)	2012/10/04
Christopher Soghoian, technologue principal et analyste principal de politiques du Projet discours, vie privée et technologie	
Computer and Communication Industry Association (CCIA)	
Ross Schulman, conseiller en réglementation et politique gouvernementale	
Electronic Privacy Information Center (EPIC)	
Marc Rotenberg, directeur exécutif	
Federal Trade Commission (FTC)	
Mark Eich Markus B. Heyder Christopher N. Olsen	
George Mason University	
James Cooper, directeur, recherche et politique, Law & Economics Center	
Google Inc.	
National Network to End Domestic Violence (NNEDV)	
Cynthia Fraser	
Cindy Southworth, vice-présidente développement et innovation	
Cato Institute	2012/10/05
Jim Harper, directeur des études de politique d'information	
Center for Data Innovation	
Chuck Curran, directeur exécutif	
George Washington University	
Howard Beales, professeur du département de Gestion stratégique et Politique gouvernementale	

DEMANDE DE RÉPONSE DU GOUVERNEMENT

Conformément à l'article 109 du Règlement, le Comité demande au gouvernement de déposer une réponse globale au présent rapport.

Un exemplaire des procès-verbaux pertinents (réunions nos 39 à 46, 49 à 51 et 53 à 60, 67 et 71) est déposé.

Respectueusement soumis,

Le président,

Pierre-Luc Dusseault, député

Rapport complémentaire du Nouveau Parti démocratique du Canada

Les membres néo-démocrates du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique se réjouissent que le Comité ait décidé de donner suite à la motion du NDP voulant que l'on se penche sur le rôle que jouent les médias sociaux dans la vie privée des Canadiens. Étant donné la mutation que connaît le domaine de la protection de la vie privée partout dans le monde, sous l'influence des médias sociaux et de la marchandisation des renseignements personnels, l'étude sur *La vie privée et les médias sociaux* a donné l'occasion aux députés d'examiner les implications de ces changements dans une perspective exclusivement canadienne.

Les membres néo-démocrates du Comité déplorent, toutefois, que malgré les témoignages recueillis au fil des mois, les recommandations figurant dans ce rapport soient peu ambitieuses et loin de répondre aux exigences. Bien que les lignes directrices publiées par le Commissariat à la protection de la vie privée constituent un outil important, elles ne sont pas assez fermes pour protéger les renseignements personnels des utilisateurs des médias sociaux étant donné l'avalanche de données en circulation dans le monde. Afin de rendre justice aux témoins, les néo-démocrates proposent neuf recommandations additionnelles, qui présentent une vision ambitieuse et équilibrée du rôle du gouvernement dans la protection de la vie privée.

Recommandations

Des témoignages de la commissaire à la protection de la vie privée, M^{me} Stoddart, et d'autres ont laissé entendre que le Commissariat est régulièrement aux prises avec des problèmes de non-respect des règles.[i] Les témoins successifs qui se sont exprimés devant le Comité ont déclaré que, dans l'ensemble, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) établit un cadre adéquat pour la protection des données. Étant donné que l'on assiste de plus en plus à la marchandisation et au partage des données personnelles au-delà des frontières, les faibles pouvoirs de contrainte dont dispose le Commissariat ne suffisent plus. Il n'est donc pas surprenant de voir que les autorités chargées de la protection des données dans des pays comme le Royaume-Uni, l'Allemagne, l'Australie et la France se sont

dotées de pouvoirs coercitifs (Annexe B). C'est pourquoi les néo-démocrates considèrent que ces pouvoirs doivent être au cœur de la réforme de la LPRPDE. Sans eux, les organisations qui le veulent pourront continuer de bafouer le droit à la protection de la vie privée des Canadiens.

> *« Il est difficile de faire respecter la loi actuelle. En effet, la commissaire n'a pas le pouvoir d'adopter des arrêtés et ne peut pas infliger des amendes ou d'autres pénalités dans le cas d'un comportement particulièrement inapproprié. »* – Teresa Scassa, professeure, Université d'Ottawa[ii]

Recommandation 1 : Le NPD recommande que le gouvernement confère au Commissariat à la protection de la vie privée des pouvoirs coercitifs tels que le pouvoir de délivrer des ordonnances et d'imposer des sanctions administratives pécuniaires.

Comme l'ont rapporté certains témoins, même des organisations faisant preuve de diligence et respectant la confidentialité des données peuvent être victimes d'intrusions dans les renseignements personnels qu'elles conservent[iii]. Les néo-démocrates considèrent que les Canadiens doivent être informés lorsqu'ils courent un danger après une intrusion. La perte de renseignements personnels peut entraîner le vol ou l'usurpation d'identité, ce qui peut coûter très cher aux personnes qui en sont victimes. Fixer des exigences en matière de déclaration d'atteinte à l'intégrité des données aurait pour effet d'inciter les organisations à investir dans de meilleurs systèmes de sécurité afin d'éviter d'être mises publiquement dans l'embarras et de préserver leur crédibilité. Cela implique une sécurité accrue pour le public et une meilleure confiance dans le marché électronique.

> *« Le Canada a grand besoin d'une obligation de notification des atteintes à la protection des données. Une telle obligation encouragera l'établissement de mesures de protection techniques plus musclées et donnera aux utilisateurs la possibilité de réparer le tort qui leur est fait, comme le vol d'identité et l'humiliation potentielle… »* – Tamir Israel, CIPPIC[iv]

Recommandation 2 : Le NPD recommande que le gouvernement oblige tous les organismes à déclarer le piratage ou la perte de données au Commissariat à la protection de la vie privée lorsqu'une personne raisonnable conclurait que le piratage ou la perte risque de causer un préjudice aux individus touchés.

L'examen actuel est en retard de deux ans, et la loi canadienne sur la protection des renseignements personnels est maintenant loin d'être un modèle pour le reste du monde. Les Canadiens méritent une loi sur la protection des renseignements personnels de calibre mondial. D'ailleurs, les témoignages recueillis par le Comité ont

révélé à de multiples reprises que le Canada accuse un net retard par rapport à d'autres pays comparables au chapitre de la protection des données et du respect de la vie privée. Bien que les néo-démocrates soient favorables au maintien d'un modèle techniquement flexible en ce qui concerne la LPRPDE, ils ne croient pas qu'il faille pour autant éviter de reconnaître le changement de paradigmes. Qui plus est, la LPRPDE doit faire l'objet d'un examen quinquennal.

> « *Le Commissariat a effectué des recherches et des analyses approfondies en prévision du deuxième examen quinquennal obligatoire de la Loi sur la protection des renseignements personnels et les documents électroniques par le Parlement, qui est maintenant échu. Nous réfléchissons attentivement à la façon dont nous pourrions moderniser le régime actuel, qui a été mis en place avant tous ces progrès technologiques novateurs. »* – Jennifer Stoddart, commissaire à la protection de la vie privée[v]

Recommandation 3 : Le NPD recommande que le gouvernement modernise les lois canadiennes sur la protection de la vie privée afin de les harmoniser avec les mesures de protection en vigueur dans des pays démocratiques comparables au nôtre et qu'il veille à ce que les renseignements personnels des Canadiens soient bien protégés à l'ère numérique.

Avec la multiplication continue des services et des applications électroniques, on assiste à une prolifération des conventions de droits d'utilisation et des politiques sur la protection de la vie privée auxquelles les Canadiens doivent se conformer. Ces conventions sont généralement longues, jargonneuses et incompréhensibles; il n'en demeure pas moins qu'elles ont des répercussions profondes sur le contrôle que peuvent exercer les gens sur leurs renseignements personnels. À ce propos, la professeure Valerie Steeves a déclaré que les conventions de droits d'utilisation et les politiques sur la protection de la vie privée sont souvent davantage conçues de manière à limiter la responsabilité des fournisseurs de services qu'à bien informer les utilisateurs[vi]. Cela a donné lieu à une érosion de l'efficacité du principe de consentement prévu dans la LPRPDE. Les néo-démocrates sont d'avis qu'avec le développement des capacités de surveillance, comme les mécanismes de géolocalisation ou les outils de reconnaissance faciale, il faudrait faire preuve de plus de transparence à l'égard des Canadiens lorsqu'ils consentent à l'utilisation de leurs renseignements personnels.

> *« . L'un des problèmes clés en matière de protection des renseignements personnels sur les sites de médias sociaux demeure la multiplication des standards et des protections relatives à la préservation de la vie privée. On déplore l'absence d'un cadre cohérent, clair et exhaustif qui*

offrirait aux utilisateurs des médias sociaux un ensemble de normes claires en matière de protection des renseignements personnels... » – Normand Landry, professeur TÉLUQ[vii]

Recommandation 4 : Le NPD recommande que le gouvernement examine l'annexe 1 de la LPRPDE afin de clarifier qu'il faudrait en règle générale obtenir le consentement explicite avant de divulguer des renseignements personnels à un tiers et que ce consentement soit particulièrement nécessaire lorsque la divulgation constitue une exigence d'une convention de licence d'utilisation.

Outre qu'il traîne de la patte en matière de protection de la vie privée, le gouvernement rechigne à élaborer une stratégie de l'économie numérique globale, alors qu'il promet de le faire depuis des années. De telles stratégies ont pourtant fait leurs preuves ailleurs, que ce soit en Australie ou en Estonie. Le NPD donne foi aux témoignages laissant entendre que le manque de leadership et d'ambition du gouvernement dans le dossier du numérique nous coûtera cher. De plus, notre parti estime qu'une éventuelle stratégie du numérique devrait aborder de front les problèmes de protection de la vie privée.

« Je crois que le fait de ne pas avoir énoncé et mis en œuvre une stratégie nationale en matière d'économie numérique revient nous hanter. » – Michael Geist, Université d'Ottawa[viii]

Recommandation 5 : Le NPD recommande que les questions de protection de la vie privée fassent partie intégrante d'une stratégie numérique globale pour le Canada.

Les consommateurs et les utilisateurs ont droit à un certain contrôle, au choix et à la transparence en ce qui concerne la façon dont on gère leurs renseignements personnels. Au cours de l'étude, le Comité a entendu des témoins vanter les mesures fructueuses qu'ont prises certains médias sociaux pour faciliter l'accès à leur cadre et à leurs paramètres par défaut de protection de la vie privée[ix]. Toutefois, ce n'est pas systématique. La marchandisation accrue des renseignements personnels incite les organisations à régler leurs paramètres par défaut de protection de la vie privée à de très faibles niveaux. De même, les fonctions de suivi comme les « cookies » sont largement répandues. Le NPD estime que le gouvernement devrait s'allier au secteur privé pour promouvoir l'inclusion de la protection intégrée dans les paramètres par défaut et mettre au point des fonctions de non-conservation des données pour les utilisateurs.

« Nous disons toujours que la protection est excellente pour les affaires. Elle devrait assurer certains avantages aux entreprises qui ont de bonnes pratiques en la matière. » – Anne Cavoukian, commissaire à l'information et à la protection de la vie privée de l'Ontario[x]

« The Devil is in the Defaults*. En bref, l'architecture de chaque technologie inclut un certain nombre de choix dans la conception. »* – Ian Kerr, Université d'Ottawa [xi]

Recommandation 6 : Le NPD recommande que le gouvernement étudie la possibilité d'examiner la LPRPDE et le règlement correspondant afin d'encourager les organisations à garantir la protection de la vie privée par principe.

Recommandation 7 : Le NPD recommande que la LPRPDE, le règlement correspondant et toute loi pertinente soient modifiés en vue d'encourager les organisations à mettre en place des fonctions de non-conservation des données.

Le NPD est déçu de constater que le rapport ne contient aucune recommandation ambitieuse sur la protection des enfants. Le Comité a entendu des témoins souligner qu'il y avait de plus en plus de publicité en ligne ciblant les enfants[xii]. Lors de sa comparution, M[me] Stoddart a dit douter que les enfants puissent réellement donner un consentement valide et éclairé au sens où l'entend la LPRPDE[xiii]. Le Comité a entendu de nombreux spécialistes relater la difficulté à protéger les renseignements personnels des enfants par la voie législative. Par exemple, Sara Grimes, professeure à l'Université de Toronto, a préconisé l'instauration, au Canada, d'une réglementation adaptée aux enfants, tandis que Valerie Steeves, professeure à l'Université d'Ottawa, a rappelé les options de consentement à plusieurs niveaux, basé sur l'âge, dont il a été question lors du dernier examen de la LPRPDE. Le NPD estime que pour qu'ils puissent profiter pleinement des avantages sociaux, culturels et démocratiques qu'offrent les médias sociaux, les enfants devraient pouvoir compter sur de solides mécanismes de protection de la vie privée.

« Il y a un besoin évident et grandissant de mettre en place une réglementation adaptée aux enfants en ce qui concerne la collecte, la gestion et l'utilisation des données relatives aux enfants. » – Sara Grimes, Université de Toronto[xiv]

Recommandation 8 : Le NPD recommande que le gouvernement continue d'étudier des façons de mieux protéger les renseignements personnels des enfants en ligne en les encourageant eux aussi à profiter des avantages sociaux, culturels et démocratiques du cyberespace.

Les internautes et adeptes des médias sociaux laissent des traces numériques chaque fois qu'ils fréquentent la Toile. Selon la LPRPDE, on ne doit conserver les

renseignements personnels qu'aussi longtemps que nécessaire pour des fins déterminées. M[me] Stoddart, toutefois, a fait savoir lors de sa comparution que les médias sociaux ne se conformaient pas toujours à ce principe et que nombre d'entre eux avaient encore des calendriers de conservation de données plutôt vagues[xv]. En outre, une bonne partie de ces données sont sauvegardées à l'échelle internationale, ce qui les rend difficiles à retracer. Certains témoins ont fait allusion à de récentes études européennes qui cherchaient à codifier le droit d'être oublié[xvi]. Avec la multiplication des traces numériques des internautes, le NPD estime que les Canadiens devraient être outillés pour contrôler leur historique en ligne.

> *« C'est presque un droit essentiel. On devrait pouvoir demander à une société de supprimer des renseignements. La loi précise bien que les sociétés sont censées supprimer les données qui ne servent plus, donc nous ne comprenons pas pourquoi les utilisateurs ne devraient pas avoir un droit de suppression des données. »* – John Lawford, Centre pour la défense de l'intérêt public[xvii]

Recommandation 9 : Le NPD recommande que le gouvernement mène une étude sur le principe de protection de la vie privée appelé « droit à l'oubli » et qu'il en fasse rapport au Parlement.

Ces neuf recommandations reflètent la vision ambitieuse et équilibrée du Nouveau Parti démocratique en ce qui concerne la réforme de l'accès à l'information à l'ère des médias sociaux, des données massives et de la connectivité numérique instantanée. L'expansion des médias sociaux nous offre des occasions sans précédent d'entrer en contact, de partager des connaissances, de nous mobiliser démocratiquement et d'ouvrir de nouveaux marchés pour nos biens et services. Les néo-démocrates croient que pour assurer la réussite future de l'économie et de la société numériques, il faudra reconnaître les nouveaux défis qui se posent en ce qui concerne la protection de la vie privée. Le gouvernement doit s'adapter et mettre à jour ses politiques et ses approches en matière de protection de la vie privée afin de préserver cette liberté civile fondamentale dans le monde numérique.

---

[i] ETHI, *Témoignages,* 1re session, 41e législature, 29 mai 2012, 1155 (Jennifer Stoddart, Commissaire à la protection de la vie privée).
[ii] ETHI, Témoignages, 1re session, 41e législature, 31 mai 2012, 1100.
[iii] ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1225 (Janet Goulding, Industrie Canada).
[iv] ETHI, *Témoignages*, 1re session, 41e législature, 19 juin 2012, 1115.
[v] ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1150.
[vi] ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1125.

[vii] ETHI, *Témoignages*, 1re session, 41e législature, 20 novembre 2012, 1540.
[viii] ETHI, *Témoignages*, 1re session, 41e législature, 31 mai 2012, 1110.
[ix] ETHI, *Témoignages*, 1re session, 41e législature, 30 octobre 2012, 1535(Colin MacKay, Google).
[x] ETHI, *Témoignages*, 1re session, 41e législature, 7 juin 2012, 1200.
[xi] ETHI, *Témoignages*, 1re session, 41e législature, 12 juin 2012, 1210.
[xii] ETHI, *Témoignages*, 1re session, 41e législature, 19 juin 2012, 1200 (Sara Grimes, University of Toronto).
[xiii] ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1150.
[xiv] ETHI, *Témoignages*, 1re session, 41e législature, 19 juin 2012, 1105.
[xv] ETHI, *Témoignages*, 1re session, 41e législature, 29 mai 2012, 1150.
[xvi] ETHI, *Témoignages*, 1re session, 41e législature, 12 juin 2012, 1225 (Vincent Gautrais, Université de Montréal).
[xvii] ETHI, *Témoignages*, 1re session, 41e législature, 18 octobre 2012, 1545.